Heinrich-Heine-Universität Düsseldorf

Quantum Cryptography: from Key Distribution to Conference Key Agreement

Inaugural dissertation

presented to the Faculty of Mathematics and Natural Sciences
of Heinrich-Heine-Universität Düsseldorf
for the degree of

Doctor of Natural Sciences (Dr. rer. nat.)

by

Federico Grasselli

from Assisi, Italy

Düsseldorf, June 2020

From the Institute for Theoretical Physics III
at the Heinrich-Heine-Universität Düsseldorf

Published by permission of the
Faculty of Mathematics and Natural Sciences at
Heinrich-Heine-Universität Düsseldorf

Supervisor: Prof. Dr. Dagmar Bruß
Co-supervisor: PD Dr. Hermann Kampermann

Date of the oral examination: 14.07.2020

Declaration of Authorship

I declare under oath that I have produced my thesis independently and without any undue assistance by third parties under consideration of the “Principles for the Safeguarding of Good Scientific Practice at Heinrich-Heine-Universität Düsseldorf”.

Düsseldorf, June 2020

Federico Grasselli

To my parents, Valeria and Sandro

Abstract

Recent years have seen major advancements in the field of quantum cryptography and particularly in quantum key distribution (QKD). A QKD protocol enables two parties to generate a shared secret key via an insecure quantum channel and an authenticated public classical channel. The security of QKD relies on intrinsic properties of quantum theory, such as quantum entanglement.

The primary aim of this thesis is the generalization of QKD to multiple parties with quantum conference key agreement (CKA). By exploiting multipartite entanglement, a CKA protocol establishes a secret conference key among a group of parties that can be later used to securely broadcast a message within the group.

To this aim, we first generalize the composable security framework of QKD to account for CKA and we introduce a multipartite version of the popular BB84 protocol. Hence, we prove the security of our multipartite BB84 protocol and of the multipartite six-state protocol in the finite-key regime and under the most powerful adversarial attacks. We further compare the performances of the two CKA protocols and demonstrate the feasibility of our new CKA protocol by collaborating to its experimental implementation.

Despite our focus on CKA, we also address a promising QKD scheme called twin-field (TF) QKD. TF-QKD allows two parties to establish a secret key over long distances with single-photon interferometric measurements occurring in an intermediate relay. We consider an improved TF-QKD protocol whose security is based on the estimation of certain detection probabilities. By deriving analytical bounds on these quantities, we optimize the protocol's performance and show that it can tolerate highly asymmetric losses and independent intensity fluctuations of the parties' lasers.

Inspired by the working principle of TF-QKD, we devise a novel CKA protocol where multiple users distil a conference key through single-photon interference, and prove its security. Thanks to this feature, the protocol significantly outperforms previous CKA schemes in high-loss scenarios and it employs a W-class state as its entanglement resource, in place of the conventional GHZ state.

Device-independent (DI) cryptographic protocols offer the ultimate level of security. Their security holds independently of the employed devices and relies on the observation of non-local correlations certified by a Bell inequality violation. We develop new theoretical tools for obtaining tight security analyses of multiparty DI protocols, with potential application to DI-CKA. We also apply our tools to the security of a specific tripartite DI scenario and improve previously obtained results.

Zusammenfassung

In den letzten Jahren wurden bedeutende Fortschritte im Bereich der Quantenkryptografie und insbesondere im Quantenschlüsselaustausch (QKD) erzielt. Ein QKD-Protokoll ermöglicht es zwei Parteien einen sicheren Schlüssel über einen unsicheren Quantenkanal und einen authentifizierten und öffentlichen, klassischen Kanal zu teilen. Die Sicherheit des QKDs beruht auf intrinsischen Eigenschaften der Quantentheorie wie zum Beispiel Quantenverschränkung.

Das primäre Ziel dieser Thesis ist die Verallgemeinerung des QKDs auf mehrere Parteien mittels der Quantenkonferenzschlüsselvereinbarung (CKA). Unter Ausnutzung von Mehrparteienverschränkung wird ein sicherer Konferenzschlüssel zwischen einer Gruppe von Parteien etabliert welcher später genutzt werden kann, um sicher Nachrichten innerhalb der Gruppe zu versenden.

Dazu erweitern wir den zusammensetzbaren Sicherheitsformalismus von QKD auf CKA und führen eine Mehrparteienversion des berühmten BB84-Protokolls ein. Wir beweisen also die Sicherheit unseres Mehrparteien BB84 und des Mehrparteien Sechs-Zustand-Protokolls in einem Regime mit endlichem Schlüssel unter Berücksichtigung der allgemeinsten Lauschangriffe. Anschließend vergleichen wir die Performance beider CKA-Protokolle miteinander und demonstrieren die Durchführbarkeit unserer neuen CKA-Protokolle, indem wir bei der experimentellen Implementierung kollaborieren.

Ungeachtet unseres Fokus auf CKA befassen wir uns ebenfalls mit einem vielversprechenden QKD Schema, dem sogenannten Zwillingsfeld (TF-) QKD. TF-QKD erlaubt es zwei Parteien einen sicheren Schlüssel über große Distanzen zu etablieren. Dies geschieht mittels interferometrischen Einzel-Photonen Messungen welche in Zwischenrelais auftreten. Wir betrachten ein verbessertes TF-QKD Protokoll dessen Sicherheit auf der Schätzung bestimmter Detektionswahrscheinlichkeiten beruht. Durch das Herleiten analytischer Schranken für diese Größen optimieren wir die Performance des Protokolls und können zeigen, dass es hohe asymmetrische Verluste und voneinander unabhängige Intensitätsschwankungen der Laser einzelner Parteien tolerieren kann.

Durch das Funktionsprinzip des TF-QKDs inspiriert, entwickeln wir ein neues CKA-Protokoll in welchem mehrere Nutzer mittels Einzel-Photonen Interferenz einen Konferenzschlüssel destillieren und beweisen dessen Sicherheit. Dank dieser Eigenschaft übertrifft das Protokoll frühere CKA-Schemata in Szenarios mit großen

Verlusten unter Verwendung eines Zustands der W-Klasse anstelle des allgegenwärtigen GHZ Zustandes.

Apparateunabhängige (DI-) Protokolle bieten den höchsten Grad kryptografischer Sicherheit. Ihre Sicherheit gilt unabhängig von der internen Funktionsweise eines spezifischen Apparats und beruht auf der Beobachtung nicht-lokaler Korrelationen, welche durch die Verletzung einer Bell-Ungleichung zertifiziert werden. Wir entwickeln neue theoretische Methoden für stringente Sicherheitsanalysen von Mehrparteien DI-Protokollen mit potentiellen Anwendungen auf DI-CKA. Außerdem wenden wir unsere Methoden auf ein spezifisches Dreiparteien DI-Szenario an und verbessern zuvor erzielte Resultate.

Acknowledgement

I would like to start by thanking my supervisor Dagmar Bruß and my co-supervisor Hermann Kampermann for giving me the opportunity to join them, on a fantastic three-year journey, in the European Innovative Training Network QCALL. It has been a privilege to work alongside all the talented scientists in the network, always within a warm and friendly atmosphere. I feel I could not have asked for a better experience as a PhD student.

My research greatly benefited from the guidance provided by Dagmar Bruß and Hermann Kampermann, from their constructive criticisms and their passionate attitude towards science. They will certainly represent an inspiration for me throughout my career.

I also would like to thank my colleagues in Düsseldorf: Carlo Liorni, Felix Bischof, Giacomo Carrara, Giulio Gianfelici, Gláucia Murta, Lucas Tendick, Sarnava Datta, Thomas Wagner and Timo Holz together with the Master's students Daniel Miller and Juan Manuel Henning. With each of them I had interesting and helpful discussions on both scientific and non-scientific topics. In particular, I acknowledge the fruitful collaborations with Gláucia and the help of Carlo, Giulio, Gláucia, Lucas, Sarnava and Thomas who proofread this thesis. I extend my gratitude to all the other members of our research group.

I am grateful for the opportunities to collaborate with other great scientists, who enriched and widened my view on many research topics. Among these, I am particularly thankful to Marcos Curty and Álvaro Navarrete in Vigo and Massimiliano Proietti, Joseph Ho and Alessandro Fedrizzi in Edinburgh.

Moving from Italy to Germany and starting a new social life was made much easier thanks to the amazing group of international friends I had the fortune to meet in these years. A special thanks goes to Ayesha Din for her love, unconditional support and for being my biggest fan.

The greatest merit for shaping the person I am and enabling me to achieve such goals goes to my parents. The value of the education I received from them becomes clearer –as for many of us– when older. Here I acknowledge all of that value and express my deepest gratitude.

Contents

List of Figures

Introduction 1

> *[...] God had meant photons to travel rather than to stay put! This was the insight that made us think of using a quantum channel to transmit confidential information.*
>
> — **Gilles Brassard**

Quantum cryptography exploits distinctive quantum properties of nature in order to perform a given cryptographic task. Most quantum cryptographic protocols are –at least in principle– information-theoretically secure, which is a very strong notion of security as it is deduced purely from information theory.

Early ideas to use quantum properties for security purposes date back to the '70s [Bra05; Ben+83], when Wiesner aimed to create unfalsifiable bank notes [Wie83]. These ideas seemed however very unpractical as they required to store a single polarized photon for days without losses (at the time, photon polarization was the only conceived carrier of quantum information).

The breakthrough occurred in 1983, when Bennett and Brassard realized that photons are best used to transmit quantum information rather than to store it. In particular, they could be used to transmit a random secret key from a sender to a receiver, who can then use the key to encrypt and decrypt sensitive messages. Shortly after, Bennett and Brassard published the first quantum key distribution (QKD) protocol in 1984 [BB84], hence named BB84 protocol. Since then, many new protocols have been proposed [Eke91; Bru98; Sca+09] and implemented [Dia+16], allowing QKD to become the major application of quantum information science.

Furthermore, pushed by increasing concerns on data security and by the prospect of commercialization, the research on QKD has spread beyond the walls of academia and attracted the attention of several companies, private institutions and governments [Com; Tec]. In fact, a growing number of companies and startups worldwide are offering QKD solutions.

In the long term scientists envision the creation of large-scale quantum networks where, thanks to quantum entanglement, QKD-enabled secure communication is possible among any subset of users in the network. With a broader perspective, such networks could be linked together in a quantum internet [Kim08; WEH18] that would serve much more scopes than just secure communication, e.g. secure access to remote quantum computers [BFK09; Fit17].

1.1 Motivation and Results

The research on QKD beautifully combines ideas and contributions coming from various fields of study, ranging from quantum information and quantum communication, to computer science and cryptography. The interplay between these diverse disciplines leads to theoretical advancements that can be of broad interest and applicable to other research fields.

Nonetheless, because of the significant commercial appeal of QKD, the on-going research is also guided by more practical purposes. For instance, combined theoretical and experimental efforts are devoted to stretching the maximum distance at which QKD can be performed, while guaranteeing high key-generation rates with simple experimental setups.

To this aim, part of our doctoral research addressed a novel QKD protocol which has recently received a lot of attention from the scientific community. The protocol, named twin-field (TF) QKD [Luc+18; CAL19], has quickly become the new benchmark for long-distance QKD while maintaining high security standards.

In this context, we derive theoretical expressions that allow us to assess the performance of the TF-QKD protocol devised in [CAL19] for a realistic implementation of the protocol. From our results [GC19; GNC19] (appendices C and D), we can conclude that the TF-QKD protocol in [CAL19] can achieve at the same time long distances and high performance even in conditions previously considered very unfavourable, as later confirmed experimentally.

The major part of our doctoral research, however, focuses on the development, security analysis and simulation of the generalization of QKD to multiple users: multipartite QKD, also known as quantum conference key agreement (CKA). A CKA protocol is employed when a confidential message needs to be securely broadcast within a group of users. The users, upon performing a CKA protocol, share a common secret key –the conference key– with which they can encrypt and decrypt the secret message. Quantum conference key agreement also represents one of the first natural applications of the emerging quantum networks.

In our first publication on this topic [GKB18] (appendix B), we introduce a multipartite generalization of the BB84 protocol. We provide a complete proof of its security in the most adversarial scenario and benchmark its performance with another multipartite QKD protocol, under realistic conditions. We also collaborate to the experimental realization of our protocol [Pro+20] (appendix F), taking care of the security aspects of its implementation.

Inspired by our work on TF-QKD, we devise a new CKA protocol [GKB19] (appendix E) which can be regarded as a multiparty generalization of the TF-QKD protocol in [CAL19]. We prove the protocol's security in very general circumstances and show that, similarly to its bipartite counterpart, it can substantially outperform other multipartite QKD protocols over long distances.

Among quantum cryptographic protocols, those offering the highest level of security are the so-called device-independent (DI) protocols, such as DIQKD protocols and DI randomness generation (DIRG) protocols. Indeed, the security of these protocols holds independently of the actual functioning of the devices used to implement them. This remarkable feature relies on the non-local nature of quantum correlations.

In our latest work [Gra+20] (appendix H), we develop important theoretical tools that enable more accurate security proofs of multiparty DI protocols. We also apply these tools to improve the security of specific protocols, with potential application to DI conference key agreement (DICKA).

Finally, we produce an exhaustive review of the existing CKA protocols [Mur+20] (appendix G), which represents the first review on this blossoming research topic.

For a more detailed list of our results, we refer the reader to chapter 7.

1.2 Thesis Structure

The contents of the thesis are organized as follows.

- In chapter 2 we set the theoretical framework by introducing all the concepts of quantum information theory that are necessary for the understanding of the remainder of the thesis. We place particular emphasis on the various entropy definitions that capture different measures of information.

- We introduce quantum key distribution (QKD) in chapter 3. After discussing the purely quantum features on which the security of QKD is based, we describe the paradigmatic BB84 protocol. We then consider a generic QKD protocol and prove its security under the most general circumstances. Subsequently we provide insights on the generalization of QKD to quantum conference key agreement (CKA) and briefly describe the functioning of our multipartite BB84 protocol. We conclude the chapter by listing some important state-of-the-art QKD experiments.

- In chapter 4 we draw attention to the security threats posed by performing QKD with imperfect quantum devices and discuss the solutions proposed so far. Specifically, we present the decoy-state method to deal with sources emitting multiple photons. We also introduce the concept of measurement-device-independent QKD, whose security is independent of the trustworthiness of the measurement devices.

- The subject of chapter 5 is the novel TF-QKD protocol, which applies the solutions to the security threats discussed in the previous chapter. In this chapter we also present recent fundamental bounds on the performance of any point-to-point QKD protocol. We introduce TF-QKD by describing its first version and the improved version that we investigate. We summarize the results of our investigation with the support of plots simulating the protocol's performance in realistic conditions. Insight is provided on the theoretical results that enable a practical performance assessment of TF-QKD. The last part of the chapter is devoted to the presentation and discussion of our new CKA protocol based on the founding idea of TF-QKD.

- We start chapter 6 by proving Bell's theorem and introducing the concept of Bell inequality. We show that quantum correlations can violate Bell inequalities and clarify the relations between local, quantum, no-signaling and causal correlations. We then elucidate the link between the violation of a Bell inequality and the security of a device-independent (DI) QKD protocol. From there, we introduce the archetypal DIQKD protocol based on the violation of the Clauser-Horne-Shimony-Holt inequality, and prove its security. We then present our theoretical results enabling similar security proofs for multipartite DI protocols. We conclude the chapter by presenting a multipartite Bell inequality specifically designed to be applied in a DICKA protocol.

- We provide a concise overview of the results of our doctoral research in chapter 7.

- Chapter 8 concludes the thesis and gives an outlook on future research directions that stem from the results of our doctoral research.

The original publications of our research manuscripts are provided in appendices B to H, while appendix A contains the proofs of statements made in the main body of the thesis.

2 Elements of Quantum Information Theory

> *Fundamental measures of information arise as the answers to fundamental questions about the physical resources required to solve some information processing problem.*
>
> — **Nielsen & Chuang**

In this thesis, we assume the reader to be familiar with the fundamental concepts of quantum mechanics and linear algebra. Nonetheless, in this chapter we will briefly review some of those concepts using the Dirac notation and the density operator formalism (sections 2.1-2.5). We also introduce the entropies characterizing information-processing tasks which commonly occur in quantum cryptography (sections 2.6 and 2.7). The content of this chapter is mostly inspired by the following literature: [KLM07; NC10; Ros11; Ren08].

2.1 Dirac Notation and Linear Algebra

The state of a quantum mechanical system, with d degrees of freedom, is represented by a normalized vector $|\psi\rangle$ in a d-dimensional Hilbert space $\mathcal{H}$ over the complex numbers $\mathbb{C}$, called the *state space* of the system. A *Hilbert space* is an inner product space, which is also complete with respect to the norm induced by the inner product if the space is infinite-dimensional.

The vector symbol $|\psi\rangle$ is called a *ket*. To every vector $|\psi\rangle$ in $\mathcal{H}$ corresponds a unique dual vector $\langle\psi|$ in the dual Hilbert space $\mathcal{H}^*$, i.e. the space of linear maps from $\mathcal{H}$ to $\mathbb{C}$. The symbol $\langle\phi|$ of a dual vector is called a *bra*. Note that the dual of a linear combination of vectors $\alpha\,|a\rangle + \beta\,|b\rangle$ is defined as $\alpha^*\,\langle a| + \beta^*\,\langle b|$, where α^* is the complex conjugate of $\alpha \in \mathbb{C}$.

The action of a linear map $\langle\phi| \in \mathcal{H}^*$ on a vector $|\psi\rangle \in \mathcal{H}$ is written as a “bra-ket”: $|\psi\rangle \mapsto \langle\phi|\psi\rangle \in \mathbb{C}$ and defines the inner product of vectors $|\psi\rangle$ and $|\phi\rangle$ in $\mathcal{H}$. Two vectors are said to be *orthogonal* if their inner product is zero. The *norm* induced by the inner product is given by: $\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$. A vector $|\psi\rangle$ is said to be *normalized*, or called a *unit vector*, if $\||\psi\rangle\| = 1$. An *orthonormal* set of vectors $\{|\psi_i\rangle\}$ is exclusively composed of normalized and mutually orthogonal vectors: $\langle\psi_i|\psi_j\rangle = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta.

The Dirac notation provides a useful way to represent the action of linear operators on $\mathcal{H}$, through the *outer product*. The outer product of $|\psi\rangle \in \mathcal{H}$ and $\langle\phi| \in \mathcal{H}^*$ is represented by $|\psi\rangle\langle\phi|$ and acts as follows on $|\gamma\rangle \in \mathcal{H}$: $|\gamma\rangle \mapsto \langle\phi|\gamma\rangle\,|\psi\rangle$. The outer product of a vector $|\psi\rangle$ by itself defines a linear operator that projects a vector $|\phi\rangle \in \mathcal{H}$ in the one-dimensional subspace spanned by $|\psi\rangle$: $|\psi\rangle\langle\psi||\phi\rangle = \langle\psi|\phi\rangle\,|\psi\rangle$.

From this definition, it immediately follows that any orthonormal basis $\{|b_i\rangle\}_{i=1}^{d}$ of the d-dimensional Hilbert space $\mathcal{H}$ satisfies the *completeness relation*: $\sum_{i=1}^{d}|b_i\rangle\langle b_i|= \mathrm{id}$, where id is the identity operator. With the completeness relation, it is possible to represent the action of any linear operator A in the outer product notation:

$$A = \mathrm{id}\,A\,\mathrm{id} = \sum_{i,j=1}^{d} \langle b_i|A|b_j\rangle\,|b_i\rangle\langle b_j|, \tag{2.1}$$

where the element $\langle b_i|A|b_j\rangle$ can be regarded as the matrix entry in the i-th row and j-th column of the *matrix representation* of A with respect to the basis $\{|b_i\rangle\}_{i=1}^{d}$.

We define the *adjoint* or *Hermitian conjugate* of an operator A on $\mathcal{H}$, the operator $A^\dagger$ on $\mathcal{H}^*$ such that:

$$(\langle\psi|A^\dagger|\phi\rangle)^* = \langle\phi|A|\psi\rangle \quad \forall\ |\psi\rangle\,, |\phi\rangle \in \mathcal{H}. \tag{2.2}$$

This implies that the matrix representing $A^\dagger$ is obtained from that of A by applying transposition and complex conjugation. It also follows that $(|\psi\rangle\langle\phi|)^\dagger = |\phi\rangle\langle\psi|$.

The evolution of a closed quantum system is determined by a *unitary* operator U, that is an operator for which $U^\dagger = U^{-1}$, where U^{-1} is the inverse of U. A unitary transformation also links any two bases $\{b_i\}_{i=1}^{d}$ and $\{b_i'\}_{i=1}^{d}$ in $\mathcal{H}$: $|b_i'\rangle = U\,|b_i\rangle$. Two bases are called *mutually unbiased* if $\langle b_i'|b_j\rangle = 1/d$ for every i and j.

The observable quantities in quantum mechanics are represented by Hermitian operators. An operator A is called *Hermitian* if $A = A^\dagger$. An important class of Hermitian operators is the orthogonal projectors.

An operator P is called a *projector* if $P^2 = P$. If P is also Hermitian, then it is called an *orthogonal* projector. An example is given by the following *rank-one* orthogonal projector $|\psi\rangle\langle\psi|$. Note that any orthogonal projector can be written as:

$$P = \sum_{i\in S}|b_i\rangle\langle b_i|\,, \quad S \subseteq \{1,\ldots,d\}, \tag{2.3}$$

i.e. as a sum of rank-one projectors on some elements of an orthonormal basis $\{|b_i\rangle\}_{i=1}^{d} \subset \mathcal{H}$.

Importantly, the eigenvalues a_i of an Hermitian operator $A = A^\dagger$ on the d-dimensional Hilbert space $\mathcal{H}$ are real and the eigenvectors form an orthonormal basis $\{|a_i\rangle\}_{i=1}^{d}$ (if d is finite), called the *eigenbasis* of A. Then, the operator A can be written in its *spectral decomposition* as follows:

$$A = \sum_{i=1}^{d} a_i |a_i\rangle\langle a_i|. \tag{2.4}$$

Finally, we define the *trace* of an operator A on $\mathcal{H}$ as follows:

$$\mathrm{Tr}[A] = \sum_{i=1}^{d} \langle b_i|A|b_i\rangle \,, \tag{2.5}$$

where $\{|b_i\rangle\}_{i=1}^{d}$ is any orthonormal basis for $\mathcal{H}$. We remark that the trace definition is independent of the chosen basis thanks to the cyclic property of the trace $\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$ and to the fact that a change of orthonormal basis is represented by a unitary operator.

2.2 Density Operator Formalism

We have so far identified the state of a quantum system by its wave function $|\psi\rangle$, implicitly assuming that it can be completely determined. However, from a practical point of view, this is not always feasible. Consider, for instance, an electron-target scattering experiment where the electron beam is prepared without the use of polarizers. The electron spin will probably be oriented in a random direction for each electron of the beam. Thus, the spin of the beam cannot be described by a *pure state* of the form:

$$|\psi\rangle = \alpha \,|{\uparrow}\rangle_z + \beta \,|{\downarrow}\rangle_z \,, \tag{2.6}$$

since the latter describes a spin oriented in a specific direction, fixed by the polar angles $\theta = 2 \arccos |\alpha|$ and $\varphi = \arg\beta - \arg\alpha$. Rather, the state of the beam spin is described by an ensemble of spins oriented in all directions, weighted by their probability of occurrence: a *mixed state*.

In cases like this, where the lack of information on an ensemble of single states prevents us from describing them one by one completely, we can still study such a collection of states statistically by means of the *density operator*, introduced by von Neumann in 1927.

Definition 2.1 (Density Operator)**.** *Consider a quantum system that is found in one of the pure states $\{|\psi_i\rangle\}$ with probabilities $p_i < 1$, where $\sum_i p_i = 1$. Then, the state of the system is called a mixed state and is described by the density operator*

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{2.7}$$

The matrix representation of ρ is called density matrix, which is often used to indicate the operator itself.

If a quantum system is in a pure state $|\psi\rangle$ with certainty, then its density operator reads: $\rho = |\psi\rangle\langle\psi|$. A criterion to determine whether a state ρ is pure or mixed is given by the computation of its *purity*: $\mathrm{Tr}[\rho^2]$. A state is pure if $\mathrm{Tr}[\rho^2] = 1$, while it's mixed if $\mathrm{Tr}[\rho^2] < 1$.

Density operators offer an alternative formulation of quantum mechanics, which is particularly useful in quantum information. Here we provide an intrinsic characterization of density operators, which allows us to abandon their interpretation in terms of an ensemble of pure states.

Theorem 2.1 (Characterization of density operators)**.** *An operator ρ is the density operator of a mixed state $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ if and only if it is normalized ($\mathrm{Tr}[\rho] = 1$) and positive ($\rho \geq 0$, i.e. Hermitian with non-negative eigenvalues).*

The proof of this Theorem can be found in [NC10].

We can now reformulate the postulates of quantum mechanics in the density operator picture.

Postulate 2.1. *The state of a quantum system is completely determined by a normalized positive operator, denoted density operator, acting on a Hilbert space $\mathcal{H}$ named the state space of the system.*

Postulate 2.2. *The evolution of a closed quantum system is determined by a unitary transformation U. Specifically, the evolved state of the system ρ' is obtained from the initial state ρ as follows:*

$$\rho' = U\rho U^\dagger. \tag{2.8}$$

Postulate 2.3. *The measurement of a quantum system is defined by a collection of measurement operators $\{M_m\}$ acting on $\mathcal{H}$ and satisfying the completeness relation: $\sum_m M_m^\dagger M_m = \mathrm{id}$. If ρ is the state of the system prior to measurement, the probability of observing the measurement outcome m is given by:*

$$\Pr(m) = \mathrm{Tr}[M_m^\dagger M_m \rho] \tag{2.9}$$

and the state of the system after the measurement reads

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}[M_m^\dagger M_m \rho]}. \tag{2.10}$$

Postulate 2.4. *The state space $\mathcal{H}$ of a composite quantum system, with subsystems numbered from 1 to n, is given by the tensor product of the state spaces $\mathcal{H}_i$ composing the system: $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n$.*

Thanks to Postulates 2.1 and 2.4, we can describe the state of a composite system commonly encountered in quantum information. Consider a quantum system Q whose state depends on the value x of a classical random variable X, with probability distribution $\mathrm{Pr}(x)$. For an observer who ignores the value of X, the global state of the quantum system and of the classical variable is given by:

$$\rho_{XQ} = \sum_x \mathrm{Pr}(x)\,|x\rangle\langle x|_X \otimes \rho_Q^x, \tag{2.11}$$

where the random variable X is represented by orthogonal pure states $|x\rangle$, since its classical outcomes can be perfectly distinguished. The quantum system is instead found in one of the *conditional states* ρ_Q^x. Moreover, we say that ρ_{XQ} is *classical on* X or is a *classical-quantum* (c.q) state if it can be written in the form (2.11).

2.2.1 POVMs and Projective Measurements

Postulate 2.3 provides the most general description of a quantum measurement. There are two special cases of quantum measurements which are of particular interest in quantum information. The first one is the positive operator-valued measure (POVM), which simplifies the formalism when only the measurement statistics matters.

Definition 2.2 (POVM). *A POVM is defined by a set of positive operators $\{E_m\}$, the POVM elements, acting on the state space, such that $\sum_m E_m = \mathrm{id}$. Then the probability of obtaining outcome m when measuring the system in state ρ is given by:*

$$\mathrm{Pr}(m) = \mathrm{Tr}[E_m \rho]. \tag{2.12}$$

One can readily see that POVMs are a special case of Postulate 2.3, when the measurement operators are given by $M_m = \sqrt{E_m}$, which implies $M_m^\dagger M_m = E_m$.

The only case in which the measurement operators and the POVM elements coincide is for *projective measurements*, i.e. when they are orthogonal projectors: $E_m = M_m = P_m$. By combining the general expression of an orthogonal projector (2.3) with the constraint given by the completeness relation: $\sum_m P_m = \mathrm{id}$, one verifies that the projectors $\{P_m\}$ are mutually orthogonal: $P_m P_n = \delta_{m,n} P_n$. From the measurement outcomes and the projectors it is possible to define an Hermitian operator M, called *observable*, through its spectral decomposition:

$$M = \sum_m m P_m. \tag{2.13}$$

Often, a projective measurement is equivalently defined as the measurement of an observable M, meaning that the projectors are those appearing in its spectral decomposition (2.13). If the projectors are all rank-one $P_m = |m\rangle\langle m|$, the measurement is called a *von Neumann measurement*.

Identifying a projective measurement with the observable M is useful when, for instance, one wants to compute the average outcome, since it can be directly written in terms of the observable M:

$$\langle M \rangle := \sum_m m \Pr(m) = \sum_m m \operatorname{Tr}[P_m \rho] = \operatorname{Tr}[M\rho]. \tag{2.14}$$

Finally we remark that, although projective measurements are particular cases of POVMs, the statistics of any POVM on a d-dimensional Hilbert space can be reproduced by combining a projective measurement on a Hilbert space of dimension $d' \geq d$ with a unitary operation. This result is known as the Naimark theorem [DJR05; Per06].

2.3 Qubits and Pauli Operators

In many quantum information applications, the fundamental quantum system is a two-level system called quantum bit or *qubit*. Physical realizations of qubits are, for example: a photon that can be found in one of two distinct paths, two orthogonal polarizations of a photon, the spin state of spin-$\frac{1}{2}$ particles, or the two lowest energy levels of an electron orbiting a nucleus.

The state of a qubit is described by a density operator acting on a two-dimensional Hilbert space, $\mathcal{H}_2$. The commonly used basis for $\mathcal{H}_2$ is the *computational basis* $\{|0\rangle, |1\rangle\}$. Thus, any pure qubit state is represented by a superposition of the form: $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.

Conversely, any general (possibly mixed) qubit state ρ on $\mathcal{H}_2$ can be expressed as a combination of the identity operator id and the Pauli operators σ_x, σ_y and σ_z [Pau27]:

$$\rho = \frac{\mathrm{id} + \vec{r} \cdot \vec{\sigma}}{2} , \quad \vec{r} \in \mathbb{R}^3 \ : \ \|r\| \leq 1, \tag{2.15}$$

where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$. The matrix representation of the Pauli operators with respect to the computational basis reads:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \; ; \; \sigma_y = \begin{bmatrix} 0 & -\mathbb{i} \\ \mathbb{i} & 0 \end{bmatrix} \; ; \; \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.16}$$

Note that, depending on the context, we also indicate the Pauli operators as $\sigma_x = \sigma_1 = X$, $\sigma_y = \sigma_2 = Y$ and $\sigma_z = \sigma_3 = Z$. The Pauli operators are Hermitian with eigenvalues ± 1, traceless, and satisfy the following relation:

$$\sigma_i \sigma_j = \delta_{i,j} \mathrm{id} + \sum_{k=1}^{3} \varepsilon_{ijk} \sigma_k, \tag{2.17}$$

where ε_{ijk} is the Levi-Civita symbol, which is equal to $+1$ (or -1) if the triple (i, j, k) is a cyclic (or anti-cyclic) permutation of $(1, 2, 3)$, and zero if any two indices are repeated.

The representation (2.15) of a qubit state, together with (2.17), is particularly useful in many computations. For instance, the purity of a qubit state can be readily computed as: $\mathrm{Tr}[\rho^2] = (1 + \|r\|^2)/2$. Thus, the norm of the vector $\vec{r}$ indicates whether the state is pure ($\|r\| = 1$) or mixed ($\|r\| < 1$). When $\|r\| = 0$, the state is said to be *maximally mixed*.

Moreover, the vector $\vec{r}$ individuates a point inside a unit sphere, called the *Bloch sphere*, where the three Cartesian coordinates are associated with the eigenstates of the Pauli operators. Often, in the quantum information jargon one can measure “in the z direction of the Bloch sphere”, meaning that one is performing a projective measurement in the eigenbasis of σ_z, which is conventionally associated with the computational basis.

Finally, the Pauli operators have a prominent role in quantum error correction, since they represent all the possible errors that can occur when processing a qubit. In particular, σ_x produces bit flips, σ_z yields phase flips and σ_y both phase and bit flips:

$$\sigma_x |a\rangle = |\bar{a}\rangle \tag{2.18}$$

$$\sigma_z |a\rangle = (-1)^a |a\rangle \tag{2.19}$$

$$\sigma_y |a\rangle = \mathbb{i}(-1)^a |\bar{a}\rangle \,, \quad a = 0, 1 \tag{2.20}$$

where $\bar{a} = 1 - a$.

2.4 Composite Systems and Entanglement

Postulate 2.4 allows us to introduce one of the most astonishing features of quantum mechanics, entanglement, which plays a crucial role in quantum information protocols.

Suppose that two parties, Alice and Bob, locally prepare their own quantum system in the state ρ_A and ρ_B, respectively. Then, the global state of the composite quantum system, $\rho_{AB} = \rho_A \otimes \rho_B$, is called a *product state*. If the prepared states are pure: $\rho_{A(B)} = |\psi_{A(B)}\rangle\langle\psi_{A(B)}|$, even the global state is pure and represented by the following product state: $|\Psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$. Note that a compact notation for $|\psi_A\rangle \otimes |\psi_B\rangle$ is $|\psi_A, \psi_B\rangle$ or $|\psi_A \psi_B\rangle$.

Alice and Bob could also agree on locally preparing the states ρ_{A_i} and ρ_{B_i}, according to a shared random variable with distribution $\{p_i\}$. This task only requires local operations and classical communication (LOCC) . In this case, the state on $\mathcal{H}_{AB}$ is described by:

$$\rho_{AB} = \sum_i p_i \, \rho_{A_i} \otimes \rho_{B_i}. \tag{2.21}$$

However, not every composite quantum system is prepared with LOCC, hence it cannot be expressed as the state in (2.21) [GT09].

Definition 2.3 (Separability, Entanglement)**.** *A quantum state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is called separable if there exists a convex combination of pure product states $|\psi_i, \phi_i\rangle\langle\psi_i, \phi_i|$, with $|\psi_i\rangle \in \mathcal{H}_A$ and $|\phi_i\rangle \in \mathcal{H}_B$, such that:*

$$\rho_{AB} = \sum_i p_i \, |\psi_i, \phi_i\rangle\langle\psi_i, \phi_i|. \tag{2.22}$$

Otherwise, ρ_{AB} is called entangled.

Note that every state of the form (2.21) can be reduced to a state like (2.22).

Classifying whether a state is entangled or not is challenging. Consider for example the following pure states, known as *Bell states*:

$$|\Phi^{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \tag{2.23}$$

whose density operators are clearly entangled:

$$|\Phi^{\pm}\rangle\langle\Phi^{\pm}| = \frac{1}{2}\left[|00\rangle\langle 00| \pm |00\rangle\langle 11| \pm |11\rangle\langle 00| + |11\rangle\langle 11|\right]. \tag{2.24}$$

Surprisingly, their convex combination is not entangled:

$$\frac{1}{2}\left[|\Phi^{+}\rangle\langle\Phi^{+}| + |\Phi^{-}\rangle\langle\Phi^{-}|\right] = \frac{1}{2}\left[|00\rangle\langle 00| + |11\rangle\langle 11|\right]. \tag{2.25}$$

The definition of entanglement can be extended to a multipartite scenario.

Definition 2.4 (Multipartite Entanglement)**.** *Consider a set of parties labelled by the indices $\mathcal{I} = \{1, 2, \dots, n\}$ and a partition $\{\mathcal{I}_k\}_k$ of $\mathcal{I}$, where $\mathcal{I}_k$ are disjoint subsets of $\mathcal{I}$ such that $\cup_k \mathcal{I}_k = \mathcal{I}$. Then a state ρ is separable with respect to the partition $\{\mathcal{I}_k\}_k$ if it can be written as:*

$$\rho = \sum_i p_i \, \rho_{\mathcal{I}_1,i} \otimes \cdots \otimes \rho_{\mathcal{I}_k,i}. \tag{2.26}$$

If every $\mathcal{I}_k$ comprises only one index, then the state (2.26) *is called fully-separable. If a state is not fully-separable, then it is entangled. If the partition is only composed of two subsets $\mathcal{I}_1$ and $\mathcal{I}_2$, the state* (2.26) *is called biseparable. If a state cannot be expressed as a convex combination of biseparable states, then it is called genuine multipartite entangled (GME).*

An example of a pure GME state which plays a major role in multipartite quantum cryptographic protocols is the Greenberger–Horne–Zeilinger (GHZ) state [GHZ89]:

$$|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle^{\otimes n} + |1\rangle^{\otimes n} \right]. \tag{2.27}$$

A remarkable application of the density operator formalism is the ability to describe subsystems of composite systems through the *reduced density operator*. This is particularly useful when the global state is entangled and the states of its subsystems are not immediately intelligible.

Definition 2.5 (Reduced density operator)**.** *Let ρ_{AB} be the state of a bipartite quantum system. Then the reduced density operator representing the state on subsystem A is given by:*

$$\rho_A = \mathrm{Tr}_B[\rho_{AB}], \tag{2.28}$$

where Tr_B is the partial trace on subsystem B.

The partial trace is defined as the regular trace (2.5) but only acts on the subsystems indicated in the subscript. Thus, for instance:

$$\mathrm{Tr}_B[|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|] = |a_1\rangle\langle a_2| \mathrm{Tr}[|b_1\rangle\langle b_2|] = |a_1\rangle\langle a_2| \langle b_2|b_1\rangle \,. \tag{2.29}$$

Definition 2.5 is justified by the fact that the reduced density operator ρ_A provides the correct measurement statistics for measurements made on subsystem A.

2.4.1 The Schmidt Decomposition and Purifications

We observed that entanglement detection is not an easy task. A bipartite *pure* state is entangled if it cannot be expressed as a product state (Definition 2.3). A useful tool to detect entanglement in bipartite pure states is given by the *Schmidt decomposition*.

Theorem 2.2 (Schmidt decomposition)**.** *Let $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be the pure state of a bipartite system. Then there exists an orthonormal basis $\{|\alpha_i\rangle\}_{i=1}^{d_A}$ of $\mathcal{H}_A$ and an orthonormal basis $\{|\beta_j\rangle\}_{j=1}^{d_B}$ of $\mathcal{H}_B$ such that:*

$$|\psi_{AB}\rangle = \sum_{k=1}^{R} \lambda_k \, |\alpha_k, \beta_k\rangle \,, \tag{2.30}$$

where λ_k are positive real coefficients called Schmidt coefficients and $R \leq \min(d_A, d_B)$ is the Schmidt rank.

Proof. Let $\{|a_i\rangle\}_{i=1}^{d_A}$ and $\{|b_j\rangle\}_{j=1}^{d_B}$ two orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then the state $|\psi_{AB}\rangle$ can be expressed as:

$$|\psi_{AB}\rangle = \sum_{i,j=1}^{d_A,d_B} c_{ij} \, |a_i, b_j\rangle \,, \tag{2.31}$$

for some complex coefficients c_{ij} which define the complex matrix $C \in \mathbb{C}^{d_A \times d_B}$. From the singular value decomposition of C we obtain: $C = UDV$, where $U \in \mathbb{C}^{d_A \times d_A}$ and $V \in \mathbb{C}^{d_B \times d_B}$ are unitary matrices and $D \in \mathbb{R}^{d_A \times d_B}$ is a rectangular diagonal matrix of non-negative numbers. By substituting the expression for C in (2.31) we get:

$$|\psi_{AB}\rangle = \sum_{k=1}^{\min(d_A,d_B)} \sum_{i,j=1}^{d_A,d_B} u_{ik} d_{kk} v_{kj} \, |a_i, b_j\rangle \,, \tag{2.32}$$

where u_{ik}, d_{kk} and v_{kj} are the matrix elements of U, D and V, respectively. We now define new basis elements $|\alpha_k\rangle = \sum_{i=1}^{d_A} u_{ik} \, |a_i\rangle$ and $|\beta_k\rangle = \sum_{j=1}^{d_B} v_{kj} \, |b_j\rangle$. The newly defined bases $\{\alpha_k\}_{k=1}^{d_A}$ and $\{\beta_k\}_{k=1}^{d_B}$ are orthonormal since the starting ones were so. By substituting the bases in (2.32) and by discarding the terms in the sum over k where $d_{kk} = 0$, we obtain the claim in (2.30). □

Note that the Schmidt coefficients are given by the square roots of the nonzero eigenvalues of $CC^\dagger$, hence they can be easily determined.

The Schmidt decomposition allows us to immediately compute the reduced state of the two subsystems according to Definition 2.5:

$$\rho_A = \sum_{k=1}^{R} \lambda_k^2 |\alpha_k\rangle\langle\alpha_k| \quad ; \quad \rho_B = \sum_{k=1}^{R} \lambda_k^2 |\beta_k\rangle\langle\beta_k| \tag{2.33}$$

We observe that ρ_A and ρ_B are written in their spectral decomposition and have the same eigenvalues! Since many properties in quantum information are determined by the eigenvalues of a state (e.g. the von Neumann entropy, see section 2.6), they will be the same for the two subsystems of a composite quantum system in a pure state.

Moreover, if the Schmidt rank is $R = 1$, the global state is separable and the two subsystems are pure. Otherwise, for $R > 1$ the global state is entangled and the two subsystems are mixed. In this case, we can completely determine the (pure) state of the combined system (2.30), but we lack information when we focus on its single constituents (2.33) –the reduced states are mixed. This bizarre fact is one of the hallmarks of entanglement.

The missing information on system A is represented by its classical randomness, which is correlated to system B as visualized in (2.30). Only a global description of systems A and B, provided by the pure state (2.30), presents no classical randomness and hence cannot be correlated with any other system. Therefore, everything that might possibly be correlated with system A is contained in system B.

This fact is widely used in quantum cryptography. Here, a group of honest parties holds a quantum system A. One then assumes the worst-case scenario where the eavesdropper, Eve, holds the quantum system E that contains all the possible correlations with A, i.e. the composite system AE is in a pure state. We say that Eve holds the *purifying system*, which can be identified as follows.

Proposition 2.3. *Let ρ_A on $\mathcal{H}_A$ be the state of a quantum system A. Then there exists an auxiliary system E with state space $\mathcal{H}_E$ and a pure state $|\psi_{AE}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E$, called a purification of ρ_A, such that:*

$$\mathrm{Tr}_E[|\psi_{AE}\rangle\langle\psi_{AE}|] = \rho_A. \tag{2.34}$$

Proof. Consider the spectral decomposition of ρ_A: $\sum_{i=1}^{d} \lambda_i |\lambda_i\rangle\langle\lambda_i|$ and a Hilbert space $\mathcal{H}_E$ of the same dimension d of $\mathcal{H}_A$, with orthonormal basis $\{|e_i\rangle\}$. The purification of ρ_A is given by:

$$|\psi_{AE}\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\, |\lambda_i\rangle \otimes |e_i\rangle\,. \tag{2.35}$$

Indeed, we have that:

$$\begin{aligned}\mathrm{Tr}_E[|\psi_{AE}\rangle\langle\psi_{AE}|] &= \sum_{i,j=1}^{d} \sqrt{\lambda_i\lambda_j}|\lambda_i\rangle\langle\lambda_j|\mathrm{Tr}[|e_i\rangle\langle e_j|] \\ &= \sum_{i=1}^{d} \lambda_i|\lambda_i\rangle\langle\lambda_i|= \rho_A, \end{aligned} \tag{2.36}$$

as claimed. □

Note that all purifications $|\psi_{AE}\rangle$ of ρ_A are related by unitaries on E.

2.5 Quantum Operations

A quantum operation $\mathcal{E}$, also called quantum channel, provides the most general description of a physical process acting on a system in state ρ. The final state of the system, after the process occurs, is given by $\mathcal{E}(\rho)$ up to some normalization factor. Both the unitary evolution of a closed system (Postulate 2.2) and quantum measurements (Postulate 2.3) are examples of quantum operations.

Quantum operations are defined by the following three axiomatic properties, based on physical grounds.

Axiom 2.1. *The probability that the process represented by $\mathcal{E}$ occurs is given by* $\mathrm{Tr}[\mathcal{E}(\rho)] \in [0,1]$*, when ρ is the initial state.*

Axiom 2.2. *The map $\mathcal{E}$ is convex-linear on the set of density operators, i.e.*

$$\mathcal{E}\left(\sum_i p_i\rho_i\right) = \sum_i p_i\mathcal{E}(\rho_i).$$

Axiom 2.3. *The map $\mathcal{E}$ is completely positive (CP). That is, $\mathcal{E}(\rho)$ is a positive operator for every input state ρ. Additionally, for every composite state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, the operator* $(\mathrm{id}_A \otimes \mathcal{E})(\rho_{AB})$ *is positive on $\mathcal{H}_A \otimes \mathcal{H}_B$.*

The axioms are chosen such that quantum operations map density operators to density operators. Axiom 2.1 includes quantum measurements (where each outcome occurs with a certain probability) as a possible quantum operation. The normalized state after the process in this case reads $\mathcal{E}(\rho)/\mathrm{Tr}[\mathcal{E}(\rho)]$. The second axiom states a desirable property, namely that if a system is in one of the states $\{\rho_i\}$ with distribution $\{p_i\}$, after applying $\mathcal{E}$ it will be in one of the states $\{\mathcal{E}(\rho_i)\}$ with the same probability distribution. Finally, Axiom 2.3 ensures that the output of a quantum operation is still a density operator, even when it acts on a subsystem of a composite system. Note that this requirement is non-trivial, as there are maps which are positive but not CP.

Kraus' theorem is a beautiful result which characterizes quantum operations with an elegant notation.

Theorem 2.4 (Kraus). *A map $\mathcal{E}$ is a quantum operation satisfying Axioms 2.1, 2.2 and 2.3 if and only if it can be represented by a Kraus decomposition:*

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger, \tag{2.37}$$

for some set of Kraus operators $\{K_i\}$ such that $\sum_i K_i^\dagger K_i \leq \mathrm{id}$. Moreover, being d the dimension of the Hilbert space of the system on which $\mathcal{E}$ acts, the number of Kraus operators is not larger than d^2.

The proof of this theorem can be found in [NC10; Par12]. We point out that the Kraus decomposition of a quantum operation is not unique, but all the possible decompositions are linked by unitary transformations.

Unitaries and measurements are two particular cases of quantum operations with one Kraus operator each, given by: $K = U$ and $K = M_m$, respectively. However, while unitaries are trace-preserving operations, $\mathrm{Tr}[U\rho U^\dagger] = \mathrm{Tr}[\rho U^\dagger U] = 1$, quantum measurements in general are not.

An equivalent description of quantum operations interprets them as the result of the interaction between the system of interest (S) and an environment (E). Conversely, in absence of interactions with an environment, the system would evolve according to a unitary transformation (Postulate 2.2). Suppose that the system and the environment are initially in a product state, where the environment is described by a pure state $|e_0\rangle$ and the system's state is ρ. Note that assuming an initial pure state for the environment is not restrictive as we did not fix its dimension, thus we could always take its purification. The composite system ($S + E$) is closed and evolves according to a unitary U. Then, the final state of system S reads:

$$\mathcal{E}(\rho) = \mathrm{Tr}_E \left[U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \right] = \sum_i \langle e_i| \, U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger \, |e_i\rangle \, , \tag{2.38}$$

for some orthonormal basis $\{|e_i\rangle\}$ of the environment. By comparing (2.38) with (2.37), we deduce an explicit expression for the Kraus operators:

$$K_i = \langle e_i|U|e_0\rangle \, . \tag{2.39}$$

Since the operators (2.39) satisfy the completeness relation $\sum_i K_i^\dagger K_i = \mathrm{id}$, they describe trace-preserving quantum operations. Instead, non-trace-preserving quantum operations can be viewed as just described with an additional projective measurement on the combined system, following the unitary U.

2.5.1 Depolarizing Channel

An important example of quantum operation is the *depolarizing channel*:

$$\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}\sum_{i=1}^{3} \sigma_i \rho \sigma_i^\dagger, \tag{2.40}$$

with Kraus operators $K_0 = \sqrt{1-p}\,\mathrm{id}$ and $K_i = \sqrt{p/3}\,\sigma_i$. Recall from section 2.3 that every qubit error can be reproduced by applying a Pauli operator σ_i. Thus, the resulting state in (2.40) is unchanged with probability $1-p$ or is affected by one of the qubit errors with probability $p/3$ each. By applying the depolarizing channel on the qubits used in a quantum information protocol, one can test the protocol's robustness against noise.

Note that, under the substitution $p = 3q/4$, the map in (2.40) can be recast as:

$$\mathcal{E}(\rho) = (1-q)\rho + q\frac{\mathrm{id}}{2}, \tag{2.41}$$

i.e. it depolarizes a qubit with probability q by replacing it with the completely mixed state $\mathrm{id}/2$.

2.6 Entropies

The uncertainty that an observer has about a physical system, i.e. the amount of randomness characterizing the system from her perspective, is quantified by a certain entropy measure. Here we review the principal entropy measures used in the remainder of this thesis.

Definition 2.6 (Shannon entropy)**.** *Let X be a random variable whose outcomes follow the probability distribution $\{p_x\}$. The Shannon entropy of X (or of the distribution $\{p_x\}$) is given by:*

$$H(X) = H(\{p_x\}) = -\sum_x p_x \log p_x. \tag{2.42}$$

Remark 2.1. *The logarithm symbol in this thesis is always intended in base 2 and by convention it holds:* $0\log 0 = 0$.

The Shannon entropy quantifies the uncertainty about X before we learn its value. Equivalently, $H(X)$ are the bits of information gained after reading the outcome of

X. If X has only two possible outcomes, the Shannon entropy is often called *binary entropy* and reads:

$$h(p) := -p \log p - (1-p)\log(1-p) \tag{2.43}$$

Given two random variables X and Y jointly distributed according to $\{p(x,y)\}$, the joint Shannon entropy reads:

$$H(X,Y) = -p(x,y)\sum_{x,y} p(x,y), \tag{2.44}$$

while the *conditional entropy* is defined as:

$$H(X|Y) = H(X,Y) - H(Y). \tag{2.45}$$

The conditional entropy of X given Y quantifies how uncertain we are about X, given that we learned the value of Y. Finally, the *mutual information* $H(X:Y)$ measures the amount of information we gain on X by observing the value of Y. This is given by the total amount of information of X, $H(X)$, minus the uncertainty that we still have on X after learning Y, i.e. $H(X|Y)$. Thus we have:

$$H(X:Y) = H(X) - H(X|Y) = H(X) + H(Y) - H(X,Y). \tag{2.46}$$

Of the many properties satisfied by the above-defined entropies, we highlight in particular that: $H(X|Y) = H(X,Y) - H(Y) \geq 0$. We could intuitively expect this, since the uncertainty on both random variables X and Y must be greater than the uncertainty on Y. Conversely, this does not hold for quantum states, whose uncertainty is quantified by the *von Neumann entropy*.

Definition 2.7 (von Neumman entropy). *The von Neumann entropy of a quantum state ρ, with eigenvalues $\{\lambda_i\}$, is defined as:*

$$H(\rho) = -\operatorname{Tr}[\rho \log \rho] = -\sum_i \lambda_i \log \lambda_i. \tag{2.47}$$

One can interpret the von Neumann entropy of ρ as the Shannon entropy of the probability distribution defined by its eigenvalues, hence we use the same symbol. Often, the von Neumann entropy of a system A in state ρ is indicated as: $H(A)_\rho$.

For the above analogy, the previous definitions of joint entropy (2.44), conditional entropy (2.45) and mutual information (2.46) can be extended to the von Neumann entropy.

We observe that $0 \leq H(\rho) \leq \log d$ for every state ρ on a d-dimensional Hilbert space. Moreover $H(\rho) = 0$ if ρ is pure and $H(\rho) = \log d$ if the state is maximally mixed.

Suppose that the state ρ_{AB} of a composite system is given by the pure entangled state in (2.23), already written in its Schmidt decomposition. Then, the von Neumann entropy of the composite system is: $H(AB)_\rho = 0$. From the Schmidt decomposition (c.f. section 2.4) we learned that the eigenvalues of ρ_A and ρ_B are equal and given by the squares of the Schmidt coefficients. This leads to: $H(A)_\rho = H(B)_\rho = 1$. Clearly, in the quantum case the entropy of a subsystem can be larger than the entropy of the composite system and the conditional entropy becomes negative.

Other important properties of the von Neumann entropy are the *strong subadditivity*:

$$H(A|B,C) \leq H(A|B), \tag{2.48}$$

and the conditional entropy of a c.q. state. Let $\rho_{AB} = \sum_a \Pr(a)\, |a\rangle\langle a| \otimes \rho_B^a$ be a c.q. state, where the state on B depends on the value a. Then the entropy of B conditioned on A can be expressed as:

$$H(B|A)_\rho = \sum_a \Pr(a)\, H(\rho_B^a). \tag{2.49}$$

2.6.1 Operational Meaning

We conclude this section by briefly providing an operational meaning of the Shannon and von Neumann entropies, which helps us motivate the introduction of smooth entropies in the next section.

Consider a source emitting a sequence of random symbols represented by random variables $X_1, X_2, \ldots, X_n$, each of them distributed according to P_X and independent from each other. They are said to be *independent and identically distributed* (i.i.d.) random variables. The goal is to store the data by encoding it in a bitstring without losing information, so that it can be later retrieved. Then *Shannon's noiseless coding theorem* affirms that asymptotically –i.e. for diverging n– the amount of bits needed per source symbol is given by $H(X)$.

More formally, if $\ell^\varepsilon_{\text{compr}}(X)$ is the minimum amount of bits needed to compress X without losing information, except for probability ε, then the *compression rate* of the example above is given by:

$$r_{\text{compr}}(X) := \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{\ell^\varepsilon_{\text{compr}}(X_1 X_2 \cdots X_n)}{n} = H(X). \tag{2.50}$$

Similarly, we consider the quantum i.i.d. source defined by the state ρ, with spectral decomposition $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$. In other words, the source emits a sequence of quantum states drawn from $\{\psi_i\}$, according to the distribution $\{p_i\}$. For *Schumacher's noiseless coding theorem*, the fraction of qubits needed to reliably encode and decode each state in the sequence is given by the von Neumann entropy $H(\rho)$.

Unfortunately, if one removes the asymptotic or the i.i.d. assumption, the Shannon and von Neumann entropies no longer describe operational quantities.

2.7 Smooth Entropies

Here we define two generalizations of the entropies introduced in the last section, which present an operational meaning in non-i.i.d. and non-asymptotic scenarios and play a fundamental role in the security of quantum cryptographic schemes.

Definition 2.8 (Min-entropy, [Tom16; KRS09])**.** *Let ρ_{AB} be a bipartite density operator. The min-entropy of A conditioned on B of the state ρ_{AB} is defined as:*

$$H_{\min}(A|B)_\rho = -\log \min\{\mathrm{Tr}(\sigma_B) \, : \, \sigma_B \geq 0, \, (\mathrm{id}_A \otimes \sigma_B) - \rho_{AB} \geq 0\}. \qquad (2.51)$$

A very useful operational interpretation of the min-entropy in (2.51) is given in [KRS09]. Consider an agent with access to a quantum system B whose state depends on a classical random variable X. This scenario is represented by the c.q. state:

$$\rho_{XB} = \sum_x p_x \, |x\rangle\langle x| \otimes \rho_B^x, \qquad (2.52)$$

where $\{|x\rangle\}$ is a orthonormal set of vectors and $\{p_x\}$ is a probability distribution. Let $p_{\text{guess}}(X|B)$ be the probability that the agent correctly guesses X when using an optimal measurement strategy, i.e.:

$$p_{\text{guess}}(X|B) = \max_{\{E_x\}} \sum_x p_x \, \mathrm{Tr}[E_x \rho_B^x], \qquad (2.53)$$

where $\{E_x\}$ are POVM elements of a generic quantum measurement on system B. Then, the min-entropy of X conditioned on B is related to the guessing probability $p_{\text{guess}}(X|B)$ by:

$$H_{\min}(X|B)_\rho = -\log p_{\text{guess}}(X|B). \qquad (2.54)$$

Definition 2.9 (Max-entropy, [Tom16; KRS09])**.** *Let ρ_{AB} be a bipartite density operator and let ρ_{ABC} be a purification of ρ_{AB}. The max-entropy of A conditioned on B of the state ρ_{AB} is defined as:*

$$H_{\max}(A|B)_\rho = -H_{\min}(A|C)_\rho. \qquad (2.55)$$

Min- and max-entropy are also defined on a probability distribution P_X by evaluating them on the state: $\rho_X = \sum_x P_X(x)|x\rangle\langle x|$, where $\{|x\rangle\}$ is an orthonormal basis.

In general, they are related as follows to the von Neumann entropy of a bipartite density operator ρ_{AB} [TCR09]:

$$H_{\min}(A|B) \leq H(A|B) \leq H_{\max}(A|B). \tag{2.56}$$

In order to account for an error probability ε in the information-processing tasks related to min- and max-entropy, we introduce the ε-smooth versions of the entropies. First, we need to provide a suitable definition of distance between states.

Definition 2.10 (Purified distance, [Tom+11a]). *The purified distance between two positive operators ρ and τ is given by:*

$$P(\rho, \tau) = \sqrt{1 - \overline{F}(\rho, \tau)^2}, \tag{2.57}$$

where $\overline{F}(\rho, \tau)$ is the generalized fidelity:

$$\overline{F}(\rho, \tau) = \|\sqrt{\tau}\sqrt{\rho}\| + \sqrt{(1 - \operatorname{Tr}\rho)(1 - \operatorname{Tr}\sigma)} \tag{2.58}$$

and the norm of an operator O is defined as: $\|O\| = \operatorname{Tr}[\sqrt{OO^\dagger}]$.

An important property of the purified distance is that if two states are separated by a distance $P(\rho, \tau)$, there exist purifications of ρ and τ with the same purified distance.

We can now define the smooth entropies.

Definition 2.11 (Smooth entropies, [Tom16; KRS09]). *Let ρ_{AB} be a bipartite density operator. The ε-smooth min- and max-entropy of A conditioned on B of the state ρ_{AB} are given by:*

$$H^{\varepsilon}_{\min}(A|B)_\rho = \max_{\sigma \in \mathcal{B}^{\varepsilon}(\rho)} H_{\min}(A|B)_\sigma \tag{2.59}$$

$$H^{\varepsilon}_{\max}(A|B)_\rho = \min_{\sigma \in \mathcal{B}^{\varepsilon}(\rho)} H_{\max}(A|B)_\sigma, \tag{2.60}$$

where $\mathcal{B}^{\varepsilon}(\rho)$ is a ball of ε-close states centered in ρ:

$$\mathcal{B}^{\varepsilon}(\rho) = \{\tau \geq 0 \,:\, \operatorname{Tr}(\tau) \leq 1,\ P(\rho, \tau) \leq \varepsilon\}. \tag{2.61}$$

The *asymptotic equipartition property* (AEP) links the smooth entropies to the Shannon/von Neumann entropy [TCR09]:

$$H(A|B)_\rho = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H^{\varepsilon}_{\min}(A^n|B^n)_{\rho^{\otimes n}} \tag{2.62}$$

$$H(A|B)_\rho = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H^{\varepsilon}_{\max}(A^n|B^n)_{\rho^{\otimes n}}, \tag{2.63}$$

where the smooth entropies are evaluated on the i.i.d. state $\rho^{\otimes n}$. Another important property of the smooth entropies is the *data-processing inequality* [Tom16]:

$$H^{\varepsilon}_{\min}(A|B)_{\rho} \leq H^{\varepsilon}_{\min}(A|B')_{(\mathrm{id}\otimes\mathcal{E})\rho} \tag{2.64}$$

$$H^{\varepsilon}_{\max}(A|B)_{\rho} \leq H^{\varepsilon}_{\max}(A|B')_{(\mathrm{id}\otimes\mathcal{E})\rho}. \tag{2.65}$$

The data-processing inequality basically states that if we process the quantum side information B through a CP trace-preserving map $\mathcal{E}$, we always increase our uncertainty on A.

2.7.1 Operational Meaning

The smooth entropies are well suited to characterize operational quantities in realistic scenarios (e.g. finite resources and errors), which often appear in quantum cryptographic schemes.

Data compression and error correction (EC). Recall that $\ell^{\varepsilon}_{\mathrm{compr}}(X)$ is the minimum amount of bits encoding a single realization of the random variable X, from which the value of X can be recovered with probability at least $1-\varepsilon$. This quantity is essentially equal to the ε-smooth max-entropy of the distribution P_X [KRS09]:

$$\ell^{\varepsilon}_{\mathrm{compr}}(X) = H^{\varepsilon'}_{\max}(X) + O(\log 1/\varepsilon), \tag{2.66}$$

for some $\varepsilon' \in [\frac{\varepsilon}{2}, 2\varepsilon]$. This result generalizes Shannon's noiseless coding theorem (2.50) to a scenario where the number of realizations of X is finite. Shannon's theorem is recovered by employing (2.66) in (2.50) and by using the AEP (2.63). The result in (2.66) can be applied to the cryptographic scenario where two parties, Alice and Bob, establish a shared secret key (bitstring) over a noisy channel. Due to the noise, Bob only has a probability distribution $P_{X|Y}$ of the possible keys X held by Alice, conditioned on his side information Y. Alice then sends to Bob the minimal amount of information that allows him to correctly guess her key, except for probability ε. This information is equal to the smallest reliable data compression of X, when Y is known, i.e. $\ell^{\varepsilon}_{\mathrm{compr}}(X|Y)$.

Privacy amplification (PA). Consider the same cryptographic scenario described above and suppose that an eavesdropper, Eve, has access to quantum side information E correlated with Alice's key X. This can be described by a c.q. state of the form (2.52). The goal of PA is to extract a secure key $f(X)$, i.e. one that is distributed uniformly from the point of view of the eavesdropper holding E. By calling $\ell^{\varepsilon}_{\text{extr}}(X|E)$ the maximum length of $f(X)$, computed from X and which is ε-close to a bitstring Z uniform and independent of E, it holds [KRS09]:

$$\ell^{\varepsilon}_{\text{extr}}(X|E) = H^{\varepsilon'}_{\text{min}}(X|E) + O(\log 1/\varepsilon). \tag{2.67}$$

Both EC and PA are fundamental tasks in any quantum key distribution (QKD) protocol. Indeed, as we shall see in the next chapter, the final secret key length of a generic QKD protocol is determined by a combination of smooth min- and max-entropies.

3 Introducing Quantum Key Distribution

> *As the need for unbreakable encryption looms in networks around the world, quantum cryptography is the solution that will safeguard and future-proof sensitive information.*
>
> — **Commercial QKD company**

The security of classical cryptographic schemes relies on assumptions on the adversary's computational capabilities and on the fact that certain mathematical problems are considered "hard" to solve. This makes classical cryptography vulnerable to retroactive attacks. That is, an adversary could store the encrypted data while it is communicated and wait to have sufficient computational power, or smarter algorithms, in order to decrypt it. Conversely, the security of quantum cryptography relies on intrinsic principles of nature, as described by quantum mechanics. Therefore, assuming that quantum mechanics is correct, the security offered by quantum cryptography is everlasting, in the sense that it is independent of future theoretical or experimental advances of the adversary.

Quantum key distribution (QKD) is arguably the most developed task of quantum cryptography, both from a theoretical and experimental point of view.

In this chapter we first present some of the security principles of QKD in section 3.1. We then describe the BB84 protocol as an example of QKD protocol and compute its key rate (section 3.2). Section 3.3 is bit more technical, here we define and prove the security of a generic QKD protocol in the finite-key scenario. Quantum conference key agreement (CKA) extends the notion of QKD to the multipartite scenario. We introduce CKA in section 3.4 and present our multipartite generalization of the BB84 protocol (appendix B). An exhaustive review of quantum CKA protocols can be found in appendix G. We conclude the chapter by listing some state-of-the-art QKD experiments (section 3.5), including the first implementation of a CKA protocol to which we contributed (appendix F).

3.1 The Origins of Security

QKD is a specific task of quantum cryptography where two honest parties, traditionally called Alice and Bob, establish a shared secret key when connected by an insecure quantum channel and an authenticated public classical channel. The combination of QKD with the Vernam cipher [Mil82; Ver26], also called one-time pad, allows for ever-lasting secure communication.

Indeed, suppose that Alice wants to send a secret message $\vec{m}$, composed of n bits, to Bob. According to the Vernam cipher, Alice encrypts her message by adding it modulo two[1] with a n-bit key $\vec{k}$ she shares with Bob, thanks to a prior execution of a QKD protocol: $\vec{m}_e = \vec{m} \oplus \vec{k}$. She then sends the encrypted message $\vec{m}_e$ to Bob, who decrypts it by again adding the encryption key: $\vec{m}_e \oplus \vec{k} = \vec{m} \oplus \vec{k} \oplus \vec{k} = \vec{m}$. The Vernam cipher is provably secure as long as the number of key bits matches the number of message bits, and the key (or parts of it) is not reused [NC10]. The security of the communication thus depends on the security of the QKD protocol.

Many QKD protocols are based on the transmission of quantum states from Alice to Bob, through the quantum channel. The crucial fact which makes QKD secure is that a potential eavesdropper, Eve, cannot gain any information from the transmitted states without disturbing them.

For instance, an obvious attack by Eve would be to create perfect copies of the transmitted states before they reach Bob, as in classical wiretapping. However, quantum mechanics prevents this, as shown by the *no-cloning theorem*.

Theorem 3.1 (no-cloning, [WZ82]). *It is not possible to perfectly clone an unknown quantum state.*

Proof. Suppose by contradiction that we have a cloning machine and that we apply it on two distinct quantum states $|\psi\rangle \neq |\phi\rangle$ which are also non-orthogonal $\langle\phi|\psi\rangle \neq 0$. The action of the cloning machine is represented by a unitary operation U, which copies the input state on some auxiliary system initially in a normalized state $|s\rangle$:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{3.1}$$

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle\,. \tag{3.2}$$

By taking the inner product of equations (3.1) and (3.2) we obtain:

$$\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2, \tag{3.3}$$

which is only true when the states $|\psi\rangle$ and $|\phi\rangle$ are either the same state or are orthogonal, thus a general cloning machine is not possible. □

[1] The “$\oplus$” symbol always indicates the XOR operation on bits or bitstrings, unless otherwise stated.

We remark that this theorem does not contradict our common sense that classical information can be copied, since the latter is always stored in physical systems (e.g. a piece of written paper) described by orthogonal quantum states. As the proof showed, quantum mechanics does not prevent to build a machine which clones orthogonal quantum states.

Considered that Eve cannot copy non-orthogonal transmitted states, at least she would like to be able to partially distinguish them, without being noticed. However, this is also forbidden by quantum mechanics.

Proposition 3.2 (Information gain entails disturbance, [NC10])**.** *In the attempt to distinguish non-orthogonal quantum states in a quantum signal, any information gain is accompanied by a disturbance of the signal.*

Proof. Let $|\psi\rangle$ and $|\phi\rangle$ be two non-orthogonal quantum states in the quantum signal sent by Alice to Bob. Eve's action on the signal is represented by a generic quantum operation, which can be viewed as a unitary acting on a larger Hilbert space (c.f. section 2.5). In particular, the unitary acts on the state $|\psi\rangle$ (or $|\phi\rangle$) and on an ancilla $|u\rangle$. We assume that Eve's action leaves the signal states unchanged:

$$U(|\psi\rangle \otimes |u\rangle) = |\psi\rangle \otimes |v\rangle \tag{3.4}$$

$$U(|\phi\rangle \otimes |u\rangle) = |\phi\rangle \otimes |v'\rangle \,. \tag{3.5}$$

Eve would like $|v\rangle$ and $|v'\rangle$ to be different states, so she could partially distinguish the corresponding signal states. However, by computing the inner product of equations (3.4) and (3.5) we obtain that:

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle \langle v'|v\rangle \,, \tag{3.6}$$

implying that $|v\rangle = |v'\rangle$. Thus, distinguishing two non-orthogonal states implies the disturbance of at least one of them. □

The above results suggest how quantum mechanical properties can be exploited in a key distribution scheme. Alice can encode the key bits in non-orthogonal quantum states and send them to Bob. By checking the disturbance of the signal, the parties can quantitatively upper bound Eve's knowledge on the exchanged key.

3.2 The BB84 Protocol

The BB84 protocol [BB84], named after its inventors Bennett and Brassard, is commonly considered to be the first ever QKD protocol, but it is also the simplest and variations of it are investigated and implemented even today. For the protocol's description, we follow the references [Sca+09; Pir+19].

Suppose Alice possesses a source of single photons, whose spectral properties are well defined so that the only remaining degree of freedom is the photon's polarization. Alice and Bob align their polarizers and agree to employ two polarization bases, one defined by the horizontal/vertical directions and the other defined by the $+45°/-45°$ directions. The polarization state of a photon is thus represented by a qubit in $\mathcal{H}_2$. We associate the eigenbasis $\{|0\rangle, |1\rangle\}$ of Pauli operator Z to the horizontal/vertical basis and the eigenbasis $\{|+\rangle, |-\rangle\}$ of X to the $+45°/-45°$ basis, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The BB84 protocol comprises the following steps:

1. Alice sends to Bob a sequence of M photons randomly prepared in one of the four states $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$, via the quantum channel. The parties identify the bit value 0 (1) with the non-orthogonal states $|0\rangle$ and $|+\rangle$ $(|1\rangle$ and $|-\rangle)$. The non-orthogonality condition ensures that any tampering with the quantum channel by Eve, in order to gain information on the transmitted key, leads to a disturbance of the signal and can be later detected by the parties.
2. Upon receiving a photon, Bob measures randomly in either the Z or the X basis. If Bob measures in the same basis Alice used to prepare the photon, he learns the bit she encoded on that photon, provided that the signal has not been altered. If instead Bob measures in the complementary basis, he obtains a random bit since the two bases are mutually unbiased (c.f. section 2.1).
3. *Sifting:* Once the quantum communication is over, Alice and Bob publicly compare the bases they used on each photon and discard the bits corresponding to unmatching bases. This process leaves Alice and Bob with strings of approximately $M/2$ bits. In absence of errors due to noise or eavesdropping, the bitstrings of Alice and Bob would coincide.
4. *Parameter estimation (PE):* Alice and Bob reveal a random sample of their bits in order to estimate the error rate in the quantum channel and thus the information gained by Eve[2]. In particular, the parties estimate the quantum bit error rate (QBER) in the Z (X) basis, i.e. the fraction E_Z (E_X) of bits generated by measuring in the Z (X) basis that disagree. The computed QBERs are the input parameters of the following steps. The parties are now left with two partially-correlated and partially-secret bitstrings, called the *raw keys*. We denote a generic raw key bit of Alice (Bob) by the random variable R_A (R_B).

[2] For security reasons one needs to consider the worst-case scenario, i.e. that all the noise in the channel is due to Eve.

5. *Error correction (EC):* Alice and Bob run a *one-way error correction* algorithm to correct Bob's raw key to match Alice's. Alice sends the required information over a classical public channel to Bob. Other EC schemes are possible.
6. *Privacy amplification (PA):* The parties remove the information that Eve gained on their error-corrected keys by compressing them to a shorter secret key via a randomness extractor (e.g. two-universal hashing).

The figure of merit of every QKD protocol is the *secret key rate*, i.e. the fraction of secure key bits produced per protocol round[3]. A round is commonly regarded as the transmission of a quantum state through the quantum channel. The secret key rate generally depends on the total number of rounds M performed.

In the following we compute the secret key rate of the BB84 protocol in the *asymptotic scenario* of infinitely many rounds: $M \to \infty$. This is, of course, an unrealistic assumption, but it greatly simplifies the math. Moreover, the asymptotic key rate is often used as a benchmark for the performance of a newly-developed QKD protocol.

The protocol above is presented in *prepare-and-measure* form, since one party prepares and sends quantum states while the other measures them. This is typically what happens in real-life implementations of many QKD protocols. However, when proving the security of a QKD protocol or computing its key rate, an equivalent *entanglement-based* description is much more convenient.

Ideally, in every round of the entanglement-based BB84 protocol the two-qubit Bell state

$$|\Phi^+\rangle_{AB} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}} \tag{3.7}$$

is generated, and the two qubits are distributed to Alice and Bob through the quantum channel. Alice and Bob then measure the received qubit in either the Z or X basis, obtaining the same outcome if they chose the same basis. This scenario is equivalent to the prepare-and-measure one since the state Bob receives, conditioned on Alice measuring e.g. X and obtaining outcome x, is exactly $|x\rangle$ where $x \in \{+, -\}$.

However, in reality Eve could be in total in control of the quantum channel, distributing a mixed state ρ_{AB} to the parties in every protocol round. We assign to Eve all the information that can be correlated with the mixed state ρ_{AB} by assuming that she holds the purifying system E (recall subsection 2.4.1). That is, the state on A, B and E is pure: $|\phi_{ABE}\rangle$. In this scenario we say that Eve performs a *collective attack* and the quantum state representing Alice and Bob's qubits in the M protocol

[3] In experiments, the secret key rate is often given by secure key bits per second. This is obtained by multiplying the secret key rate defined here by the repetition rate of the protocol, i.e. the number of protocol rounds per second.

rounds is the i.i.d. state $\rho_{AB}^{\otimes M}$. The parties detect the presence of Eve from the errors (E_Z and E_X) in the outcomes generated by measuring ρ_{AB} at every round.

There is even a more general scenario where Eve directly distributes the state ρ_{AB}^{M} describing all the M qubit pairs to be measured, of which she holds the purifying system E, i.e. ρ_{ABE}^{M} is pure. In this case Eve is performing a *coherent attack*, which is generally more powerful than collective attacks since the states shared by Alice and Bob in each round can be correlated with past and future rounds –formally, it holds: $\rho_{AB}^{M} \neq \rho_{AB}^{\otimes M}$.

We address the case of coherent attacks in the next section, where we investigate the security of QKD when the number of protocol rounds is finite. Conversely, in the asymptotic regime discussed here, the two attacks are proven to be equivalent (c.f. subsection 3.3.3), hence we restrict to collective attacks and focus on one specific protocol round.

3.2.1 Secret Key Rate

The asymptotic secret key rate of any QKD protocol with one-way EC is given by the Devetak-Winter rate [DW05]:

$$r_{\mathrm{DW}} = H(R_A : R_B) - H(R_A : E), \tag{3.8}$$

which can be recast in the more familiar form [Ren08; SR08a; SR08b]:

$$r = H(R_A|E) - H(R_A|R_B), \tag{3.9}$$

by using the definition of mutual information (c.f. section 2.6). Recall that R_A and R_B are the random variables representing Alice's and Bob's raw key bit.

An intuitive explanation of the key rate expression (3.8) is the following. The fraction of secret bits shared by Alice and Bob per round is quantified by the amount of information that their raw key bits have in common $H(R_A : R_B)$ minus the information that Eve gained on Alice's key bit $H(R_A : E)$.

We now compute explicitly the key rate in (3.9) for the BB84 protocol, in terms of the observed quantities E_Z and E_X. For simplicity, in the computation we consider an asymmetric version of the BB84 protocol where the raw key is only extracted from Z basis measurements, while the X outcomes are used for PE (together with a fraction of Z outcomes).

The entropies in the key rate expression are computed on the c.c.q. state $\rho_{R_A R_B E}$ resulting after Alice and Bob measured their qubit in the Z basis to generate the raw key bits R_A and R_B, respectively. Alice and Bob's projective measurements are represented by the quantum maps $\mathcal{E}_{R_A}$ and $\mathcal{E}_{R_B}$ such that the state $\rho_{R_A R_B E}$ reads:

$$\begin{aligned}\rho_{R_A R_B E} &= (\mathcal{E}_{R_A} \otimes \mathcal{E}_{R_B} \otimes \mathrm{id}_E)|\phi_{ABE}\rangle\langle\phi_{ABE}| \\ &= \sum_{a,b=0}^{1} (P_{|a\rangle} \otimes P_{|b\rangle} \otimes \mathrm{id}_E)|\phi_{ABE}\rangle\langle\phi_{ABE}|(P_{|a\rangle} \otimes P_{|b\rangle} \otimes \mathrm{id}_E), \end{aligned} \tag{3.10}$$

where $P_{|a\rangle} = |a\rangle\langle a|$ and similarly $P_{|b\rangle}$ are rank-one projectors on the Z basis, i.e. $|a\rangle, |b\rangle \in \{|0\rangle, |1\rangle\}$. We remark that we restricted without loss of generality to collective attacks where $|\phi_{ABE}\rangle$ represents the global state in a generic round of the protocol.

We start the key rate computation by assuming without loss of generality (w.l.o.g.) that, before distributing the state ρ_{AB} to the parties, Eve applies to it the maps $\mathcal{D}_1$ and $\mathcal{D}_2$, defined by:

$$\mathcal{D}_i(\rho_{AB}) = \frac{1}{2}\rho_{AB} + \frac{1}{2} D_i \rho_{AB} D_i^\dagger \qquad i = 1, 2, \tag{3.11}$$

where the operators D_i read:

$$D_1 = X \otimes X \quad ; \quad D_2 = Z \otimes Z. \tag{3.12}$$

One can easily verify that the resulting state $\tilde{\rho}_{AB}$ received by Alice and Bob:

$$\begin{aligned}\tilde{\rho}_{AB} = (\mathcal{D}_1 \circ \mathcal{D}_2)\,\rho_{AB} = \frac{1}{4}[&\rho_{AB} + (Z \otimes Z)\rho_{AB}(Z \otimes Z) \\ &+(X \otimes X)\rho_{AB}(X \otimes X) + (Y \otimes Y)\rho_{AB}(Y \otimes Y)]\end{aligned} \tag{3.13}$$

is diagonal in the Bell basis $\{|\psi_{ij}\rangle\}_{i,j=0}^{1}$ of two qubits, with the same diagonal coefficients of the original state ρ_{AB}. We can thus express $\tilde{\rho}_{AB}$ in the Bell basis as:

$$\tilde{\rho}_{AB} = \sum_{i,j=0}^{1} \lambda_{ij} |\psi_{ij}\rangle\langle\psi_{ij}| \tag{3.14}$$

for some eigenvalues $0 \le \lambda_{ij} \le 1$ such that $\sum_{i,j} \lambda_{ij} = 1$, where the Bell basis states read:

$$|\psi_{ij}\rangle = \frac{|0, j\rangle + (-1)^i |1, 1-j\rangle}{\sqrt{2}}, \qquad i, j \in \{0, 1\}. \tag{3.15}$$

The assumption that Alice and Bob are given the Bell-diagonal state (3.14) is not restrictive due to two reasons. First, since the state $\tilde{\rho}_{AB}$ is prepared by Eve, she also holds its purification and one can show that her uncertainty on Alice's key is not increased when she distributes $\tilde{\rho}_{AB}$ in place of ρ_{AB}: $H(R_A|E)_\rho \geq H(R_A|E)_{\tilde{\rho}}$. The interested reader can find the proof of this fact in appendix A.1. The second reason is that from the point of view of the parties, the action of $\mathcal{D}_1 \circ \mathcal{D}_2$ corresponds to a simultaneous flip of both Alice's and Bob's bits, which occurs with probability 1/2. This implies that both the marginal distributions of Alice's and Bob's raw key bits are symmetrized. However, the observed QBERs are unaffected[4] as well as the correlation of the raw keys of Alice and Bob. Therefore, the only visible effect is the symmetrization of the marginals. This could be directly enforced by the parties by agreeing on flipping their outcomes with probability 1/2, while communicating over the public channel. Thus Eve would be aware of the flipping.

For the above arguments, Eve distributes w.l.o.g. the state (3.14) to Alice and Bob.

Recall the definitions of the QBERs E_Z and E_X in terms of probabilities: The QBER E_Z (E_X) is the probability that the Z (X) measurement outcomes of Alice and Bob differ. Given that the parties share the state $\tilde{\rho}_{AB}$ in (3.14), it holds:

$$E_Z = \mathrm{Tr}[(P_{|0\rangle} \otimes P_{|1\rangle} + P_{|1\rangle} \otimes P_{|0\rangle})\tilde{\rho}_{AB}] = \lambda_{01} + \lambda_{11} \tag{3.16}$$

$$E_X = \mathrm{Tr}[(P_{|+\rangle} \otimes P_{|-\rangle} + P_{|-\rangle} \otimes P_{|+\rangle})\tilde{\rho}_{AB}] = \lambda_{10} + \lambda_{11}. \tag{3.17}$$

Moreover, Eve holds the purifying system of $\tilde{\rho}_{AB}$ such that the global pure state reads:

$$|\phi_{ABE}\rangle = \sum_{i,j=0}^{1} \sqrt{\lambda_{ij}}\, |\psi_{ij}\rangle_{AB} \otimes |e_{ij}\rangle_E\,, \tag{3.18}$$

where $\{|e_{ij}\rangle\}_{i,j=0}^{1}$ is an orthonormal basis in $\mathcal{H}_E$.

In order to compute the conditional entropy $H(R_A|E)$, we express it as follows:

$$H(R_A|E) = H(E|R_A) + H(R_A) - H(E). \tag{3.19}$$

The first term is computed on the state ρ_{R_AE} derived from (3.10) by tracing out Bob's subsystem:

$$\begin{aligned}
\rho_{R_AE} &= \sum_{a=0}^{1} |a\rangle\langle a|_{R_A} \otimes \mathrm{Tr}_{AB}\left[(|a\rangle\langle a| \otimes \mathrm{id}_{BE})|\phi_{ABE}\rangle\langle\phi_{ABE}|\right] \\
&= \sum_{a=0}^{1} |a\rangle\langle a|_{R_A} \otimes \sum_{i,j,k,l=0}^{1} \sqrt{\lambda_{ij}\lambda_{kl}}\, \mathrm{Tr}_{AB}\left[(|a\rangle\langle a| \otimes \mathrm{id}_B)|\psi_{ij}\rangle\langle\psi_{kl}|\right] |e_{ij}\rangle\langle e_{kl}|_E \\
&=: \sum_{a=0}^{1} \Pr(a)\, |a\rangle\langle a|_{R_A} \otimes \rho_E^a,
\end{aligned} \tag{3.20}$$

[4] This is due to the fact that either both Alice's and Bob's bits are flipped, or none is.

where the probability of Alice observing outcome a is $\Pr(a) = 1/2$ due to the symmetrized distribution of R_A, whereas Eve's state ρ_E^a, conditioned on Alice observing a, simplifies to:

$$\rho_E^a = \sum_{i,j,k=0}^{1} \sqrt{\lambda_{ij}\lambda_{kj}}\,(-1)^{(i+k)a}\,|e_{ij}\rangle\langle e_{kj}|. \tag{3.21}$$

The non-zero eigenvalues of (3.21) are independent of a and given by: $\{\lambda_{00} + \lambda_{10}, \lambda_{01} + \lambda_{11}\}$. By recalling the expression (2.49) of the conditional entropy of a c.q. state, we can compute the first term in (3.19) as follows:

$$H(E|R_A) = \sum_{a=0}^{1} \Pr(a) H(\rho_E^a) = H(\{\lambda_{00} + \lambda_{10}, \lambda_{01} + \lambda_{11}\}) = h(E_Z), \tag{3.22}$$

where we used the binary entropy $h(p)$ expression (2.43) and the fact that the coefficients λ_{ij} sum to one. Symmetrized marginals imply that $H(R_A) = 1$ and since the state on ABE is pure, the entropies of the subsystems E and AB are equal: $H(E) = H(AB) = H(\{\lambda_{ij}\})$. Substituting everything in (3.19) we obtain:

$$H(R_A|E) = 1 + h(E_Z) - H(\{\lambda_{ij}\}). \tag{3.23}$$

Note that the eigenvalues $\{\lambda_{ij}\}$ are not completely fixed by the observed error rates E_Z and E_X through (3.16) and (3.17). Thus we must consider the worst-case scenario and minimize (3.23) over $\{\lambda_{ij}\}$, with the constraints given by (3.16) and (3.17). The minimization leads to the following result [Sca+09]:

$$H(R_A|E) = 1 + h(E_Z) - (h(E_X) + h(E_Z)) = 1 - h(E_X). \tag{3.24}$$

We remark that we could minimize $H(R_A|E)$ independently of $H(R_A|R_B)$ since the latter is fixed by the QBER E_Z. Indeed, the conditional Shannon entropy $H(R_A|R_B)$ is computed on the probability distribution $\Pr(a, b)$ of Alice and Bob's Z outcomes. Due to the symmetrization of the marginals, it is easy to express the entropy exclusively in terms of E_Z as follows:

$$H(R_A|R_B) = h(E_Z). \tag{3.25}$$

By employing (3.24) and (3.25) in (3.9), we obtain the asymptotic key rate of the BB84 protocol in terms of the observed error rates:

$$r_{\mathrm{BB84}} = 1 - h(E_X) - h(E_Z). \tag{3.26}$$

3.3 Finite-key Security

The asymptotic secret key rate given in (3.9) is only valid in the limit of infinitely many protocol rounds. Here, we generalize that result by presenting the secret key length achieved by a general QKD protocol with finite resources and prove its security. In doing so, we mainly follow the reference [Tom+12].

3.3.1 General QKD Protocol

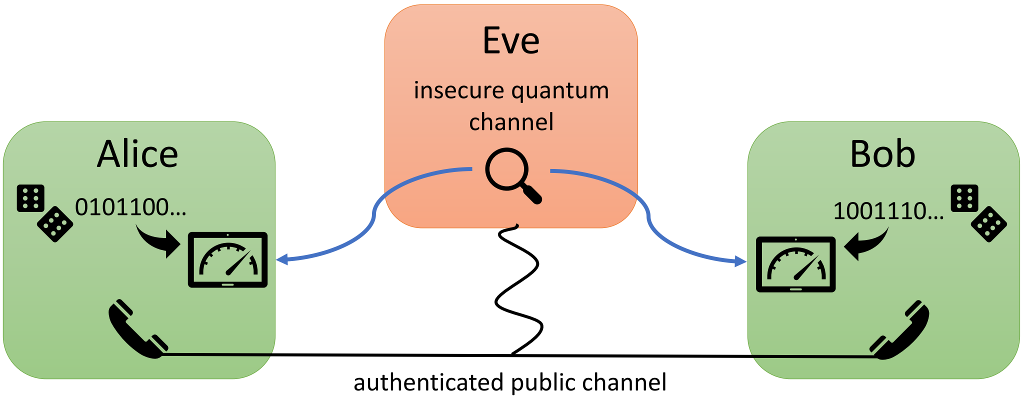

Fig. 3.1.: Schematic representation of the setup of an entanglement-based QKD protocol. In each round, Eve distributes a quantum signal to Alice and Bob through the quantum channel. Alice and Bob locally measure the incoming signal with a randomly-chosen measurement setting and record the classical output. After the transmission of quantum signals is over, the parties communicate via the classical public channel to perform error correction and privacy amplification.

Consider two parties, Alice and Bob, who have access to fresh randomness and are linked by an insecure quantum channel and an authenticated classical public channel (see figure 3.1). A potential eavesdropper, Eve, is assumed to have full control over the quantum channel and access to the messages sent via the public channel.

The parties run a QKD protocol, whose goal is to output a pair of identical keys (s_A, s_B) for Alice and Bob, respectively, completely unknown to Eve. The protocol could also abort and output the symbol: $s_A = s_B = \perp$. We describe the general QKD protocol in the entanglement-based view.

1. The protocol starts with the distribution of M quantum signals through the quantum channel. The joint state of the signals is represented by ρ_{AB}^{M} and Eve holds its purifying system (we allow for coherent attacks). Alice and Bob perform local measurements on each signal received and collect the classical

outcomes. Depending on the protocol, Alice and Bob can randomly choose among certain measurement settings. Typically, one setting is chosen with higher probability and is used for key generation, while the other(s) form the test rounds.

2. In PE, the parties reveal the settings and the outcomes of the test rounds, as well as the outcomes of a random sample of key-generation rounds. This information is used to estimate the noise in the quantum channel (and thus Eve's knowledge). If the noise is above a certain threshold, the protocol aborts.

3. At this point, both Alice and Bob hold a string of $n < M$ partially correlated key bits forming their raw key, denoted R_A^n and R_B^n, respectively. The parties perform an EC procedure in order for Bob to compute a guess $\hat{R_A^n}$ of Alice's raw key. In doing so, they reveal $\mathrm{leak}_{\mathrm{EC}}$ bits of information over the public channel. In order to verify if EC was successful, Alice computes a hash h_A (bitstring) of length $\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil$ from her raw key R_A^n by applying a two-universal hash function[5] [CW79; Ren08]. She publicly announces the function and h_A. Bob uses the same function to compute the hash h_B from his guess $\hat{R_A^n}$. If $h_A \neq h_B$, the protocol aborts. The total amount of information about Alice's raw key R_A^n revealed during EC is thus given by: $\mathrm{leak}_{\mathrm{EC}} + \lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil \leq \mathrm{leak}_{\mathrm{EC}} + \log(2/\varepsilon_{\mathrm{EC}})$.

4. In PA, Alice and Bob both apply the same two-universal hash function to their error-corrected keys R_A^n and $\hat{R_A^n}$ and obtain shorter, secret keys s_A and s_B of length ℓ. The final key length ℓ is chosen such that:

$$\ell \leq H_{\min}^{\varepsilon}(R_A^n|E) - \mathrm{leak}_{\mathrm{EC}} - \log \frac{2}{\varepsilon_{\mathrm{EC}}} - 2 \log \frac{1}{2\,\varepsilon_{\mathrm{PA}}}, \tag{3.27}$$

for some $\varepsilon, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{PA}} > 0$ which depend on the required level of security (see below). Intuitively, the length of the secret key cannot be larger than Eve's uncertainty on Alice's raw key (quantified by the min-entropy term) from which we subtracted the information revealed during EC.

The (non-asymptotic) secret key rate of the described protocol is given by:

$$r = \tau \frac{\ell}{M}, \tag{3.28}$$

where τ is the repetition rate of the experimental setup, i.e. the inverse of the time needed to perform one round of the protocol (distribution of quantum signal and measurements). In this thesis we always consider $\tau = 1$.

[5] The probability that the outputs corresponding to two different inputs of a two-universal has function coincide, is smaller or equal than 2^{-l_o}, where l_o is the bit-length of the outputs.

Remark 3.1 (Min-entropy estimation). *We emphasize that the secret key length in* (3.27) *is valid for an arbitrary QKD protocol. However, the smooth min-entropy term appearing in its expression cannot be directly computed since Eve's action is unknown, i.e. the state $\rho^n_{R_A E}$ representing Alice's raw key and Eve's quantum side information is not known. Hence, the challenge of every QKD protocol is to estimate the min-entropy term in the tightest way possible, by relying on the observed data employed for PE.*

3.3.2 Security Definition and Proof

We now define what it means for a QKD protocol to be "secure" and subsequently prove the security of the general QKD protocol outlined above.

Definition 3.1 (Correctness). *A QKD protocol is said to be ε_{cor}-correct if:*

$$\Pr[s_A \neq s_B] \leq \varepsilon_{\text{cor}}. \tag{3.29}$$

Definition 3.2 (Secrecy). *A QKD protocol is said to be ε_{sec}-secret if, for Ω being the event that the protocol does not abort,*

$$\Pr[\Omega]\frac{1}{2}\left\|\rho_{S_A E_{\text{tot}}|\Omega} - \omega_{S_A} \otimes \rho_{E_{\text{tot}}}\right\| \leq \varepsilon_{\text{sec}}, \tag{3.30}$$

where $\rho_{S_A E_{\text{tot}}|\Omega}$ is the state that describes the correlation between Alice's final secret key S_A and the total information available to Eve E_{tot} given that the protocol did not abort, while $\omega_{S_A} = \frac{1}{|S|}\sum_{s_i \in S}|s_i\rangle\langle s_i|$ is the maximally mixed state over all the possible realizations of Alice's key s_A.

The correctness definition implies that the protocol always outputs identical keys for Alice and Bob, except for probability at most ε_{cor}. The secrecy statement guarantees that Alice's key s_A is drawn randomly from the the set S of all possible keys and Eve has no information about it, or the protocol aborted, except for probability ε_{sec}.

The secrecy of Alice's key s_A alone does not guarantee that even Bob's key s_B is secret, unless we combine it with a statement on the correctness of the protocol. Therefore we define the security of a QKD protocol as follows.

Definition 3.3 (Security). *A QKD protocol is said to be ε_{tot}-secure if it is ε_{cor}-correct and ε_{sec}-secret, with $\varepsilon_{\text{tot}} \geq \varepsilon_{\text{cor}} + \varepsilon_{\text{sec}}$.*

Note that a trivial protocol that always aborts and outputs $s_A = s_B = \perp$ is secure according to the above definitions. Thus, another important feature of a QKD protocol is its *completeness*, i.e. the existence of an honest implementation of the protocol such that the probability of not aborting is $\Pr[\Omega] \geq 1 - \varepsilon_c$, for some small ε_c.

We also remark that the Defs. 3.1, 3.2 and 3.3 are *composable*. This means that when a QKD protocol –proven secure according to these definitions– is composed with another cryptographic task, the security of their combination can be inferred based on their individual security proofs and does not require a separate new proof. This is particularly relevant for QKD, which is often composed with one-time pads as seen in section 3.1.

Lemma 3.1 (Security of QKD). *The general QKD protocol of subsection 3.3.1 is $\varepsilon_{\mathrm{tot}}$-secure, with $\varepsilon_{\mathrm{tot}} \geq \varepsilon_{\mathrm{EC}} + \varepsilon + \varepsilon_{\mathrm{PA}}$.*

In order to prove this statement, one first shows that the general QKD protocol described earlier is $\varepsilon_{\mathrm{EC}}$-correct. This is guaranteed by the fact that Alice and Bob verify the success of EC by computing and comparing hashes of length $\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil$. The second step is to show that the protocol is at least $(\varepsilon + \varepsilon_{\mathrm{PA}})$-secret by employing the quantum leftover hash lemma [Ren08; Tom+11b], which is at the core of finite-key QKD security. We provide the full proof of Lemma 3.1 in appendix A.2.

3.3.3 Reduction to Asymptotic Key Rate

We emphasize that the non-asymptotic secret key rate in (3.28), computed with the key length in (3.27) of a generic QKD protocol, reduces to the asymptotic key rate given in (3.9) in the limit $M \to \infty$ of infinitely many rounds. This fact shows that the results presented in this section properly generalize QKD key rates to the scenario of finite resources.

In order to prove the reduction of (3.28) to (3.9), we make use of an important tool called the *postselection technique* (PST) [CKR09], valid for discrete-variable QKD protocols where the dimension $d = \dim(\mathcal{H}_A \otimes \mathcal{H}_B)$ of the quantum systems held by Alice and Bob can be characterized. The PST states that if a QKD protocol of M rounds is $\varepsilon_{\mathrm{tot}}$-secure against collective attacks, then it is also $(M+1)^{d^2-1}\varepsilon_{\mathrm{tot}}$-secure against coherent attacks if the secret key length (3.27) (the output of PA) is shortened by $2(d^2-1)\log(M+1)$ bits.

Recall that in case of collective attacks, the state shared by the parties in the M rounds is the i.i.d. state $\rho_{AB}^{\otimes M}$, while for coherent attacks –as we consider in this finite-key analysis– the shared state is the more general ρ_{AB}^{M}.

Since in the asymptotic limit ($M \to \infty$, and $\varepsilon_{\mathrm{tot}} \to 0$ exponentially fast) the corrections to the secret key rate introduced by the PST are negligible, proving the security of a generic QKD protocol against coherent attacks reduces to proving the security of the same protocol against collective attacks [Ren07; Sca+09; CKR09]. In other words, we can assume without loss of generality that the state distributed to the parties by Eve is an i.i.d. state $\rho_{AB}^{\otimes M}$. As a consequence, the smooth min-entropy term in (3.27) is now computed on the state $\rho_{R_A E}^{\otimes n}$: $H_{\min}^{\varepsilon}(R_A^n|E)_{\rho_{R_A E}^{\otimes n}}$.

Moreover, by recalling the operational meaning of the smooth max-entropy (c.f. section 2.6), the minimum amount of leakage in (3.27) is quantified by $\mathrm{leak}_{\mathrm{EC}} \approx H_{\max}^{\varepsilon'}(R_A^n|R_B^n)$, where we neglected terms that tend to zero in the asymptotic limit. In case of collective attacks, the smooth-max entropy is evaluated on the i.i.d. state $\rho_{R_A R_B}^{\otimes n}$ and reads: $H_{\max}^{\varepsilon'}(R_A^n|R_B^n)_{\rho_{R_A R_B}^{\otimes n}}$.

Finally, by applying the AEP (2.62) and (2.63) on the smooth entropy terms appearing in (3.27), we reduce them to the correspondent von Neumann entropies: $H(R_A|E)$ and $H(R_A|R_B)$. In this way (3.9) is recovered.

Note that the PST has been fundamental for the application of the AEP, since the latter only holds for i.i.d. quantum states.

3.4 Quantum Conference Key Agreement

The rapid development of quantum technologies allows us to foresee quantum networks [EKB16a; EKB16b; PWD18; HPE19] as one of its near-future applications. Quantum networks could be composed of matter-based quantum nodes where quantum information can be processed and stored, linked together by quantum channels where light distributes entangled states. Successful experiments on matter-latter entanglement [Kru+19; Tch+19] bring us closer to realizing such networks. The ultimate vision for quantum networks is building the quantum internet [Kim08; WEH18].

A more accessible application of quantum networks is the generalization of the task of QKD to a multiparty scenario, in what is called multipartite QKD or quantum conference key agreement (CKA). Here, N parties in a quantum network wish to establish a common secret key –a conference key– and use it to securely broadcast messages within the network. We recently produced the first complete review on this topic [Mur+20], which can be found in appendix G.

A CKA could be carried out by simply performing bipartite QKD schemes between pairs of parties, and then employing the established keys to securely distribute the conference key to all involved parties. However, such a solution would not exploit the possibility offered by quantum networks of distributing multipartite entangled states across several network nodes.

Conversely, it is possible to devise CKA protocols which make use of the correlations arising in multipartite entangled states in order to establish a conference key among several users [Wu+16; Epp+17; ZSG18; GKB18; GKB19; CP19]. This type of truly multipartite schemes can outperform the solution based on the iteration of bipartite schemes in certain network configurations (e.g. networks with bottlenecks) [Epp+17] and noise regimes [RMW19]. It is worth mentioning that the conference key rates achievable in a given network configuration are upper bounded by recently-derived fundamental limits, which depend on the network topology [Pir19a; Das+19; Pir19b; Tak+19].

We emphasize that CKA based on multipartite entanglement is one of the main research topics of this thesis. In the remainder of this section we outline the path that led to the development of the first (discrete-variable) CKA protocols [Epp+17; GKB18], where the second one is a result of our doctoral research and is reported in appendix B.

3.4.1 Multipartite BB84 Protocol

Consider a scenario where Alice and $N-1$ Bobs, denoted B_1, B_2 up to B_{N-1}, want to establish a secret conference key with a generalization of the BB84 protocol presented in section 3.2. In this multipartite scenario, the conference key is extracted from Alice's raw key, hence during EC every Bob attempts to correct his raw key to match Alice's. As a consequence, even in CKA protocols the main quantity to be estimated is the smooth min-entropy $H_{\min}^{\varepsilon}(R_A^n|E)$ of Alice's raw key conditioned on Eve's information (see Remark 3.1).

A naive approach to generalize the BB84 protocol would be to reproduce its prepare-and-measure description, where Alice now sends a state $|\phi_k\rangle$ $(k = 1, \dots, 4)$ out of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to every Bob ($|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$). This means that in each round of the protocol the product state $|\phi_k\rangle^{\otimes(N-1)}$ is sent through the quantum channel. Since Eve is in control of the whole quantum channel, she can attempt to distinguish the four product states $|\phi_k\rangle^{\otimes(N-1)}$, whose overlap (scalar product) is either 0 or $(1/\sqrt{2})^{N-1}$. As N increases, the four states become more distinguishable thus allowing Eve to retrieve more information about the key without being noticed. This leads to a dramatic decrease of the secret key rate and eventually makes the protocol useless, even assuming a flawless implementation.

The described CKA does not rely on entangled states (as the original BB84 protocol) and has actually been investigated for $N = 3$ in [Mat07]. However, the idea is clearly not scalable to larger numbers of parties.

In order to devise a generalization of the BB84 protocol which would work with an arbitrary number of parties, we resort to its entanglement-based description. In the ideal implementation of the BB84 protocol, Alice and Bob measure their qubit in either the Z or X basis and obtain perfectly correlated and random outcomes since their qubits have been prepared in the Bell state given in (3.7). Typically, the outcomes of the Z basis are used for key generation and those of the X basis are used to estimate the noise E_X in the channel and thus Eve's knowledge.

In generalizing this idea to $N \geq 3$ parties we encounter a fundamental problem. The only N-qubit state which leads to perfectly correlated and random outcomes in one measurement basis –necessary condition for generating a shared key– is the N-party GHZ state:

$$|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle^{\otimes N} + |1\rangle^{\otimes N} \right], \tag{3.31}$$

when measured in the Z basis. However, the authors in [Epp+17] prove that even bipartite perfect correlations are forbidden in any other basis, contrary to what happens with the Bell state (3.7) for $N = 2$.

Therefore, in an ideal N-party BB84 protocol Alice and the Bobs share an N-party GHZ state and measure in the Z basis for key generation. However, they cannot estimate the channel's noise by a pairwise comparison of the X outcomes (or any other basis), since they would be uncorrelated even in the ideal scenario. How can we still estimate Eve's knowledge in the multipartite scenario?

Recall that the goal is to find a lower bound on the min-entropy $H^{\varepsilon}_{\min}(R^n_A|E)$ in the secret key length (3.27), or, in the asymptotic scenario, a bound on the von Neumann entropy $H(R_A|E)$ of the asymptotic secret key rate (3.9).

One possible solution is provided in [Epp+17] for the asymptotic scenario. It basically consists in requiring the parties to measure their qubit in one of three bases, namely the X, Y or Z basis. In doing so, the parties can sufficiently characterize the state $\rho_{R_A E}$ describing Alice's raw key and Eve's quantum side information, to the extent that $H(R_A|E)$ is completely fixed by the measurement statistics. This solution can be interpreted as the N-party generalization of the six-state QKD protocol [Bru98], where Alice and Bob are required to measure in the same three bases.

Alternatively, the security of a multipartite QKD scheme based on the GHZ state can also be ensured with just two measurement bases, making the protocol a multipartite version of the BB84 protocol. We introduce such a scheme in our work [GKB18], which can also be found in appendix B.

The main idea is to view all the Bobs as one single Bob and define E_X as the error rate between the X outcomes of Alice (X_A) and the product of the X outcomes of all Bobs ($X_{\Pi B} := \prod_{i=1}^{N-1} X_{B_i}$): $E_X = \Pr[X_A \neq X_{\Pi B}]$. Indeed, in an ideal implementation where the parties share the GHZ state (3.31), X_A and $X_{\Pi B}$ are perfectly correlated like in the bipartite scenario and the channel noise would be zero: $E_X = 0$.

In [GKB18] we directly bound the min-entropy term $H^{\varepsilon}_{\min}(Z^n_A|E)$ as a function of E_X, where we emphasized the fact that the raw keys are obtained from Z-basis measurements. This is possible thanks to the *uncertainty relation for smooth entropies* [TR11]. The uncertainty relation states that, given the state $\rho^n_{AB_1\dots B_{N-1}E}$ of the n rounds yielding the raw keys and assuming that Alice measures her n qubits in either the Z or X basis, it holds:

$$H^{\varepsilon}_{\min}(Z^n_A|E) \geq q - H^{\varepsilon}_{\max}(X^n_A|B_1 \dots B_{N-1}), \tag{3.32}$$

where X^n_A represents the outcomes Alice would obtain had she measured the n raw-key rounds in the X basis. The term q is the quality factor of the two measurements of Alice (see [TR11] for a formal definition). In our case, since Alice measures each qubit either in the Z or X basis, it reads: $q = n$. Thanks to the data-processing inequality (2.65), we can lower bound the r.h.s. of (3.32) by letting every Bob measure his qubit in the X basis and by multiplying the outcomes:

$$H^{\varepsilon}_{\min}(Z^n_A|E) \geq n - H^{\varepsilon}_{\max}(X^n_A|X^n_{\Pi B}). \tag{3.33}$$

Finally we remark that the max-entropy on the r.h.s. of the last expression can always be upper-bounded by (n times) the binary entropy of the error rate E_X affecting the strings X^n_A and $X^n_{\Pi B}$, with a correction Δ due to statistical fluctuations (which also depends on n):

$$H^{\varepsilon}_{\max}(X^n_A|X^n_{\Pi B}) \leq n\, h(E_X + \Delta). \tag{3.34}$$

One can interpret the inequality (3.34) as the finite version of the equality (3.25) linking the conditional von Neumann entropy of two random variables to their error probability. In conclusion we obtain:

$$H^{\varepsilon}_{\min}(Z^n_A|E) \geq n(1 - h(E_X + \Delta)). \tag{3.35}$$

An important aspect in any CKA is the information leakage during EC. As anticipated, in our protocol we require every Bob to correct his raw key to match Alice's. By employing one-way EC, Alice needs to publicly broadcast enough information such that even the Bob with the largest amount of errors can correct his key. Since the information leak_i she would send to each B_i only depends on the estimated Z-basis error rate E_{AB_i} but otherwise it's independent of B_i, by broadcasting $\max_i \mathrm{leak}_i$ we ensure that every Bob will be able to correct his raw key. In other words, the leakage of one-way EC in a multipartite QKD protocol is equivalent to that of a bipartite protocol performed with the worst-case Bob.

In [GKB18] we prove the finite-key security of both the novel multipartite BB84 protocol and the multipartite six-state protocol of [Epp+17], by introducing security definitions analogous to those presented in section 3.3. We also compare the performance of the two protocols.

The asymptotic secret key rate of the N-partite BB84 protocol can be heuristically inferred starting from the secret key length of a bipartite QKD protocol in (3.27). We use Eq. (3.35) to bound the min-entropy term, while we replace the leakage term with $\max_i \mathrm{leak}_i$ according to the argument above. Analogously to section 3.3.3, we estimate the minimum leakage relative to B_i as $\mathrm{leak}_i \approx H^{\varepsilon'}_{\max}(R^n_A|R^n_{B_i})$ and bound the max-entropy with a version of the bound (3.34) where the relevant error rate is the Z-basis error rate E_{AB_i}. Finally, by taking the limit $M \to \infty$ we remove all the corrections due to statistical fluctuations and obtain:

$$r_{N\text{-BB84}} = 1 - h(E_X) - \max_{1 \leq i \leq N-1} h(E_{AB_i}). \tag{3.36}$$

Notably, the resulting key rate reads exactly like the BB84 one in (3.26), except for a maximization on the QBERs in the Z basis and a more general definition of E_X.

Remark 3.2 (Entanglement is necessary). *We emphasize that both multiparty QKD protocols discussed in this section require the generation of entangled states even in their prepare-and-measure version, opposed to the bipartite BB84 protocol where Alice sends simple qubits to Bob. Indeed, in the entanglement-based view of the two multipartite QKD protocols, the parties are given the N-partite GHZ state* (3.31). *Now note that the conditional state of the Bobs, given that Alice measured X on the GHZ state and obtained outcome a, reads:*

$$|\psi_a\rangle_{B_1 \dots B_{N-1}} = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes(N-1)} + (-1)^a |1\rangle^{\otimes(N-1)}\right), \tag{3.37}$$

which is an entangled state. Therefore, in an equivalent prepare-and-measure version of the protocol, Alice would need to prepare the entangled state (3.37) *and send it to the Bobs in the rounds where she chooses the X basis. However, the X-basis rounds are test rounds and are much less frequent than the key-generation rounds. In the key-generation rounds the conditional state of the Bobs, upon Alice measuring Z, is given by one of the two product states $|0\rangle^{\otimes(N-1)}$ and $|1\rangle^{\otimes(N-1)}$. Hence for key generation Alice can just prepare the same qubit state $N-1$ times and send each of them to the corresponding Bob.*

3.5 State-of-the-art Experiments

Before continuing our theoretical analysis of QKD schemes, we provide a brief and incomplete overview of the most recent experimental achievements involving QKD and CKA. More complete and elaborated reviews can be found in [Sca+09; Dia+16; Pir+19].

In October 1989 Bennett, Brassard and other scientists implemented for the first time a QKD protocol, specifically a version of the BB84 protocol [BB89; Ben+92]. The experiment was carried out in a laboratory and was characterized by the transmission of polarized light over (just) $32.5\,\mathrm{cm}$.

Since then much progress has been made, also thanks to the interest and investments of governments and companies [Com; Tec]. Current QKD implementations can reach secret key rates of the order of $\mathrm{Mbit\,s^{-1}}$ over about $50\,\mathrm{km}$ of telecom fiber [Dix+08; Pat+14; Hua+15]. Moreover, QKD has also successfully undergone field tests on commercial telecom fibers [Zha+19b] in view of its implementation in existing urban networks.

Thanks to novel architectures and security proofs, it has been possible to extend the longest achieved distance of QKD to over $400\,\mathrm{km}$ using optical fibers [Yin+16; Boa+18; Wan+19; Liu+19].

In 2017, Chinese and Japanese research groups independently realized the first QKD protocols in free-space using low-Earth-orbit satellites. In particular, the Chinese group led by Prof. Pan implemented QKD over $1000\mathrm{km}$ with satellite-to-ground links [Lia+17; Tak+17], including a quantum-secured video call between Beijing and Vienna [Lia+18].

The experimental implementations listed so far involve just two parties establishing a secure key. Recently, thanks to the collaboration with the EMQL research group led by Prof. Fedrizzi in Edinburgh, we performed the first experimental demonstration of a four-party CKA protocol [Pro+20] (appendix F). The experiment implements the multiparty BB84 protocol [GKB18] mentioned in the previous section and presented in appendix B. It is characterized by the generation of polarization-encoded GHZ states at telecom wavelength and by their distribution to the four parties over up to a total of $50\,\mathrm{km}$ of optical fibers.

4 Quantum Key Distribution with Imperfect Devices

The unconditional security which is, in principle, promised by QKD, is undermined by the difficulty of ensuring that the assumptions on its implementation (quantum sources or measurement devices) are met in practice.

In this chapter we outline some of the experimental flaws that allow a potential eavesdropper to successfully breach the security of a QKD protocol. We then focus on the solutions to such problems, which are given by a combination of theoretical advances and clever experimental design. In particular, in sections 4.1 and 4.2 we discuss how security can be proven when the BB84 protocol is implemented with weak coherent pulses instead of single-photon sources. We then introduce measurement-device-independent QKD in section 4.3 and consider a practical implementation of it in section 4.4.

4.1 BB84 with Weak Coherent Pulses

The majority of the sources used in QKD experiments are highly attenuated lasers producing weak coherent pulses (WCPs), whose state is of the form:

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,, \tag{4.1}$$

where $|n\rangle$ is called a *Fock state* and represents n identical photons, while $|\alpha|^2$ is the intensity of the pulse and represents the average number of photon in the pulse. Indeed, the probability of finding n photons in the coherent state (4.1) follows a Poisson distribution and is given by:

$$\Pr(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}. \tag{4.2}$$

Clearly the number of photons in a WCP is not well defined, opposed to the assumption made in the previous chapter of Alice sending a single photon to Bob in each round of the protocol. The multiphoton signals allow Eve to perform new eavesdropping attacks which severely compromise security, like the photon number splitting attack (PNS) [Hut+95; Bra+00]. Here Eve blocks all single-photon signals and splits one photon off each multiphoton signal, allowing the remaining photons to reach Bob. In this way, she has a copy of what Bob receives without being noticed, thus compromising the security of those protocols not accounting for multiphoton signals.

From the above example, we learn that only the single-photon signals emitted by Alice are still secure. The security proof by Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [Got+04] states that a BB84 protocol implemented with WCPs is still secure, provided that one extracts the key only from single-photon signals. The resulting asymptotic secret key rate, for an asymmetric BB84 protocol where the Z basis is used for key generation and the X basis for PE, reads [LMC05; Wei+13]:

$$r_{\mathrm{GLLP}} = p_Z^2 \left[Q_Z^0 + Q_Z^1 (1 - h(e_X^1)) - Q_Z h(E_Z) \right], \tag{4.3}$$

where p_Z is the probability that Alice (Bob) chooses the Z basis (asymptotically it can be chosen $p_Z \to 1$). In the GLLP rate (4.3), we recognize the contribution coming from the estimation of Eve's uncertainty from single-photon signals $Q_Z^0 + Q_Z^1(1-h(e_X^1))$ from which we subtract the information leaked during error correction (EC) $Q_Z h(E_Z)$, similarly to the asymptotic BB84 rate in (3.26). In particular, Q_Z^n $(n = 0, 1)$ is the probability that Alice sent n photons in the Z basis and Bob had a detection event, while Q_Z is the *gain* in the Z basis, i.e. the probability that Bob had a detection given that Alice sent a WCP in that basis. Analogous quantities are defined for the X basis. We have that:

$$Q_{Z(X)} = \sum_{n=0}^{\infty} Q_{Z(X)}^n. \tag{4.4}$$

We note that $Q_Z^0 = Q_X^0 = Q^0$ is independent of the basis, since in this case Bob's detection is caused by dark counts or stray light in his detectors. Hence, the data Bob collected in these instances is secure and added to Eve's uncertainty, as there is no way for Eve to know it.

Finally $E_{Z(X)}$ is the QBER in the Z (X) basis given that Bob had a detection, and $e_{Z(X)}^n$ is the error rate in the Z (X) basis given that Alice sent n photons and Bob had a detection. It thus holds:

$$E_{Z(X)} Q_{Z(X)} = \sum_{n=0}^{\infty} Q_{Z(X)}^n e_{Z(X)}^n. \tag{4.5}$$

In a real experiment, the observed quantities are the gains Q_Z, Q_X and the QBERs E_Z, E_X, while p_Z is an input parameter and Q^0, Q_Z^1 and e_X^1 must be estimated. In particular, one can lower bound the achievable key rate (4.3) by upper bounding

e_X^1 and by lower bounding Q^0 and Q_Z^1. The decoy-state method [Hwa03; Wan05; LMC05] provides an excellent way to obtain such bounds, thus guaranteeing high key rates for QKD protocols implemented with WCPs.

4.2 Decoy-state Method

We start by requiring Alice to prepare and send a phase-randomized WCP in each round, whose state is a mixture of Fock states:

$$\rho_\mu = \frac{1}{2\pi}\int_0^{2\pi} \mathrm{d}\theta \, |\sqrt{\mu}e^{\mathrm{i}\theta}\rangle\langle\sqrt{\mu}e^{\mathrm{i}\theta}| = \sum_{n=0}^{\infty} e^{-\mu}\frac{\mu^n}{n!}|n\rangle\langle n|. \tag{4.6}$$

This can be viewed as Alice preparing one of the Fock states $|n\rangle\langle n|$ according to a Poisson distribution like (4.2) with mean photon number μ. Thus the probability of Alice sending exactly n photons in the Z (X) basis and Bob having a detection, $Q^n_{Z(X)}$, is given by:

$$Q^n_{Z(X)} = e^{-\mu}\frac{\mu^n}{n!}Y^n_{Z(X)}, \tag{4.7}$$

where the n-photon *yield* $Y^n_{Z(X)}$ is the conditional probability that Bob had a detection, given that Alice sent n photons. Again, while the intensity μ of the WCP is an input parameter, the yields are not directly observable.

According to the decoy-state method [Hwa03; Wan05; LMC05], Alice will intersperse her states ρ_μ used for key generation –called signal states– with decoy states ρ_{μ_i} with the same characteristics of the signal states except for their intensity, which is randomly drawn from a set $\{\mu_i\}_i$ (typically $\mu_i \leq \mu$). This can be achieved with intensity modulators such as variable optical modulators (VOAs). In doing so, the parties observe the gains $Q^{\mu_i}_{Z(X)}$ and QBERs $E^{\mu_i}_{Z(X)}$.

The central idea is that, from Eve's viewpoint, in every round a Fock state $|n\rangle\langle n|$ is picked according to a probability distribution that is unknown to her and sent through the quantum channel. In other words, Eve cannot distinguish a signal state from a decoy state. This means that Eve's action can only depend on the photon number and on the basis (e.g. photon polarization), but not on the probability distribution that generated the photons.

Therefore the yields $Y^n_{Z(X)}$ and the error rates $e^n_{Z(X)}$, which are a reflection of Eve's action on the quantum channel, are independent of the intensity determining the photons' distribution. This fact allows us to derive a set of linear constraints on the yields and error rates, in terms of the observed gains Q_Z, Q_X and QBERs E_Z, E_X. Indeed, by combining (4.7) with (4.4) and (4.5), we obtain:

$$Q_Z^{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_Z^n \quad , \quad \mu_i \in \{\mu_i\}_i \tag{4.8}$$

$$Q_X^{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_X^n \quad , \quad \mu_i \in \{\mu_i\}_i \tag{4.9}$$

$$E_X^{\mu_i} Q_X^{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} Y_X^n e_X^n \quad , \quad \mu_i \in \{\mu_i\}_i . \tag{4.10}$$

Every equality above represents a system of equations determined by different decoy intensities μ_i. The larger the number of decoy intensities, the more constrained are the yields and error rates. By combining the different equations in a system with Gaussian elimination techniques, one can derive bounds on the yields and error rates of interest in terms of the observed gains and QBERs. Importantly, since the employed decoy intensities are typically small (e.g. $\mu_i \sim 0.1$), the higher order terms in each sum can be crudely approximated without heavily affecting the bounds. Moreover, we remark that already two decoy intensities are enough to find good bounds [Wan05; Wei+13; Lim+14] and that recently it was shown that the BB84 protocol can also be implemented with just one decoy intensity setting [Rus+18].

From the first set of equations (4.8) one derives lower bounds $Y^{0\downarrow}$ and $Y_Z^{1\downarrow}$ which correspond to lower bounds on the quantities Q^0 and Q_Z^1 appearing in the key rate (4.3). From the second set (4.9), one derives bounds on the yields that are then employed in the third set (4.10) to derive the upper bound $e_X^{1\uparrow}$.

Let us briefly sum up the implementation of the asymmetric BB84 protocol with the integration of the decoy-state method. Alice prepares phase-randomized WCPs polarized in the Z (X) basis with probability p_Z $(1-p_Z)$. Upon choosing the Z basis, she modulates the pulse intensity to μ with probability q to generate a signal state, or to one of the decoy intensities $\{\mu_i\}$ to generate a decoy state with probability $1-q$. If Alice picks the X basis instead, she only generates decoy states. Bob chooses to measure the incoming pulse in the Z (X) basis with probability p_Z $(1-p_Z)$.

At the end of the transmission, Alice reveals the intensity setting and the basis she used in every round. Bob instead reveals all the X outcomes to estimate $E_X^{\mu_i}$ and some of the Z outcomes of the signal state to estimate E_Z^{μ}.

The asymptotic secret key rate of an asymmetric BB84 protocol with decoy states is obtained with the GLLP analysis and reads [Wei+13]:

$$r_{\text{decoy}} \geq p_Z^2 q \left[Q^{0\downarrow} + Q_Z^{1\downarrow}(1-h(e_X^{1\uparrow})) - Q_Z^{\mu} h(E_Z^{\mu}) \right] , \tag{4.11}$$

where Q^{μ}_Z and E^{μ}_Z are the gain and QBER of the signal state, while $Q^{0\downarrow}$ ($Q^{1\downarrow}_Z$) is a lower bound on the probability that Alice sent 0 (1) photon and Bob had a detection event, given that Alice sent a signal state: $Q^0 = e^{-\mu}Y^{0\downarrow}$ and $Q^{1\downarrow}_Z = e^{-\mu}\mu Y^{1\downarrow}_Z$.

Finally, we mention that the key rate could be optimized by using the decoy-state rounds in the Z basis even for key generation [Lim+14].

4.3 Introduction to Measurement-device-independent QKD

The security proof of the general QKD protocol presented in section 3.3 is based on the assumption that the measurement devices held by the parties are trusted, while the source of quantum states can be untrusted. Indeed, we assume that Eve distributes uncharacterised quantum states, on which the parties perform characterised measurements[1] (e.g. in the Z or X basis). All the information that Eve can gain on the measurement outcomes comes from her quantum side information E (apart from the information leaked in the classical public channel).

However, measurement detectors can suffer from imperfections causing them to operate differently from their theoretical models used to prove security. Eve could exploit such imperfections to launch powerful eavesdropping attacks [Zha+08; Lyd+10; Ger+11] that go under the name of *detector side channels*. An example is the *detector blinding attack* [Lyd+10], where Eve first sends bright light to Bob's single-photon detectors to "blind" them and make them operate in linear-mode. This means that his detectors are now unable to detect single photons and produce a click only above a certain intensity threshold. Eve then sends tailored light pulses to Bob which yield a click only when Bob chooses the same basis in which Eve prepared the pulse. Hence Eve knows the outcome of each detection observed by Bob, without introducing noticeable disturbance.

Measurement-device-independent QKD (MDI-QKD) [LCQ12; Xu+15] provides a solution which removes all possible detector side channels with a new QKD paradigm. Here, the honest parties send quantum signals to an intermediate relay which applies some measurement and publicly announces the outcome. The founding idea is to remove all trust from the measurement apparatus, which can be operated by Eve, and place it on the sources, held by Alice and Bob. Typically, QKD sources are attenuated lasers which can be easily characterized in a controlled environment represented by Alice's and Bob's laboratory. Note that this scenario is opposite to the previous one, where the source was untrusted and the measurement devices were trusted.

[1] Note that specifying the measurement operators of a party effectively fixes the dimension of the quantum system on which they are performed.

Despite the fact that Eve has potentially full control on the relay and on the connecting quantum channels, Alice and Bob can still establish a secret key. This is possible if the measurement outcome publicly announced by the relay, in an honest implementation, is informative for Alice and Bob but is not informative –i.e. it does not reveal information on the key– for anyone else, including Eve.

To make things more concrete, let us consider an idealized MDI-QKD protocol [Pir+19] where Alice and Bob independently encode their bits in the rectilinear or diagonal polarization of single-photon states, represented by the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ (with $|\pm\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$), respectively. The quantum signals are then sent to the relay. Here a Bell-state measurement, i.e. a projection on one of the four Bell states $|\psi_{ij}\rangle$ given in (3.15), is applied on the incoming signals and its outcome (i, j) is announced. Upon sifting, Alice and Bob are only left with bits corresponding to rounds in which they used the same basis. If both parties used the rectilinear basis, the outcomes $(i, 0)$ (for $i = 0, 1$) inform them that their bit values coincide, while the outcomes $(i, 1)$ indicate that they encoded opposite bit values. Similarly, if Alice and Bob used the diagonal basis, the outcomes $(0, j)$ indicate they have same bit values while $(1, j)$ indicate opposite bit values. Bob can thus flip his bit according to the measurement outcome and recover Alice's bit.

In simple terms, the outcome of the Bell-state measurement reveals the parity of the parties' bits but not their values. Therefore, it provides useful information only if one of the two bit values is known (i.e. to Alice and Bob), while being useless otherwise.

Of course, Eve could implement any other operation on the incoming pulses but she is still required to announce an outcome of the form (i, j) at every round. Thus, by comparing a fraction of their sifted bits, Alice and Bob can verify the deviation of the actual measurement apparatus from the ideal one and quantify the amount of information gained by Eve.

4.4 Practical Measurement-device-independent QKD

The first practical version of an MDI-QKD protocol was introduced by Lo and co-workers in [LCQ12] with a fully optical setup. The single-photon pulses are replaced by phase-randomized WCPs in combination with the decoy-state method to guarantee security, while the Bell-state measurement is implemented using linear optics. Unfortunately, with linear optics only two out of four Bell-state projectors can be realized. This, however, does not undermine security as it only introduces some inconclusive measurement outcomes, which reduce the key rate. The protocol's setup is reported in figure 4.1.

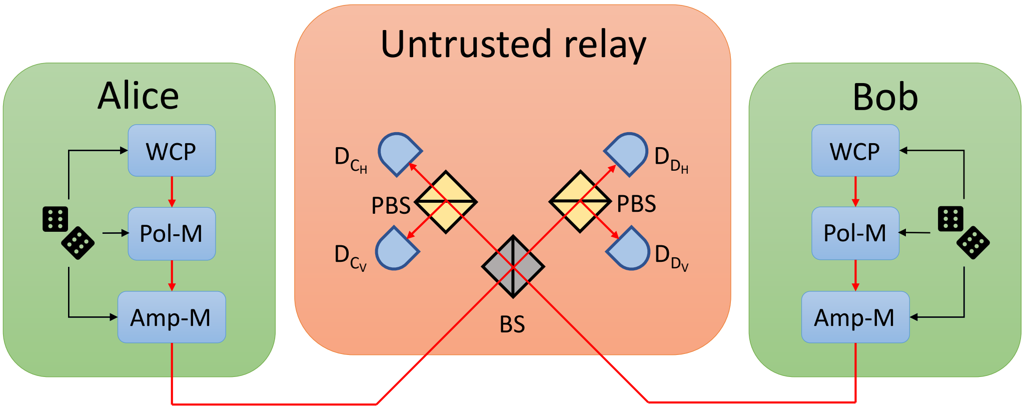

Fig. 4.1.: Schematic setup of the MDI-QKD protocol in [LCQ12]. Each party prepares a phase-randomized weak coherent pulse (WCP). With a polarization modulator (Pol-M), the party encodes a random bit in the polarization of the pulse. The intensity of the pulse is attenuated with an amplitude modulator (Amp-M) to implement the decoy state method. The parties send their pulses to the central relay, which in principle applies a 50:50 beam splitter (BS) followed by two polarizing beam splitters (PBS) at each output port, which project the incoming pulses on the horizontal or vertical polarization states. The resulting pulses are detected by four single-photon detectors ($D_{C_H}, D_{C_V}, D_{D_H}, D_{D_V}$). The detection pattern is publicly revealed.

In every round of the protocol, Alice (Bob) prepares a phase-randomized WCP. Upon randomly selecting the rectilinear (horizontal, vertical) or diagonal ($45°$, $-45°$) polarization basis, Alice (Bob) encodes a random bit in the polarization state of the pulse with a polarization modulator. The amplitude of the pulse is randomly tuned through an amplitude modulator, generating signal or decoy states. The two pulses are then sent to the central relay where they interfere at a 50:50 beam splitter (BS). At each output port of the BS, a polarizing beam splitter (PBS) projects the incoming pulses onto the horizontal (H) or vertical (V) polarization states, which are then detected by the corresponding single-photon detectors (SPDs): D_{C_H}, D_{D_H} (horizontal) and D_{C_V}, D_{D_V} (vertical). The outcome of the detections is publicly announced.

The click of exactly two detectors corresponding to orthogonal polarizations indicates a successful Bell-state measurement. In particular if D_{C_H}, D_{C_V} or D_{D_H}, D_{D_V} clicked, the pulses have been projected on the Bell state $|\psi_{01}\rangle$. If a click occurs in D_{C_H}, D_{D_V} or D_{D_H}, D_{C_V}, the projection is on the Bell state $|\psi_{11}\rangle$. All other detection events are inconclusive and the corresponding bits get discarded. The parties also discard the bits for which they used different bases. Bob flips all his remaining bits, except for those generated in rounds where he selected the diagonal basis and the pulses were projected on $|\psi_{01}\rangle$.

In order to grasp how the optical setup depicted in figure 4.1 corresponds to a Bell-state measurement, we imagine a virtual scenario where the state preparation goes as follows. We assume for simplicity that the parties can prepare single-photon states. Alice (and similarly Bob) prepares an entangled state between a virtual qubit she (he) holds and a single photon polarized either horizontally or vertically:

$$|\Phi_A^+\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle_A |1\rangle_{A_H} + |V\rangle_A |1\rangle_{A_V}\Big] = \Big[|H\rangle_A\, a_H^\dagger + |V\rangle_A\, a_V^\dagger\Big]\, |0\rangle \tag{4.12}$$

$$|\Phi_B^+\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle_B |1\rangle_{B_H} + |V\rangle_B |1\rangle_{B_V}\Big] = \Big[|H\rangle_B\, b_H^\dagger + |V\rangle_B\, b_V^\dagger\Big]\, |0\rangle\,. \tag{4.13}$$

The kets $|H\rangle_A\,, |V\rangle_A$ define the qubit's computational basis (Z basis) indicating the polarization state the single photon, while the Fock states $|1\rangle_{A_H}\,, |1\rangle_{A_V}$ describe a single photon polarized horizontally or vertically, and can be expressed in terms of the corresponding creation operators $a_H^\dagger, a_V^\dagger$ acting on the vacuum $|0\rangle$. Analogous definitions hold for Bob's state.

If now Alice (Bob) measures the virtual qubit in the Z or X basis, this is equivalent to Alice (Bob) preparing the single-photon in a random polarization state of the corresponding basis, which is the protocol's state preparation described above. However, since Alice and Bob's operations on their qubits commute with the detection at the relay, they can delay their qubit measurements until the photon detection has occurred.

Therefore, after preparing the entangled states (4.12) and (4.13), the parties send their photons to the relay. The global quantum state before the photons enter the 50:50 BS reads:

$$|\Phi_A^+\rangle \otimes |\Phi_B^+\rangle = \\ \frac{1}{2}\Big[|HH\rangle_{AB}\, a_H^\dagger b_H^\dagger + |HV\rangle_{AB}\, a_H^\dagger b_V^\dagger + |VH\rangle_{AB}\, a_V^\dagger b_H^\dagger + |VV\rangle_{AB}\, a_V^\dagger b_V^\dagger\Big]\, |0\rangle\,. \tag{4.14}$$

At the BS, every photon has a 50% chance of being transmitted or being reflected. By labelling $c^\dagger$ ($d^\dagger$) the creation operator of the photons exiting the BS from the left (right) output port (c.f. figure 4.1), the unitary action of the BS can be summarized as follows:

$$a^\dagger \mapsto \frac{c^\dagger + d^\dagger}{\sqrt{2}} \tag{4.15}$$

$$b^\dagger \mapsto \frac{c^\dagger - d^\dagger}{\sqrt{2}}\,. \tag{4.16}$$

By inserting the relations (4.15) and (4.16) in the state (4.14) and by using the fact that creation operators relative to different optical paths or different polarization states commute, we obtain the following global state at the exit of the BS:

$$
\begin{aligned}
&|\Phi_{BS}\rangle = \\
&\frac{1}{2}\left[|\psi_{01}\rangle_{AB}\left(\frac{|1\rangle_{C_H}|1\rangle_{C_V} - |1\rangle_{D_H}|1\rangle_{D_V}}{\sqrt{2}}\right) - |\psi_{11}\rangle_{AB}\left(\frac{|1\rangle_{C_H}|1\rangle_{D_V} - |1\rangle_{C_V}|1\rangle_{D_H}}{\sqrt{2}}\right)\right. \\
&\left. + |HH\rangle_{AB}\left(\frac{|2\rangle_{C_H} - |2\rangle_{D_H}}{2}\right) + |VV\rangle_{AB}\left(\frac{|2\rangle_{C_V} - |2\rangle_{D_V}}{2}\right)\right]. \qquad (4.17)
\end{aligned}
$$

In the last expression $|\psi_{01}\rangle_{AB}$ and $|\psi_{11}\rangle_{AB}$ are Bell states written in the computational basis $\{|H\rangle, |V\rangle\}$, so for example $|\psi_{01}\rangle_{AB} = (|HV\rangle + |VH\rangle)/\sqrt{2}$, and e.g. $|1\rangle_{C_H}, |2\rangle_{C_H}$ are the Fock states of one and two photons polarized horizontally in the left output port of the BS.

From (4.17) we immediately deduce that if the detectors D_{C_H}, D_{C_V} or D_{D_H}, D_{D_V} click, then the qubits have been projected on the Bell state $|\psi_{01}\rangle_{AB}$. If the clicks occur in D_{C_H}, D_{D_V} or D_{C_V}, D_{D_H}, the qubits are projected on $|\psi_{11}\rangle_{AB}$. Since the qubits indicate the polarization state of the photons, this confirms that the optical setup performs the mentioned Bell state measurement. Moreover, we observe that even in an ideal scenario (single-photons and no losses), this implementation of a Bell state measurement cannot succeed with probability higher than $1/2$, thus reducing the key rate.

Note that the click of only one detector would reveal the polarization of both photons (in absence of losses), hence this event cannot be used for MDI-QKD. The same thing would happen if both detectors D_{C_H}, D_{D_H} or D_{C_V}, D_{D_V} clicked. However, this event cannot happen (c.f. (4.17)) due to the *Hong-Ou-Mandel (HOM) effect*. The HOM effect occurs when two identical photons (like Alice's and Bob's photons when prepared with the same polarization) enter the input ports of a 50:50 BS. Due to the unitary nature of the BS, the two photons always exit the same output port of the BS. If the HOM interference would not occur, the possible detection patterns at the relay would increase, making the Bell state measurement less likely and thus harming the key rate.

Consequently, preparing indistinguishable photons from independent light sources and obtaining good HOM interference is an important requirement for a successful implementation of the described protocol. For this, the authors in [LCQ12] also show that such a requirement can be fulfilled with current technology.

The virtual qubit approach also plays a fundamental role in proving the security of the MDI-QKD protocol here presented. Indeed, in the virtual scenario and after the photon detection has occurred, the protocol can be interpreted as an entanglement-based BB84 protocol where Alice and Bob are given a pair of qubits in an entangled state, which ideally is either $|\psi_{01}\rangle$ or $|\psi_{11}\rangle$. The parties then independently measure their qubit in the Z or X basis and compute the QBERs. In this way, one can prove the security of the MDI scheme by relying on the security proof of the BB84 protocol with WCPs [Got+04; LCQ12] (c.f. section 4.1). Note that in this case the secure bits generated by the MDI-QKD protocol are those where both Alice and Bob sent a single photon to the relay. Moreover, a detection event is successful only when exactly two detectors clicked in the combinations described above.

The authors in [LCQ12] provide the asymptotic secret key rate achieved by their MDI-QKD protocol. They consider a version of the protocol where the rectilinear basis is used for key generation and the diagonal basis (selected in a small fraction of rounds) is used for estimating Eve's knowledge (PE). The resulting secret key rate reads:

$$r_{\text{MDI}} = Q^{1,1}_{\text{rect}}(1 - h(e^{1,1}_{\text{diag}})) - Q_{\text{rect}} h(E_{\text{rect}}), \tag{4.18}$$

where Q_{rect} and E_{rect} are the gain and QBER of the signal state in the rectilinear basis. That is, Q_{rect} is the probability of a successful detection given that both Alice and Bob sent a signal state in the rectilinear basis. Instead, $Q^{1,1}_{\text{rect}}$ is the probability that both parties sent one photon and the relay had a successful detection, given that they both prepared a signal state in the rectilinear basis. Finally $e^{1,1}_{\text{diag}}$ is the error rate in the diagonal basis given that Alice and Bob sent one photon each and the detection was successful.

As expected, the secret key rate in (4.18) resembles the one in (4.11) of an asymmetric BB84 protocol with decoy states. Similarly to that case, the quantities $Q^{1,1}_{\text{rect}}$ and $e^{1,1}_{\text{diag}}$ can be bounded with the decoy state method presented in the previous section.

5 Beyond Point-to-point Quantum Key Distribution

By definition, point-to-point QKD protocols are implemented with a single quantum channel which directly connects the two parties establishing the key, e.g. the BB84 protocol introduced in chapter 3.

In this chapter we present the recently-derived theoretical limits on the secret key rate that can be extracted by any point-to-point QKD protocol (section 5.1). Subsequently, we present in detail the (arguably) simplest solution found by researchers to overcome such limitations, which is twin-field (TF) QKD (sections 5.2 and 5.3). This is followed by a detailed investigation of the performance of TF-QKD in realistic conditions (section 5.4), based on our works in appendices C and D. In section 5.5 we describe the generalization of the TF-QKD idea to more parties which is at the core of our work reported in appendix E.

5.1 Fundamental Limits of Point-to-point QKD

The secret key rate of any QKD protocol is limited by the losses that inevitably occur in the quantum channel(s) linking the end users. In most QKD implementations, the information is encoded in one of the degrees of freedom of photons. The photons are then transmitted over lossy quantum channels, whose *transmittance* η represents the probability that a photon is successfully transmitted. For instance, the optical attenuation in standard telecom fibers is about $\gamma = 0.2\,\mathrm{dB\,km^{-1}}$, which leads to an overall loss of γL over L kilometers of fiber. The transmittance of an L-kilometer telecom fiber is thus given by: $\eta = 10^{-\gamma L/10}$. This shows that the probability of a photon being transmitted decreases exponentially with the length of the channel, thus severely affecting the key rate.

The exact relation between the key rate and the channel transmittance depends on the protocol. Nevertheless, researchers have recently derived fundamental bounds [TGW14; Pir+17] on the secret key rate of any *point-to-point* QKD protocol, which only depend on the channel transmittance η. In particular, the secret key rate of any QKD protocol performed over a lossy channel of transmittance η is upper bounded by the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [Pir+17]:

$$r_{\mathrm{PLOB}} = -\log(1-\eta), \tag{5.1}$$

where the logarithm is intended in base 2, as usual. In the high-loss regime ($\eta \ll 1$), we can expand the logarithm in (5.1):

$$r_{\mathrm{PLOB}} \approx 1.44\,\eta, \tag{5.2}$$

and observe that the key rate cannot scale better than linearly with the transmittance of the channel, thus decreasing exponentially with the channel length.

The only way to overcome such severe limitations on the achievable key rate is to employ one or more intermediate nodes in the quantum channel connecting the users. However, this fact alone is not sufficient in general to yield key rates with an improved scaling compared to the PLOB bound.

Consider for instance the MDI-QKD protocol presented in the section 4. Despite featuring an intermediate measuring station that splits the channel between Alice and Bob of transmittance η in two channels of transmittance $\sqrt{\eta}$ each[1], the key rate does not scale better than the PLOB bound. Indeed, in order to have a successful detection, both photons sent by Alice and Bob need to arrive at the central relay, which occurs with probability $\sqrt{\eta} \cdot \sqrt{\eta} = \eta$. Thus, the gain and hence the key rate cannot scale better than linearly with the transmittance η of the whole channel.

A possible solution is instead represented by quantum repeaters [Bri+98; San+11], which guarantee a polynomial scaling of the communication efficiency with the distance. However, such devices are still very challenging to implement as they require either quantum memories [San+11; Dua+01; Maz+14] or quantum error correction [Mun+12; ATL15].

Other viable options are evolutions of the original MDI-QKD scheme, like memory-assisted MDI-QKD featuring quantum memories [Pan+14; AKB14] or adaptive MDI-QKD with quantum non-demolition measurements [ATM15]. In both cases, the protocol adapts to the photon losses ensuring that the Bell-state measurement is performed between pulses from Alice and Bob that actually arrived, even combining pulses sent in different rounds. In this way, only one photon per round is required to arrive, thus yielding a key rate proportional to $\sqrt{\eta}$. Despite the square-root improvement in the key rate scaling, the evolved MDI schemes still rely on two-photon interference events and their implementation is far from being practical.

In the next section we introduce a novel QKD protocol which represents the simplest solution, found so far, to improve the key rate scaling of QKD beyond the PLOB bound and to reach further distances.

[1] Each channel has length $L/2$, if L is the total channel length between Alice and Bob. The transmittance of each channel is thus $e^{-\gamma L/(2\cdot 10)} = \sqrt{\eta}$.

5.2 Twin-field QKD: Original Protocol

In 2018, Lucamarini et al. [Luc+18] proposed a new QKD scheme which is based on the same working principle of MDI-QKD: a central untrusted relay measures the pulses sent by Alice and Bob. The measurement outcome reveals the parity of Alice and Bob's bits, but not their values. However, opposed to MDI-QKD, it is based on *single-photon* interference events. Thanks to this feature, it naturally retains the square-root improvement in the key rate scaling since the successful events are exactly those where only one photon arrived, sent either from Alice or Bob. This removes the necessity of sophisticated systems to adapt the Bell-state measurements to photon losses.

The protocol in [Luc+18] takes the name of twin-field (TF) QKD and its original formulation goes as follows. Alice (Bob) generates phase-randomized WCPs by picking a random phase value ρ_a (ρ_b) in the interval $[0, 2\pi)$. The phase interval is split into M phase slices $\Delta_k = 2\pi k/M$ $(k = 0, \dots, M-1)$ and the selected random phase necessarily falls into one of them: $\Delta_{k(a)}$ $(\Delta_{k(b)})$. Alice (Bob) then encodes a secret bit and a secret basis in another phase φ_a (φ_b) which is added to the phase of the pulse. The pulses are then sent to a central station where they are combined in a 50:50 beam splitter with single-photon detectors at its output ports. After the detection outcome is announced, the parties publicly reveal the slices $\Delta_{k(a)}, \Delta_{k(b)}$ and the encoded bases, and keep only the rounds with matching values. Indeed, the optical fields whose random phase falls in the same slice are "twins" and can be used to generate a secret key. The detection outcome combined with the revealed information indicate to Bob whether he needs to flip his bit or not, in order to match it with Alice's.

Since the first TF-QKD protocol has been published, an intense research activity led to several variants of the original scheme [CAL19; Cui+19; LL18; MZZ18; WYH18] and to many experimental demonstrations [Wan+19; Liu+19; Zho+19; Min+19]. In particular, experimentalists managed to obtain secret key rates surpassing the limit imposed by the PLOB bound, thus proving the improved scaling of TF-QKD.

In the following, we are going to focus on the TF-QKD protocol proposed by Curty et al. [CAL19], which is simpler and arguably better-performing than many other TF-QKD variants. Before moving on, we briefly mention a couple of drawbacks of the original TF scheme in [Luc+18].

Firstly, the random phases of a pair of twin fields are not identical and differ by less than $2\pi/M$. This induces an intrinsic QBER that tends to zero for $M \to \infty$. However, the probability of having matching slices scales as $1/M$, thus increasing M leads to more discarded rounds. There exists an optimal value for M that can be determined by appropriately modelling the experimental setup and optimizing the key rate. The authors in [Luc+18] obtained an optimal value of $M_{\mathrm{opt}} = 16$. In any case, the use of locally randomized phases by Alice and Bob and the post-selection of the matching ones causes a consistent amount of rounds to be discarded.

The main challenge in implementing the TF-QKD protocol of [Luc+18] is controlling the phase drifts of the twin fields. Indeed, the differential phase fluctuation between the two signals sent by Alice and Bob can be quantified as follows:

$$\delta_{ab} = \frac{2\pi}{c_f} \left(\Delta\nu L + \nu \Delta L \right), \tag{5.3}$$

where c_f is the speed of light in the fiber, while $\Delta\nu$ is the frequency difference between the users' lasers and ΔL is the difference of path lengths travelled by the two signals. While $\Delta\nu$ can be compensated with phase-locking techniques already used in optical communications, the contribution due to ΔL is a more serious drawback. Indeed, even if the two fibers have nominally the same length, the distance travelled by each signal can fluctuate in time due for instance to thermal expansions of the fibers, resulting in a phase drift at the output of the fiber. This issue could be mitigated with active stabilization techniques.

5.3 Twin-field QKD without Phase Post-selection

The TF-QKD protocol introduced in [CAL19] removes the need to post-select matching global phases ρ_a and ρ_b for Alice and Bob, thus sensibly increasing the protocol's performance. It instead relies on a preselected global phase shared by Alice and Bob. We remark that a very similar scheme has been independently developed in [Cui+19], but it is equipped with an alternative security proof.

5.3.1 Idealized Protocol

In order to elucidate the protocol's functioning, we start by presenting an idealized version of it, which also has the merit to show where the inspiration came from, namely entanglement-generation protocols in quantum repeaters.

The idealized TF-QKD protocol in [CAL19] is composed of the following steps.

1. Alice (and analogously Bob) prepares an optical signal entangled with a qubit she holds:

$$|\Phi\rangle_{Aa} = \sqrt{q}\,|0\rangle_A\,|0\rangle_a + \sqrt{1-q}\,|1\rangle_A\,|1\rangle_a \qquad 0 \leq q \leq 1, \tag{5.4}$$

where $|0\rangle_a, |1\rangle_a$ are the Fock states of the photon representing the vacuum and a single-photon state, while $\{|0\rangle_A, |1\rangle_A\}$ is the qubit's computational basis (Z basis).

2. Both parties send their optical pulses to a central relay through optical channels, each with transmittance $\sqrt{\eta}$ (the overall transmittance between Alice and Bob is η).

3. The central relay applies a 50:50 beam splitter to the incoming pulses followed by two threshold detectors D_c and D_d (i.e. unable to distinguish the detection of one or more photons).

4. The relay broadcasts the outcomes k_c and k_d of detector D_c and D_d, where $k_c = 0$ and $k_c = 1$ ($k_d = 0$ and $k_d = 1$) correspond to a no-click and a click event, respectively.

5. With probability p_X Alice (Bob) measures her (his) qubit in the X basis given by $\{|\pm\rangle_{A(B)} = (|0\rangle_{A(B)} \pm |1\rangle_{A(B)})/\sqrt{2}\}$, while with probability $1 - p_X$ she (he) measures the qubit in the Z basis. Upon obtaining the outcome x, where $x = \pm 1$ are the eigenvalues of the X and Z operators, Alice (Bob) records the bit value b_A (b_B) with $(-1)^{b_A} = x$ ($(-1)^{b_B} = x$).

6. The bits b_A and $b_B \oplus k_d$, collected by Alice and Bob in the rounds where they measured in the X basis and where the relay announced $k_c \oplus k_d = 1$ (i.e. only one detector clicked), form their raw keys. The bits collected in the Z-basis rounds where $k_c \oplus k_d = 1$ are instead used for PE. All the other rounds are discarded.

To understand why the protocol enables the parties to distil a secret key, imagine that we choose $1 - q \ll 1$ in the state preparation. This means that both parties prepare their signals strongly unbalanced towards the vacuum. For this reason, in the relevant events where only one detector clicked, the detection is likely to be caused by the sending and arrival of just one photon coming from either Alice or Bob. However, the beam splitter creates a coherent superposition of these two possibilities, implying that either Alice's or Bob's qubit are in state $|1\rangle$, but not both of them. The conditional state of the parties' qubits is thus well approximated by the Bell states: $|\psi_{k_d 1}\rangle_{AB} = (|01\rangle + (-1)^{k_d} |10\rangle)/\sqrt{2}$ ($k_d = 0, 1$). The parties then measure their respective qubit in either the X or Z basis. From here, the protocol can be regarded as an entanglement-based BB84 protocol whose security we proved in the previous chapter. Any deviation from the described picture can be detected by computing appropriate error rates.

The states $|\psi_{k_d 1}\rangle$ prompt us to define the following error rates in the X and Z basis:

$$E_X = p_{XX}[b_A \neq b_B \oplus k_d | k_c \oplus k_d = 1] \tag{5.5}$$

$$E_Z = p_{ZZ}[b_A = b_B | k_c \oplus k_d = 1], \tag{5.6}$$

where $p_{XX(ZZ)}[\Omega]$ is the probability that the event Ω occurred given that both Alice and Bob measured in the X (Z) basis. The two error rates are zero if the parties share one of the Bell states $|\psi_{k_d 1}\rangle$.

According to the above explanation, ideally the relevant detections are caused by the sending and arrival of just one photon. This shows that the protocol is based on *single-photon interference* events, thus producing a key rate that scales with $\sqrt{\eta}$ (the transmittance of one of the two channels) as the original TF-QKD scheme.

We can support this statement with more analytical grounds, by first computing the conditional state of the parties' qubits, given that only detector D_c ($k_d = 0$) or only detector D_d ($k_d = 1$) clicked:

$$\begin{aligned}\rho_{AB}^{k_d} = &\frac{p_1}{p_{\text{click}}}\left[\frac{q}{q+(1-q)(1-\sqrt{\eta})}|\psi_{k_d 1}\rangle\langle\psi_{k_d 1}|_{AB}\right.\\ &\left.+\frac{(1-q)(1-\sqrt{\eta})}{q+(1-q)(1-\sqrt{\eta})}|11\rangle\langle 11|_{AB}\right] + \frac{p_2}{p_{\text{click}}}|11\rangle\langle 11|_{AB},\end{aligned} \tag{5.7}$$

where $p_{\text{click}} = p_1 + p_2$ is the probability that only detector D_c (D_d) clicked, while p_1 (p_2) corresponds to the event where the detection was caused by a single-photon (two-photon) pulse:

$$p_1 = \sqrt{\eta}(1-q)q + (1-q)^2\sqrt{\eta}(1-\sqrt{\eta}) \tag{5.8}$$

$$p_2 = \frac{1}{2}(1-q)^2\eta. \tag{5.9}$$

In (5.7) we recognize the contribution due to the Bell states $|\psi_{k_d 1}\rangle$, however we also have other spurious contributions which lead to intrinsic errors in the protocol. The resulting error rates, for the state (5.7), read:

$$2E_X = E_Z = \frac{p_1}{p_{\text{click}}}\frac{(1-q)(1-\sqrt{\eta})}{q+(1-q)(1-\sqrt{\eta})} + \frac{p_2}{p_{\text{click}}}. \tag{5.10}$$

The asymptotic secret key rate of the described protocol is simply given by the BB84 protocol key rate (3.26), rescaled by the probability $2p_{\text{click}}$ that a successful detection occurred. We thus get:

$$r_{\text{idealTF}} = 2p_{\text{click}}(1 - h(E_Z) - h(E_X)). \tag{5.11}$$

By optimizing the key rate over the input parameter q, one obtains an optimal value in the range: $q \in [0.88, 0.94]$ for every value of η. This increases the weight of the desired contribution $|\psi_{k_d 1}\rangle\langle\psi_{k_d 1}|_{AB}$ in the parties' shared state (5.7), as explained above.

The overall scaling of the key rate (5.11) with respect to η can be immediately visualized by neglecting the terms of second order in $(1-q)$ (which are small when q is optimized). In this approximation we have that $E_X \approx E_Z \approx 0$ and that $2p_{\text{click}} \approx 2q(1-q)\sqrt{\eta}$, hence the key rate scales with $\sqrt{\eta}$, as anticipated.

5.3.2 Actual Protocol

Here we present the actual TF-QKD protocol introduced in [CAL19], which is inspired by the idealized protocol above but it is much more practical to implement. First of all, note that the measurements performed by Alice and Bob commute with the operations of the relay. This means that the measurements in step 5 can be performed right after step 1, i.e. the parties can directly measure their qubit after generating the entangled state (5.4). In doing so, we turn the protocol into a prepare-and-measure scheme where Alice, upon choosing the X basis, prepares an optical pulse a in the state:

$$|X_{b_A}\rangle_a := \sqrt{q}\,|0\rangle_a + (-1)^{b_A}\sqrt{1-q}\,|1\rangle_a\,, \tag{5.12}$$

depending on the value of a bit b_A, chosen at random. Instead, when Alice chooses the Z basis, she prepares the pulse in the Fock state:

$$|Z_{b_A}\rangle := |b_A\rangle_a \tag{5.13}$$

where the vacuum $|0\rangle_a$ ($b_A = 0$) is selected with probability q and the single-photon state $|1\rangle_a$ ($b_A = 1$) is selected with probability $1-q$. Bob prepares his optical signal in analogous states. The other steps of the protocol remain unchanged.

We remark that this prepare-and-measure scheme is equivalent to the entanglement-based idealized protocol from the point of view of the security and achieved key rate. However, it does not require the generation of entanglement between a local qubit and an optical signal, which might be experimentally demanding. We now replace the states prepared in the current prepare-and-measure scheme with more practical ones, while leaving all the other protocol steps unchanged. In this way we come to the final TF-QKD protocol of [CAL19], which is summed up in figure 5.1.

The form of the states (5.12) prepared when the X basis is chosen, combined with the fact that the optimal value for q is close to one, suggest much more practical states to prepare an optical pulse in, namely coherent states $|(-1)^{b_A}\alpha\rangle$ of low intensity $|\alpha|^2$. Indeed, by recalling that a coherent state can be expressed as a superposition of Fock states (4.1), one notices that the states in (5.12) can be well approximated by the WCP:

$$X \text{ basis:} \quad |(-1)^{b_A}\alpha_A\rangle\,, \tag{5.14}$$

with an appropriate amplitude α_A and where b_A is a random bit. Bob prepares a coherent state analogous to (5.14) whose amplitude α_B can differ from Alice's.

The Z-basis states (5.13) are Fock states of fixed photon number. Thus, the corresponding error rate E_Z is linked to the probabilities that Alice and Bob send a certain number of photons to the relay and the detection is successful. We have seen (c.f. section 4.2) that such probabilities can be estimated by using the decoy-state method. Now, since the Z-basis rounds do not contribute to key generation, the states prepared in these rounds have the only purpose of quantifying E_Z. Therefore, we can replace them with the more practical phase-randomized WCPs, and estimate E_Z with the decoy-state method. Thus, upon choosing the Z basis, Alice prepares a phase-randomized WCP:

$$Z \text{ basis:} \quad \rho_{\mu_i} = \sum_{n=0}^{\infty} e^{-\mu_i}\frac{\mu_i^n}{n!}|n\rangle\langle n|, \tag{5.15}$$

whose intensity μ_i is randomly drawn from a set $\{\mu_i\}$. Analogously, Bob prepares a phase-randomized WCP ρ_{ν_i} with intensity ν_i randomly drawn from the set $\{\nu_i\}$. The two sets of intensities can be different for Alice and Bob.

Remark 5.1. *We stress the fact that the TF-QKD protocol of [CAL19], instead of requiring a global phase post-selection like the original TF-QKD scheme [Luc+18], requires a global phase pre-selection which fixes the phases of the coherent states in the X-basis rounds. This can be achieved if the parties share a phase-reference that can also be controlled by Eve. The feasibility of this solution was recently proved in some experiments [Wan+19; Liu+19; Min+19]. Conversely, in the Z-basis rounds the phase-reference is not needed as the parties prepare locally phase-randomized WCPs. This makes the TF-QKD protocol of [CAL19] quite robust against potential phase misalignments, since they only affect the X-basis rounds.*

5.3.3 Error Rates Estimation

When performing the practical TF-QKD protocol outlined above, the quantities that Alice and Bob observe, after revealing their inputs in a fraction of the rounds, are the gains $p_{XX}(k_c, k_d|b_A, b_B)$ and $p_{ZZ}(k_c, k_d|\mu_i, \nu_j)$. The former is the probability that the relay announces the detection pattern k_c, k_d given that Alice (Bob) prepared $|(-1)^{b_A}\alpha_A\rangle$ ($|(-1)^{b_B}\alpha_B\rangle$), while the latter is the probability that the relay announces the detection pattern k_c, k_d given that Alice (Bob) prepared ρ_{μ_i} (ρ_{ν_j}).

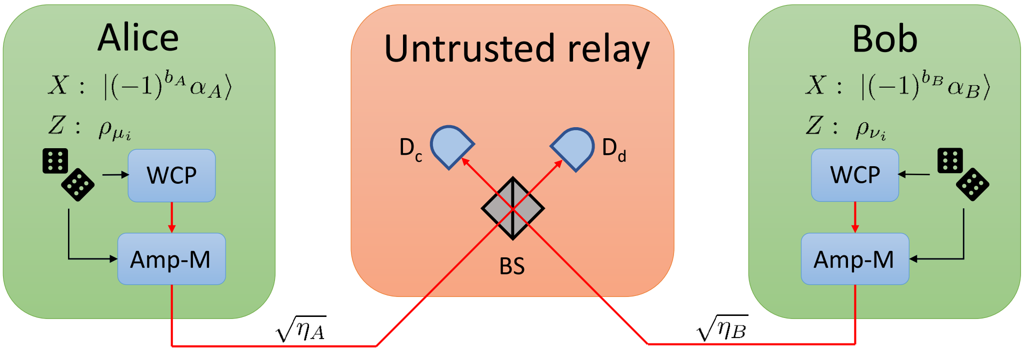

Fig. 5.1.: Schematic setup of the practical TF-QKD protocol introduced in [CAL19]. In every round, each party selects the X (Z) basis with probability p_X $(1-p_X)$. When selecting the X basis, Alice (Bob) prepares a WCP whose phase encodes her (his) random key bit b_A (b_B). When the Z basis is selected, she (he) prepares a phase-randomized WCP to implement the decoy state method. Both parties send their pulses to the central relay through channels of transmittance $\sqrt{\eta_A}$ for Alice and $\sqrt{\eta_B}$ for Bob. Here, the incoming pulses are combined into a 50:50 BS followed by two threshold detectors at its output ports. The relay announces the results of the detection k_c, k_d. The parties only keep those rounds in which they chose the same basis and $k_c \oplus k_d = 1$, all the other rounds are discarded. The bits b_A and $b_B \oplus k_d$ form the parties' raw keys.

From the observed gains, the parties can estimate the error rates E_X and E_Z as follows. In the following, we assume that the detection pattern k_c, k_d is such that $k_c \oplus k_d = 1$.

E_X estimation: From Bayes' theorem [SO94] we obtain:

$$p_{XX}(b_A, b_B|k_c, k_d) = \frac{1}{4}\frac{p_{XX}(k_c, k_d|b_A, b_B)}{p_{XX}(k_c, k_d)}, \tag{5.16}$$

where:

$$p_{XX}(k_c, k_d) = \frac{1}{4}\sum_{b_A, b_B=0}^{1} p_{XX}(k_c, k_d|b_A, b_B). \tag{5.17}$$

We can then compute the error rate E_X in (5.5), for the detection pattern k_c, k_d, as follows:

$$E_X^{k_c,k_d} = \sum_{j=0}^{1} p_{XX}(b_A = j, b_B = j \oplus k_c|k_c, k_d), \tag{5.18}$$

where the probabilities $p_{XX}(b_A, b_B|k_c, k_d)$ are given in (5.16).

E_Z estimation: What we want is an estimation of the error rate E_Z that characterizes the rounds where Alice and Bob chose the X basis. Suppose that, upon choosing the X basis, Alice (Bob) implements and entanglement-based version of the TF-QKD protocol, i.e. she (he) prepares the entangled state $|\Phi\rangle_{Aa}$ ($|\Phi\rangle_{Bb}$) defined as:

$$|\Phi\rangle_{Aa} = \frac{|+\rangle_A |\alpha_A\rangle_a + |-\rangle_A |-\alpha_A\rangle_a}{\sqrt{2}}, \tag{5.19}$$

and she (he) delays the X measurement on the qubit until the detection at the relay has occurred. Note that Eve cannot distinguish this scenario from the actual scenario in (5.14). The global state of the parties' qubits and signals, after the relay announced outcome k_c, k_d, reads:

$$|\chi^{k_c,k_d}\rangle_{Aa'Bb'} := \frac{M_{a,b}^{k_c,k_d} |\Phi\rangle_{Aa} |\Phi\rangle_{Bb}}{\sqrt{p_{XX}(k_c,k_d)}}, \tag{5.20}$$

where $M_{a,b}^{k_c,k_d}$ is the Kraus operator describing the action of the relay on the signals of Alice and Bob, corresponding to outcome k_c, k_d. The Z-basis error, as defined in (5.6), affecting the X-basis rounds is thus given by:

$$E_Z^{k_c,k_d} = \sum_{j=0}^{1} \left\| {}_{AB}\langle jj|\chi^{k_c,k_d}\rangle_{Aa'Bb'} \right\|^2 . \tag{5.21}$$

Now, one can derive an upper bound on (5.21) in terms of the yields $Y_{nm}^{k_c,k_d}$ in the Z basis, i.e. the probability that the relay announces k_c, k_d given that Alice and Bob sent n and m photons, respectively, after choosing the Z basis. The upper bound on E_Z reads [CAL19]:

$$\begin{aligned} \bar{E}_Z^{k_c,k_d} := \frac{1}{p_{XX}(k_c,k_d)} \Bigg[& \left(\sum_{n,m=0}^{\infty} c_{2n}^A c_{2m}^B \sqrt{Y_{2n\,2m}^{k_c,k_d}} \right)^2 \\ & + \left(\sum_{n,m=0}^{\infty} c_{2n+1}^A c_{2m+1}^B \sqrt{Y_{2n+1\,2m+1}^{k_c,k_d}} \right)^2 \Bigg], \end{aligned} \tag{5.22}$$

where $c_n^{A(B)}$ is defined as: $c_n^{A(B)} = e^{\frac{-\alpha_{A(B)}^2}{2}} \alpha_{A(B)}^n / \sqrt{n!}$. Then, the yields appearing in the bound (5.22) can be estimated with the decoy-state method, by relying on the gains observed in the Z basis: $p_{ZZ}(k_c, k_d|\mu_i, \nu_j)$. Specifically, the yields are constrained by the following set of equations, each corresponding to a particular pair of decoy intensities (μ_i, ν_j):

$$p_{ZZ}(k_c, k_d|\mu_i, \nu_j) = \sum_{n,m=0}^{\infty} e^{-\mu_i - \nu_j} \frac{\mu_i^n \nu_j^m}{n!\, m!} Y_{nm}^{k_c,k_d} \quad \mu_i \in \{\mu_i\}, \nu_j \in \{\nu_j\}, \tag{5.23}$$

similarly to what we have seen for the decoy-state method applied to the BB84 protocol (4.8). Note that in this case, differently from the usual decoy-state method, one needs to derive *upper* bounds on the yields in (5.22), which correspond to a lower bound on the key rate. Furthermore, typically one can only bound a subset of the infinite amount of yields appearing in (5.22), while the remaining yields are trivially upper bounded by one.

5.3.4 Secret Key Rate

The asymptotic secret key rate of the practical TF-QKD protocol introduced in [CAL19] is given by:

$$r_{\mathrm{TF}} \geq r_{\mathrm{TF}}^{1,0} + r_{\mathrm{TF}}^{0,1}, \tag{5.24}$$

where $r_{\mathrm{TF}}^{k_c,k_d}$ is the contribution due to the detection event k_c, k_d with $k_c \oplus k_d = 1$, defined as:

$$r_{\mathrm{TF}}^{k_c,k_d} = p_{XX}(k_c, k_d)\left[1 - h(E_X^{k_c,k_d}) - h(\bar{E}_Z^{k_c,k_d})\right] \tag{5.25}$$

with $p_{XX}(k_c, k_d)$, $E_X^{k_c,k_d}$ and $\bar{E}_Z^{k_c,k_d}$ given in (5.17), (5.18) and (5.22), respectively. In figure 5.2 we plot the asymptotic key rate (5.24) of the practical TF-QKD protocol

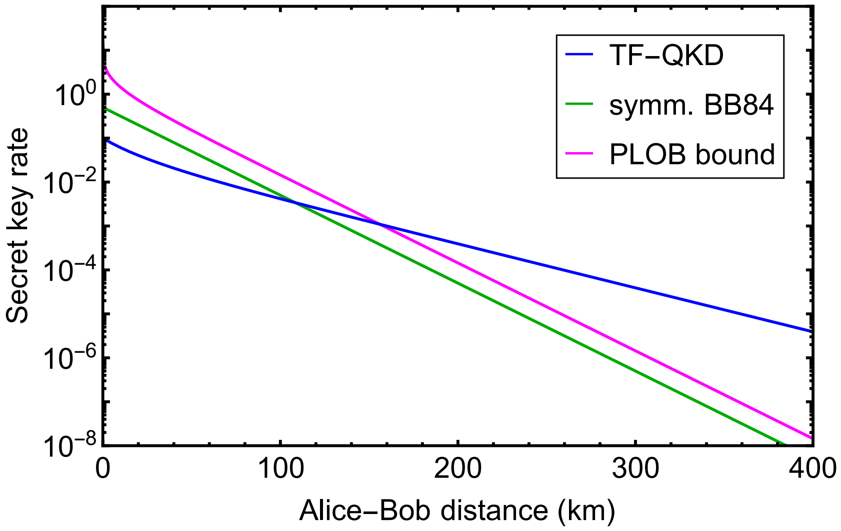

Fig. 5.2.: Logarithmic plot of the asymptotic secret key rates of the TF-QKD scheme in [CAL19] (Eq. 5.24, blue) and of the symmetric BB84 protocol with a single-photon source (Eq. 5.26, green), as a function of the distance between Alice and Bob. We assume that the quantum channels are telecom fibers with $0.2\,\mathrm{dB\,km^{-1}}$ of loss. Apart from this, the implementation of both protocols is error-free. We also plot the PLOB bound (Eq. 5.1, magenta). We observe the square-root improvement in the scaling of the TF key rate with the transmittance, compared to the BB84 protocol and to the PLOB bound. Note that a square-root improvement results in an increased slope in this logarithmic plot.

in [CAL19] as a function of the total distance L between Alice and Bob, assuming that they are both linked to the central relay by equally-long telecom fibers with $0.2\,\mathrm{dB\,km}^{-1}$ of loss. Hence the transmittances of their channels are: $\sqrt{\eta_A} = \sqrt{\eta_B} =: \sqrt{\eta} = 10^{-\frac{0.2L}{20}}$. In the figure we also report the PLOB bound (5.1) and the asymptotic key rate of a symmetric BB84 protocol (c.f. section 3.2) implemented with a single-photon source:

$$r_{\mathrm{symBB84}} = \eta/2. \tag{5.26}$$

For both protocols, we assume an ideal implementation where the only source of errors is the loss in the quantum channel(s) (simulations including other sources of error can be found in [CAL19]). In the case of the TF scheme, we also assumed an infinite number of decoy intensity settings, which basically means that the parties know the exact values of all the yields appearing in the upper bound $\bar{E}_Z^{k_c,k_d}$. Finally, we optimized the TF key rate (5.24) over the *signal intensities* α_A^2 and α_B^2 of the WCPs prepared by Alice and Bob in the X-basis rounds (for simplicity $\alpha_A, \alpha_B \in \mathbb{R}$). Note that, for identical losses $\sqrt{\eta_A} = \sqrt{\eta_B}$, the optimal signal intensities are equal: $\alpha_A^2 = \alpha_B^2$.

From figure 5.2 we observe the improved scaling of the TF key rate compared to the BB84 protocol and to the upper bound on the key rate of any point-to-point QKD protocol, i.e. the PLOB bound. Indeed, while the TF key rate scales with $\sim \sqrt{\eta}$, the BB84 protocol and the PLOB bound scale with $\sim \eta$. In particular, there exists a loss threshold/distance after which TF-QKD performs better than any point-to-point QKD scheme, i.e. when the PLOB bound is surpassed. We emphasize that this theoretical prediction has been recently confirmed experimentally [Wan+19; Liu+19; Zho+19; Min+19].

5.4 Twin-field QKD with Finite Decoys and Asymmetric Channels

In the reference [CAL19] that introduced the TF-QKD protocol without phase post-selection, the key rate performance is mainly investigated in the unrealistic scenario where Alice and Bob can use an infinite number of decoy intensity settings.

In order to investigate the real performance of the proposed TF scheme, in our paper [GC19] (also reported in appendix C) we derive analytical bounds on several yields appearing in the upper bound (5.22) on the error rate E_Z, when the parties have at their disposal either two, three, or four decoy intensity settings.

Note that, since to every pair of decoy intensities corresponds a linear constraint on the yields (see (5.23)), increasing the number of decoy intensities enables us to bound a larger number of yields and more tightly. In the limit of infinitely many decoy intensity settings, the parties can correctly estimate all the infinite yields appearing in (5.22). Moreover, the larger the number of yields with an analytical bound, the smaller the number of yields trivially bounded by one in (5.22). This has the obvious effect of increasing the protocol's key rate.

Equipped with the derived bounds on the yields, we show that two decoy settings are enough to beat the PLOB bound (5.1) and that four decoy settings are close to optimal, i.e. the resulting key rate is almost indistinguishable from that where Alice and Bob have infinite decoy settings.

Furthermore, in the performance analysis in [CAL19] it is assumed that the losses affecting the quantum channels of Alice and Bob are equal and so are the optimal signal and decoy intensities. However, this does not reflect realistic scenarios where two parties establishing a secret key, e.g. in the context of a quantum network, are likely to be at different distances from the untrusted relay which processes their signals according to the TF-QKD protocol in [CAL19]. Moreover, potential intensity fluctuations affecting the parties' lasers are likely to be uncorrelated, causing the parties to effectively employ different signal and decoy intensities.

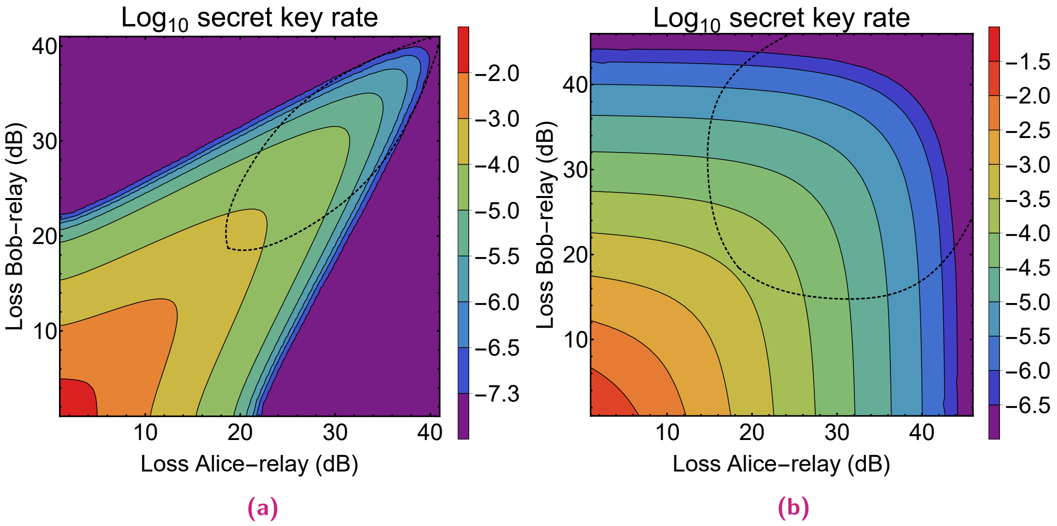

Fig. 5.3.: Contour lines for the asymptotic secret key rate of the TF-QKD scheme in [CAL19], evaluated with the yields bounds derived in [GNC19] relative to three decoy intensity settings. The key rate is optimized over the signal α_A^2, α_B^2 and decoy intensities $\{\mu_i\}, \{\nu_i\}$ of Alice and Bob, respectively. In (a) we additionally imposed the constraints: $\alpha_A = \alpha_B$ and $\{\mu_i\} = \{\nu_i\}$. We observe that, when the parties can use asymmetric intensities (b), the key rate is never enhanced by adding noise in one of the channels in order to symmetrize the losses. The black dotted lines enclose the region where the key rate beats the PLOB bound (5.1). We employed a realistic channel model with 2% polarization and phase misalignments and a dark count probability in each detector of 10^{-7}.

In order to address these issues, in another paper [GNC19] (also reported in appendix D) we investigate the performance of the TF-QKD protocol of [CAL19] in asymmetric-loss scenarios and in the presence of independent laser intensity fluctuations. To this aim, we derive new analytical bounds on the relevant yields appearing in (5.22), when the parties use two independent sets of decoy intensities ($\{\mu_i\}$ and $\{\nu_j\}$). In particular, inspired by the results of the previous work [GC19], we consider the cases of two, three and four decoy intensity settings for each party. We then numerically optimize the key rate over the (potentially) different signal and decoy intensities.

An example of the advantage gained by allowing Alice and Bob to independently select their signal and decoy intensities is given in figure 5.3. Here, we provide two contour plots of the secret key rate optimized over the signal and decoy intensities, as a function of the loss (measured in dB) in the quantum channels linking Alice and Bob to the untrusted relay. For instance, if Loss_A is the loss in Alice's channel, then the transmittance of her channel is given by: $\sqrt{\eta_A} = 10^{-\mathrm{Loss}_A/10}$.

The plot in figure 5.3a is optimized with the constraint that Alice and Bob use the same set of decoy intensities and the same signal intensity, while the plot in figure 5.3b is optimized without that constraint –i.e. Alice and Bob are free to independently optimize their intensities. We observe a drastic improvement of the key rate when the parties can independently select the signal and decoy intensities, especially when the losses in two channels are highly asymmetric. Surprisingly, when the parties are forced to employ the same intensities and their losses are significantly asymmetric, it is convenient for them to artificially increase the loss in one of their channels (e.g. by adding fiber) in order to maximize the key rate (see figure 5.3a). Further plots and analyses can be found in the paper [GNC19] reported in appendix D.

Finally we illustrate, in the simplest case of two decoy intensities per party, the procedure we adopt in [GC19; GNC19] to derive good bounds on the relevant yields in (5.22). In particular, as an example we derive the upper bound on $Y_{11}^{k_c,k_d}$. We assume that Alice (Bob) can choose among the decoy intensities $\{\mu_0, \mu_1\}$ with $\mu_0 > \mu_1$ ($\{\nu_0, \nu_1\}$ with $\nu_0 > \nu_1$). To keep the notation simple, we define the following rescaled gains in the Z basis (where we omit the detection pattern k_c, k_d):

$$\tilde{Q}^{\mu_i,\nu_j} = e^{\mu_i+\nu_j} p_{ZZ}(k_c, k_d|\mu_i, \nu_j), \tag{5.27}$$

and we rewrite the linear constraints on the yields (5.23) as follows:

$$\tilde{Q}^{\mu_i,\nu_j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!\, m!} \mu_i^n \nu_j^m. \tag{5.28}$$

Consider the following combination of gains:

$$G := \tilde{Q}^{0,0} + \tilde{Q}^{1,1} - \tilde{Q}^{0,1} - \tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!\,m!}(\mu_0^n - \mu_1^n)(\nu_0^m - \nu_1^m), \tag{5.29}$$

and note that the coefficients of the yields Y_{n0} and Y_{0m} are null for every n and m. We can then recast the last expression as follows:

$$G = Y_{11}(\mu_0 - \mu_1)(\nu_0 - \nu_1) + \sum_{\substack{n,m=1 \text{ s.t.} \\ n+m>2}}^{\infty} \frac{Y_{nm}}{n!\,m!}\left(\mu_0^n - \mu_1^n\right)\left(\nu_0^m - \nu_1^m\right) \ . \tag{5.30}$$

We emphasize that Y_{11} is now the yield with the largest coefficient[2] in (5.30), thus trivially bounding the other yields is not as harmful as it would be if they had the largest coefficients.

An upper bound on Y_{11} is then obtained by considering the worst-case scenario for the other yields, taking into account that they are probabilities, i.e. $0 \leq Y_{nm} \leq 1$. Since all the yields' coefficients have the same sign in (5.30), the yield Y_{11} is maximal when all the other yields are minimal. Hence, the upper bound on Y_{11} is obtained by setting all the other yields to zero in (5.30):

$$Y_{11}^U = \min\left\{\frac{G}{(\mu_0 - \mu_1)(\nu_0 - \nu_1)}\, ,\, 1\right\}. \tag{5.31}$$

Note that by taking the minimum in the above expression we make sure that Y_{11}^U is a meaningful bound on a probability. The upper bound in (5.31) is only expressed in terms of input parameters (the decoy intensities) and observed gains contained in G (see (5.29)).

5.5 Conference Key Agreement with Single Photon Interference

The founding idea of TF-QKD, elucidated in subsection 5.3.1, can also be generalized with some adjustments to the multiparty scenario. Indeed, in our work [GKB19] (also found in appendix E) we devise a conference key agreement (CKA) where N parties simultaneously distil a secret conference key through single-photon interference occurring at an untrusted relay.

In particular, parties Alice$_1$, Alice$_2$, . . . , Alice$_N$ establish the conference key by sending optical pulses to the relay and by performing suitable measurements on their

[2] Optimal decoy intensity values are typically smaller than one, and one of the decoy intensities of each party is always as small as allowed by the experimental equipment [GC19; GNC19].

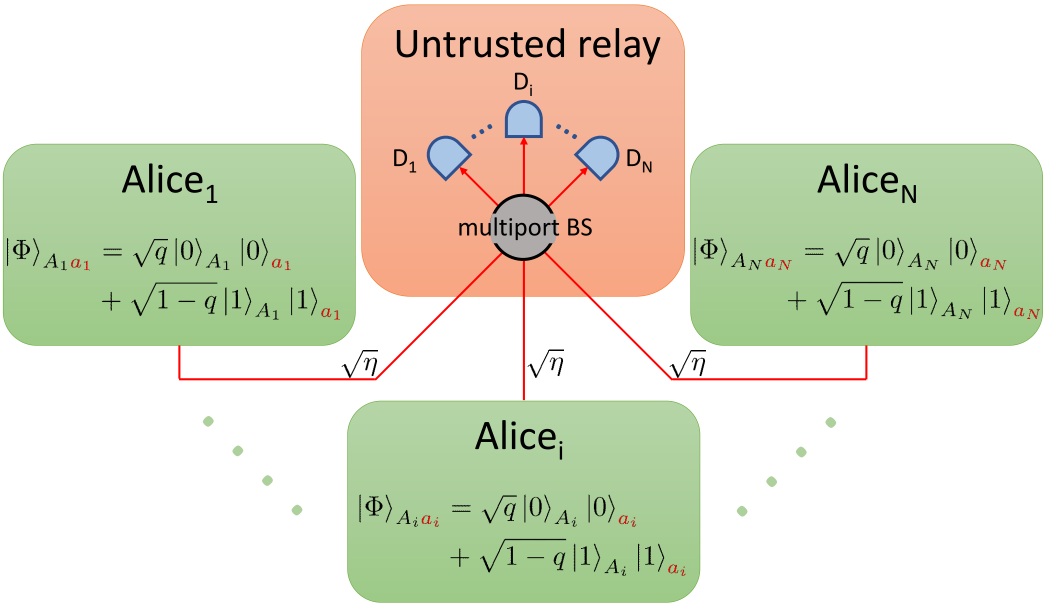
Untrusted relay
D_i
D_1
D_N
multiport BS
Alice$_1$
$|\Phi\rangle_{A_1a_1} = \sqrt{q}\,|0\rangle_{A_1}|0\rangle_{a_1} + \sqrt{1-q}\,|1\rangle_{A_1}|1\rangle_{a_1}$
Alice$_N$
$|\Phi\rangle_{A_Na_N} = \sqrt{q}\,|0\rangle_{A_N}|0\rangle_{a_N} + \sqrt{1-q}\,|1\rangle_{A_N}|1\rangle_{a_N}$
$\sqrt{\eta}$
$\sqrt{\eta}$
$\sqrt{\eta}$
Alice$_i$
$|\Phi\rangle_{A_ia_i} = \sqrt{q}\,|0\rangle_{A_i}|0\rangle_{a_i} + \sqrt{1-q}\,|1\rangle_{A_i}|1\rangle_{a_i}$

Fig. 5.4.: In the CKA we introduce in [GKB19], every party initially prepares an entangled state between a qubit she holds and an optical signal given by (5.32). The state is unbalanced towards the vacuum: $1-q \ll 1$. The signals are then sent to the untrusted relay through optical channels with transmittance $\sqrt{\eta}$. The relay combines the pulses in a balanced multiport BS featuring a detector at every output port, and then announces the outcome of the detection of each detector. The events in which only one detector clicked are most likely caused by the detection of just one photon, sent by one of the parties with equal probability (single-photon interference). Hence, the conditional state of the qubits $A_1,\dots,A_N$ is well approximated by a W state, which can be used by the parties to distil a conference key.

qubits. The resulting CKA is sketched in figure 5.4 and each round is characterized by the following steps.

1. Alice$_i$ ($i=1,\dots,N$) prepares an optical pulse a_i entangled with a qubit A_i she holds:

$$|\Phi\rangle_{A_ia_i} = \sqrt{q}\,|0\rangle_{A_i}|0\rangle_{a_i} + \sqrt{1-q}\,|1\rangle_{A_i}|1\rangle_{a_i} \quad 0 \leq q \leq 1 \tag{5.32}$$

   where $|0\rangle_{a_i}, |1\rangle_{a_i}$ are the photon's vacuum and single-photon state, while $\{|0\rangle_{A_i}, |1\rangle_{A_i}\}$ is the computational basis of qubit A_i (Z basis).

2. Every party sends her optical pulse a_i to the relay via optical channels of transmittance $\sqrt{\eta}$. The transmittance between any two parties is thus η.

3. The relay applies a Bell-multiport beam splitter [ZZH97; LB05; Per+11; Spa+13] with M input and M output ports (where $M \geq N$) to the incoming pulses and is followed by a threshold detector D_i ($i=1,\dots,M$) at each output port. If $M > N$, some inputs ports receive the vacuum. The action of the

multiport beam splitter (BS) is defined by the following unitary transformation which reduces to the standard 50:50 BS for $M = 2$:

$$a^\dagger_{\text{in},i} \mapsto \sum_{j=1}^{M} U_{ij} a^\dagger_{\text{out},j}, \tag{5.33}$$

where $a^\dagger_{\text{in},i}$ ($a^\dagger_{\text{out},j}$) are the creation operators of the incoming (outgoing) photons and U_{ij} are the coefficients of a unitary matrix defined as:

$$U_{ij} = \frac{1}{\sqrt{M}} e^{\mathbb{i}\frac{2\pi}{M}(i-1)(j-1)} \qquad i, j \in \{1, \ldots, M\}. \tag{5.34}$$

4. The relay broadcasts the outcome k_j of every detector D_j, with $k_j = 0$ ($k_j = 1$) corresponding to a no-click (click) event. The round is discarded when $\sum_{j=1}^{M} k_j \neq 1$, i.e. whenever single-photon interference did not occur. The probability that only detector D_j clicked is p_D and is independent of the detector due to the symmetric action of the multiport BS.

5. The round is classified either as a parameter-estimation (PE) round with probability p_r or as a key-generation (KG) round with probability $1 - p_r$. In case of a PE round, every party measures her qubit in the Z-basis. In case of a KG round, conditioned on detector D_j clicking, Alice_i measures her qubit in the basis of the operator $O_{XY}(\varphi_i) = \cos(\varphi_i)X + \sin(\varphi_i)Y$ (where X and Y are the Pauli operators), with $\varphi_i = \arg(U_{ij})$. Upon observing the outcome x_i (where $x = \pm 1$ are the eigenvalues of Z and $O_{XY}(\varphi_i)$), Alice$_i$ records the bit value b_i with $(-1)^{b_i} = x_i$.

6. The bits b_i measured in KG rounds form Alice$_i$'s raw key, while those obtained in PE are used to detect Eve's action and quantify the information she gained on Alice$_1$'s raw key.

After performing a suitable number of rounds, all the parties perform one-way error correction to match their raw keys to Alice$_1$'s raw key. The parties then perform privacy amplification on their error-corrected keys to distil a shorter, secret, conference key.

The error rates E_Z and $E_{A_1 A_i}$ devoted to quantify Eve's knowledge and the information that Alice$_1$ needs to send for error correction are defined as follows:

$$E_Z = p_{\text{PE}} \left[b_1 = \bigoplus_{i=2}^{N} b_i | \sum_{j=1}^{M} k_j = 1 \right] \tag{5.35}$$

$$E_{A_1 A_i} = p_{\text{KG}} \left[b_1 \neq b_i | \sum_{j=1}^{M} k_j = 1 \right], \tag{5.36}$$

where $p_{\text{PE(KG)}}[\Omega]$ is the probability that the event Ω occurred in a PE (KG) round. The asymptotic secret conference key rate achieved by the described CKA protocol based on single-photon interference events reads:

$$r_{\text{spCKA}} = M p_D \left(1 - h(E_Z) - \max_{2\leq i\leq N} h(E_{A_1 A_i})\right) \tag{5.37}$$

Notably, the above CKA scheme and the relative asymptotic key rate reduce to the idealized TF-QKD protocol presented in subsection 5.3.1 when $N = M = 2$.

Remark 5.2 (Preshared key)**.** *The parties can know beforehand the nature of each round of the protocol thanks to a preshared secret key they hold. For instance, they could share a key with as many bits as rounds, where the bit value* 1 *(*0*) indicates a PE (KG) round. Since* p_r *is typically small, the key is composed mainly of zeroes and can thus be highly compressed. In particular, if* R *is the total number of rounds, the parties need a preshared secret key of* $R\,h(p_r)$ *bits, where* $h(x)$ *is the binary entropy. The length of the preshared key must be subtracted from the final secret key length in order to quantify the amount of fresh secret bits produced by the protocol. However, in the asymptotic regime (*$R \to \infty$*) considered here, the penalty introduced by the preshared key on the asymptotic conference key rate is given by* $h(p_r)$ *and is negligible, e.g. by choosing* $p_r \sim 1/R$*.*

5.5.1 Multipartite QKD with a W state

Here we would like to provide, as in the case of the idealized TF-QKD protocol, a bit of intuition on why the above CKA protocol works.

When optimizing the conference key rate in (5.37) over q, we obtain values such that $1 - q \ll 1$, that is the initial entangled states (5.32) are strongly unbalanced towards the vacuum. Therefore, the rounds where only one detector clicked are mainly caused by the sending and detection of just one photon. The photon could be sent by any Alice$_i$, implying that her qubit would be in state $|1\rangle_{A_i}$ while the qubits of the other parties would be in state $|0\rangle_{A_{\neq i}}$. Since the multiport BS creates a coherent superposition of all these possibilities, by post-selecting the rounds where e.g. detector D_j clicked, the state of the parties' qubits is approximately given by the following W-class state[3] [DVC00]:

$$|W_j\rangle_{A_1 \dots A_N} = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \sqrt{M} U_{ij} \, |\vec{v}_i\rangle \,, \tag{5.38}$$

[3] The W state usually considered in the literature reads: $\frac{1}{\sqrt{N}} \sum_{i=1}^{N} |\vec{v}_i\rangle$.

where the bitstring $\vec{v}_i \in \{0,1\}^N$ is composed of all zeroes except for the i-th bit which has value one and where U_{ij} is defined in (5.34). We remark that the qubits' state in (5.38) is only an approximation in the limit $1-q \ll 1$ where terms of second or higher order in $1-q$ have been neglected and in the ideal scenario of no losses ($\sqrt{\eta}=1$) and no other sources of noise.

Although it is proven [Epp+17] that no N-qubit state other than the GHZ state (3.31) can lead to perfectly correlated outcomes in one measurement basis (for $N \geq 3$), the parties can still distil a secret conference key by properly measuring their qubits in state (5.38).

Indeed, the measurements that the parties perform in KG rounds (see protocol description) are chosen to minimize the key-bit error rate $E_{A_1 A_i}$ between Alice$_1$ and any other party. In particular, one could view the measurement of Alice$_i$ in the eigenbasis of $\cos[\arg(U_{ij})]X + \sin[\arg(U_{ij})]Y$ as composed of two steps. First she rotates her X operator in the (x,y)-plane of the Bloch sphere by an angle $\arg(U_{ij})$, in order to remove the effect of the complex phase $\sqrt{M}U_{ij}$ introduced by the BS when D_j clicked. Then she measures in the eigenbasis of the rotated operator.

The resulting error rate $E_{A_1 A_i}$ (5.36) the parties would observe if their qubits were exactly in the state (5.38) is given by:

$$E_{A_1 A_i} = \frac{1}{2} - \frac{1}{N}. \tag{5.39}$$

This intrinsic error rate affecting the parties' raw key bits is unavoidable due to the fact that they are measuring a W-class state, instead of a GHZ state. Conversely, the error rate E_Z (5.35) computed in PE is null on the state (5.38), confirming that in ideal conditions Eve does not gain any information.

We have thus argued that multipartite QKD can also be implemented on a W state, instead of the conventional GHZ state used in the majority of cases, e.g. with the multiparty BB84 and six-state protocols (c.f. section 3.4). Despite presenting the drawback of the intrinsic error rate (5.39), the CKA based on the W state becomes dramatically advantageous in high-loss scenarios.

Indeed, the W state is post-selected when single-photon interference occurred at the relay. This implies that the resulting conference key rate (5.37) scales linearly with the transmittance $\sqrt{\eta}$ of one of the channels linking the parties to the relay.

Let us now consider a generic optical implementation of a CKA based on an N-qubit GHZ state, where the qubit state is encoded in one of the photon's degrees of freedom (e.g. the polarization). The N photons described by an N-qubit GHZ state are distributed from a central untrusted node to the N parties through the same quantum channels with transmittance $\sqrt{\eta}$. The conference key rate of this protocol cannot scale better than $\sim (\sqrt{\eta})^N$, since all the photons are required to arrive in order to have a successful round.

Clearly, in a high-loss scenario ($\sqrt{\eta} \to 0$) the conference key rate of our CKA based on single-photon interference will outperform any CKA based on GHZ states and implemented as described above.

Remark 5.3 (Impossibility of prepare-and-measure CKA)**.** *We emphasize that the measurements performed by the parties in the KG rounds do not commute with the operations of the relay, inasmuch as they depend on which detector clicked. This means that the CKA cannot be turned into a prepare-and-measure scheme where each party prepares some optical signal depending on a random bit and on the basis choice. For this reason, it cannot be regarded as an MDI-QKD protocol since the parties still need to perform trusted measurements on their qubits.*

This contrasts with the TF-QKD idealized protocol presented in subsection 5.3.1, which is recovered here for $N = M = 2$. The bipartite case is special since the complex phase introduced by the BS in the shared state (5.38) *reduces to a minus sign, which can be reabsorbed by asking Alice$_2$ to flip her classical outcome b_2 when detector D_2 clicks, as described in subsection 5.3.1. This removes the need to adjust the parties' measurements depending on the result of the detection, hence making these two steps commute.*

Nevertheless, the quantum operations required by our CKA seem to be feasible with present-day technology [Ber+13; Roz+19; Abo+18].

5.5.2 Performance assessment

In [GKB19], we prove the CKA security in the finite-key scenario for the most general attacks the eavesdropper can perform. We also investigate the protocol's performance for a realistic channel model that accounts for polarization and phase misalignments and dark counts in the detectors.

In order to benchmark the performance of our CKA based on a central untrusted relay, we consider a scenario where the relay is removed and the parties are all connected in a star network where the transmittance between any two parties is η. In this configuration, we consider the conference key rate generated by the following strategy and compare it with the CKA key rate (5.37). One special party, say Alice$_1$, performs the best possible bipartite QKD protocol with every other party, thus establishing $N - 1$ secret keys whose key rate is given by the PLOB bound (5.1). Alice$_1$ then uses the established keys to distribute the conference key to the other parties with one-time pad encryption. The resulting conference key rate is thus given by the rate at which the bipartite keys were generated, rescaled by the factor $1/(N-1)$ which accounts for the fact that Alice$_1$ repeated the bipartite scheme

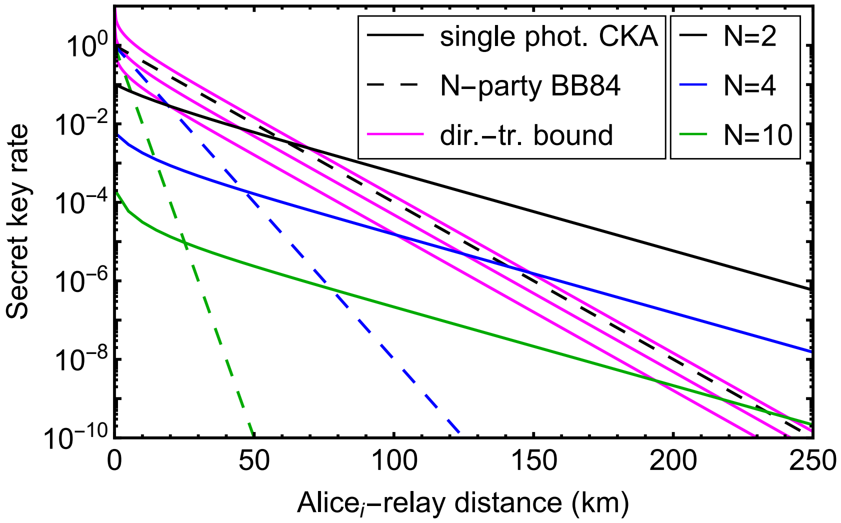

Fig. 5.5.: Conference key rates yielded by the CKA based on single-photon interference (solid lines, Eq. 5.37 optimized over q with $M = N$) and by the N-party BB84 protocol (dashed lines, Eq. 5.41) as a function of the channel length between one party and the untrusted relay, for different numbers of parties N. The solid magenta lines are the direct-transmission bound ($N = 2$ top, $N = 4$ middle, $N = 10$ bottom; Eq. 5.40). The experimental setup is assumed to be ideal except for the lossy quantum channels with $0.2\,\mathrm{dB\,km}^{-1}$ of loss. The improved key rate scaling of the single-photon-based CKA enables it to outperform both the N-BB84 protocol and the direct-transmission bound on longer distances.

$N - 1$ times. The conference key rate resulting from the above strategy implemented on the star network reads:

$$r_{\text{dir.tr.}} = \frac{-\log_2(1-\eta)}{N-1} \tag{5.40}$$

and we call it the *direct-transmission* bound. This is similar to what is done for TF-QKD when benchmarked against the PLOB bound (c.f. figure 5.2), which bounds the highest possible key rate achieved between Alice and Bob if the untrusted relay is removed.

In figure 5.5 we plot the CKA key rate in (5.37) (solid lines) and the conference key rate of the N-partite BB84 protocol (dashed lines), as a function of the distance between one party and the relay and for different numbers of parties ($N = 2, 4, 10$). In the same figure, we also plot the direct-transmission bound (5.40) (solid magenta lines; the top line corresponds to $N = 2$, the middle to $N = 4$ and the bottom to $N = 10$).

The conference key rates are obtained in an ideal experimental setup where the only source of errors is the photon loss in the quantum channels. We assumed as usual $0.2\,\mathrm{dB\,km}^{-1}$ of loss in each quantum channel, the typical loss of standard telecom fiber. In [GKB19] (appendix E) we account for more realistic channel models, which include dark counts in the detectors and misalignments of the phase and polarization.

The considered N-BB84 protocol is such that the relay has the function of distributing the entangled photon state to the N parties. In the chosen ideal setting, the conference key rate of the N-BB84 protocol is just given by the probability that each photon reaches the corresponding party:

$$r_{\mathrm{NBB84}} = \eta^{N/2}. \tag{5.41}$$

The CKA key rate (5.37) has been optimized over the parameter q and we fixed the number of BS ports to match the number of parties: $M = N$. We remark that the optimal number of BS ports –and thus detectors– is $M \approx N$ but it actually depends on the loss. Indeed, a larger number of BS ports decreases the possibility of detecting two photons in the same detector, which is a source of error especially at low losses. However, when accounting for dark counts in the detectors, increasing the number of detectors implies a higher probability of dark counts, which is another source of error manifesting itself at high losses with a drop of the key rate.

As anticipated, figure 5.5 clearly shows the significant improvement in the conference key rate when employing our CKA based on single-photon interference, as opposed to employing a GHZ-state-based CKA like the N-party BB84 protocol. Moreover, due to the improved scaling with the loss, the CKA key rate (5.37) also surpasses the direct-transmission bound (5.40) for sufficiently long distances, similarly to what happens with the TF-QKD protocol and the PLOB bound (see figure 5.2).

6 Device-independent Cryptography

> *Bell's theorem, formulated in 1964, is one of the profound scientific discoveries of the century.*
>
> — **Alain Aspect**

We have already seen in chapters 4 and 5 how imperfections in the quantum devices employed in a QKD protocol, when not accounted for in the security proof, can be exploited by an eavesdropper to spoil the protocol's security. In this context, MDI-QKD and TF-QKD protocols represent possible solutions as they do not require to trust the measurement devices, which can be completely controlled by the eavesdropper, and yet derive a secret key. However, both MDI-QKD and TF-QKD still require to trust the sources held by the parties.

Until now we presented QKD protocols where at least some devices in the experimental apparatus need to be trusted. Of course, we could place our trust in such devices more lightheartedly upon deeply characterizing their functioning. However, the characterization process is often challenging and we might not be capable or willing to do it. Indeed, in most cases QKD users are laymen who simply want to purchase a service which guarantees a high level of security, without bothering to verify the claimed security.

Quite astonishingly, secure QKD is still possible even when the whole experimental apparatus is untrusted and potentially under the control of the eavesdropper[1]. Indeed, by exploiting the non-local properties of quantum correlations, device-independent (DI) QKD protocols [YM98; AGM06; Pir+09; MPA11; VV14; Arn+18] and DI conference key agreement (DICKA) protocols [SG01a; SG01b; RMW19; HKB19] deliver the same secret key to a group of two or more parties, respectively, where the security of the key is independent of the actual functioning of the employed devices.

In a similar fashion, in DI randomness generation (DIRG) protocols [Col07; Pir+10; CK11; Nie+18; PM13; FGS13], the intrinsic randomness generated by quantum mechanical processes is proven to be private upon the observation of

[1] Minimal requirements on the devices are still in place, such as the isolation of the trusted parties' labs. Without this requirement, the devices could simply broadcast the established secret key upon completing the protocol.

certain non-local correlations. Note that secret true randomness is one of the prerequisites of most quantum cryptographic protocols.

The chapter is organized as follows. In section 6.1 we introduce the concept of non-local correlations and show how they can be witnessed through a Bell inequality violation. We formalize the definitions of different kinds of correlations in section 6.2. Then, we link the observation of a Bell violation to the security proof of DI protocols in section 6.3. In section 6.4 we provide an explicit example of DIQKD protocol and prove its security in section 6.5. In section 6.6 we illustrate our recent results which enable tight security proofs of certain multiparty DI protocols (paper in appendix H). We conclude by discussing the suitability of full-correlator Bell inequalities for DICKA and present a multipartite Bell inequality specifically built for the task of DICKA (section 6.7).

6.1 Bell's Theorem

Bell's theorem [Bel64; Bel04] states that there exist predictions of quantum theory that cannot be explained by any local theory, i.e. a theory based on the assumption of *locality*. In this section we clarify our definition of locality and prove Bell's theorem. The proof critically relies on the introduction of a *Bell inequality* [Bel04], that is an inequality involving a linear combination of correlators which is satisfied by every local theory but is violated by quantum mechanics.

In the literature one can find several versions of Bell's theorem's proof, leveraging on different assumptions. Here, we mainly follow the proofs presented in [Val02; Gol+11; Bru+14; HR19] that make use of the Clauser-Horne-Shimony-Holt (CHSH) inequality [Cla+69], arguably the most popular Bell inequality.

Let us consider the following Bell experiment, depicted in figure 6.1. Two physical systems, which could have interacted in the past, are now far apart and are individually measured by two parties, Alice and Bob. No information is given on the systems, which are thus treated as black boxes. Each box (system) is equipped with two inputs corresponding to the measurement choices of the parties, and generates a binary output upon selecting an input. Hence, the measurement process consists in Alice (Bob) selecting an input $x \in \{0, 1\}$ ($y \in \{0, 1\}$) on her (his) system and collecting the output $a \in \{-1, 1\}$ ($b \in \{-1, 1\}$). We assume that the measurement processes of Alice and Bob are spacelike separated events.

By repeating the experiment several times, the parties can roughly estimate the probability distribution $p(a, b|x, y)$ governing the occurrence of the outcomes a and b, given the inputs x and y. In general, the outcomes recorded by Alice and Bob

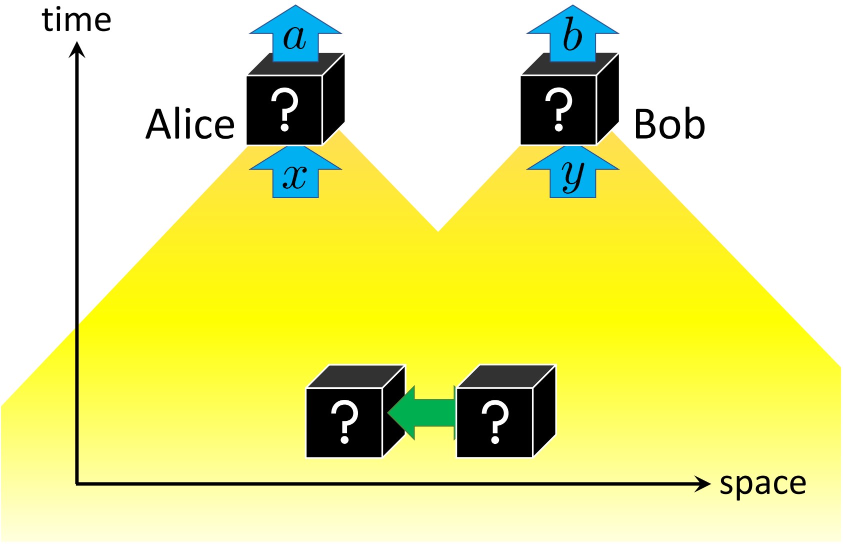

Fig. 6.1.: In a bipartite Bell experiment, two unknown systems are given to Alice and Bob. The systems might have interacted in the past, in the spacetime region where their past light cones overlap. Alice (Bob) can only interact with her (his) system by selecting an input x (y) and collecting an output a (b). The interactions of the two parties with the respective systems are assumed to be spacelike separated events.

may not be statistically independent, which means that the probability distribution $p(a,b|x,y)$ is not factorized:

$$p(a,b|x,y) \neq p(a|x,y)p(b|x,y). \tag{6.1}$$

This fact could be caused by the previous interaction of the two systems and does not necessarily imply any kind of direct influence of one system on the other. Let us denote with λ the set of underlying (or hidden) variables that completely describe the two systems under consideration. By fixing the value of λ, we fix the *microstate* of the Bell experiment. Hence, λ can account for any dependence relation between the two systems due to their previous interaction. Since the value of λ could vary in different runs of the experiment, the probability distribution $p(a,b|x,y)$ can be expressed as:

$$p(a,b|x,y) = \int d\lambda\, p(a,b|x,y,\lambda)p(\lambda|x,y). \tag{6.2}$$

We remark that so far we did make any assumption on the theory we employ to describe the Bell experiment, indeed Eq. (6.2) is still completely general. We now assume that any theory describing the experiment should satisfy the following (apparently) natural conditions:

1. (Bell-)locality: All the statistical correlations of the outputs a and b are fully attributable to their past interaction and thus explainable with the knowledge of λ. Formally we have that:

$$\begin{aligned} p(a,b|x,y,\lambda) &= p(a|b,x,y,\lambda)p(b|x,y,\lambda) \\ &= p(a|x,y,\lambda)p(b|x,y,\lambda), \end{aligned} \tag{6.3}$$

   where the second equality represents the fact that, conditioned on the knowledge of λ, the residual indeterminacy of a is local and not due to a lack of knowledge of b.

2. Parameter independence: For each microstate λ, the probability of Alice (Bob) obtaining outcome a (b) is independent of the input y (x) selected by Bob (Alice):

$$\begin{aligned} p(a|x,y,\lambda) &= p(a|x,\lambda) \\ p(b|x,y,\lambda) &= p(b|y,\lambda). \end{aligned} \tag{6.4}$$

   This assumption is justified by special relativity, according to which spacelike separated measurements do not influence each other's outcome probability distribution.

3. Free will: The measurements inputs are uncorrelated from the underlying state of the systems described by λ:

$$p(x,y,\lambda) = p(x,y)p(\lambda). \tag{6.5}$$

   In other words, Alice and Bob are free to choose their inputs independently of the value of the hidden variables λ. By combining this assumption with the previous one, we are basically assuming that spacelike separated parties cannot communicate superluminally, which is the *causality* constraint of relativity.

By employing the assumptions (6.3), (6.4) and (6.5) in (6.2), we obtain the Bell experiment description of a local hidden variable (LHV) model:

$$p(a,b|x,y) = \int d\lambda\, p(\lambda)p(a|x,\lambda)p(b|y,\lambda). \tag{6.6}$$

We will now show that the correlations predicted by quantum mechanics on certain implementations of the Bell experiment cannot be expressed in the form (6.6). To this aim, we define the correlator:

$$\langle a_x b_y \rangle = \sum_{a,b=\pm 1} ab\, p(a,b|x,y), \tag{6.7}$$

as the expectation value of the product of Alice and Bob's outcomes, given that they selected inputs x and y. We then define the CHSH value [Cla+69]:

$$S_{\text{CHSH}} = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \tag{6.8}$$

and prove that if the probabilities $p(a,b|x,y)$ are explainable in terms of a LHV model (6.6), then the *CHSH inequality* holds:

$$S_{\text{CHSH}} = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \leq 2. \tag{6.9}$$

We start by using (6.6) to express the correlators $\langle a_x b_y \rangle$ in (6.7) as a product of local expectation values:

$$\langle a_x b_y \rangle = \int d\lambda\, p(\lambda) \left\langle a_x \right\rangle_\lambda \left\langle b_y \right\rangle_\lambda \tag{6.10}$$

where $\langle a_x \rangle_\lambda = \sum_a a\, p(a|x,\lambda)$ and similarly for $\langle b_y \rangle_\lambda$, with $\langle a_x \rangle_\lambda, \langle b_y \rangle_\lambda \in [-1,1]$ (recall that $a, b \in \{-1,1\}$). By inserting (6.10) into (6.8) we can write that:

$$S_{\text{CHSH}} = \int d\lambda\, p(\lambda) S^\lambda_{\text{CHSH}}, \tag{6.11}$$

where:

$$\begin{aligned} S^\lambda_{\text{CHSH}} &= \langle a_0 \rangle_\lambda \langle b_0 \rangle_\lambda + \langle a_0 \rangle_\lambda \langle b_1 \rangle_\lambda + \langle a_1 \rangle_\lambda \langle b_0 \rangle_\lambda - \langle a_1 \rangle_\lambda \langle b_1 \rangle_\lambda \\ &= \langle a_0 \rangle_\lambda (\langle b_0 \rangle_\lambda + \langle b_1 \rangle_\lambda) + \langle a_1 \rangle_\lambda (\langle b_0 \rangle_\lambda - \langle b_1 \rangle_\lambda). \end{aligned} \tag{6.12}$$

Since every expectation value is in the range $[-1,1]$, the last expression can be upper bounded by:

$$S^\lambda_{\text{CHSH}} \leq \left| \langle b_0 \rangle_\lambda + \langle b_1 \rangle_\lambda \right| + \left| \langle b_0 \rangle_\lambda - \langle b_1 \rangle_\lambda \right|. \tag{6.13}$$

Without loss of generality we can assume that: $\langle b_0 \rangle_\lambda \geq \langle b_1 \rangle_\lambda \geq 0$ (the other cases lead to the same result), which substituted in the last expression yields:

$$S^\lambda_{\text{CHSH}} \leq 2 \langle b_0 \rangle_\lambda \leq 2. \tag{6.14}$$

By employing (6.14) in (6.11), we prove the CHSH inequality in (6.9) for every probability distribution that can be written in the form (6.6).

In order to complete the proof of Bell's theorem, we demonstrate that quantum theory predicts correlations violating the CHSH inequality (6.9) for a specific implementation of the Bell experiment. This implies that they cannot be explained in terms of an LHV model (6.6).

Suppose that Alice's system and Bob's system are qubits in the entangled (Bell) state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{6.15}$$

whose corresponding density operator can be written in terms of the Pauli operators X, Y and Z as follows [TG05; Hol+19]:

$$|\Phi^+\rangle\langle\Phi^+| = \frac{1}{4}\left(\mathrm{id}\otimes\mathrm{id} + X\otimes X + Z\otimes Z - Y\otimes Y\right). \tag{6.16}$$

Notably, the last expression decomposes the projector on the state $|\Phi^+\rangle$ as a sum over all the *stabilizer operators* of the state $|\Phi^+\rangle$. An operator O is a stabilizer of a state $|\psi\rangle$ if $O\,|\psi\rangle = |\psi\rangle$, i.e. if the state is an eigenstate of O with eigenvalue one.

In this setting, we describe Alice's (Bob's) measurement on her (his) qubit as a binary projective measurement represented by the observable A_x (B_y), corresponding to input x (y). The generic form of A_x (B_y) is given by $A_x = \vec{\alpha}^{(x)}\cdot\vec{\sigma}$ ($B_y = \vec{\beta}^{(y)}\cdot\vec{\sigma}$), where $\vec{\sigma}$ is the vector of Pauli operators: $\sigma_1 = X$, $\sigma_2 = Y$ and $\sigma_3 = Z$ and where $\left\|\vec{\alpha}^{(x)}\right\| = \left\|\vec{\beta}^{(y)}\right\| = 1$.

Then, the correlators in the CHSH inequality (6.9) can be written as:

$$\begin{aligned}\langle a_x b_y\rangle &= \langle\Phi^+|A_x\otimes B_y|\Phi^+\rangle = \mathrm{Tr}\left[|\Phi^+\rangle\langle\Phi^+|(A_x\otimes B_y)\right]\\ &= \alpha_1^{(x)}\beta_1^{(y)} - \alpha_2^{(x)}\beta_2^{(y)} + \alpha_3^{(x)}\beta_3^{(y)},\end{aligned} \tag{6.17}$$

where we used the decomposition (6.16), the multiplication rule of Pauli operators in (2.17) and the fact that the Pauli operators are traceless.

We aim at maximizing the CHSH value (6.8), expressed in terms of the measurement directions $\vec{\alpha}^{(x)}$ and $\vec{\beta}^{(y)}$ of Alice and Bob via (6.17):

$$\begin{aligned}S_{\mathrm{CHSH}} =& \alpha_1^{(0)}(\beta_1^{(0)} + \beta_1^{(1)}) - \alpha_2^{(0)}(\beta_2^{(0)} + \beta_2^{(1)}) + \alpha_3^{(0)}(\beta_3^{(0)} + \beta_3^{(1)})\\ & \alpha_1^{(1)}(\beta_1^{(0)} - \beta_1^{(1)}) - \alpha_2^{(1)}(\beta_2^{(0)} - \beta_2^{(1)}) + \alpha_3^{(1)}(\beta_3^{(0)} - \beta_3^{(1)}).\end{aligned} \tag{6.18}$$

The last expression is maximized if we choose, for instance,

$$\begin{aligned}\vec{\alpha}^{(0)} &= (1,0,0) \quad & \vec{\alpha}^{(1)} &= (0,0,1)\\ \vec{\beta}^{(0)} &= \left(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}}\right) \quad & \vec{\beta}^{(1)} &= \left(\frac{1}{\sqrt{2}},0,-\frac{1}{\sqrt{2}}\right),\end{aligned} \tag{6.19}$$

With these measurement settings the CHSH value (6.18) is given by:

$$S_{\text{CHSH}} = 2\sqrt{2} > 2, \tag{6.20}$$

i.e. the CHSH inequality (6.9) is violated.

Note that the measurement settings in (6.19) correspond to Alice and Bob measuring the observables:

$$\begin{aligned} A_0 &= X \quad & A_1 &= Z \\ B_0 &= \frac{X+Z}{\sqrt{2}} \quad & B_1 &= \frac{X-Z}{\sqrt{2}}, \end{aligned} \tag{6.21}$$

which substituted into the CHSH expression (6.8) and upon simplifications lead to:

$$S_{\text{CHSH}} = \sqrt{2}\,\langle\Phi^+|X\otimes X|\Phi^+\rangle + \sqrt{2}\,\langle\Phi^+|Z\otimes Z|\Phi^+\rangle = 2\sqrt{2}. \tag{6.22}$$

The last expression has the merit to show that it is optimal for the parties to choose measurements such that the resulting CHSH expression (after being simplified) is exclusively composed of correlators of stabilizers of the state $|\Phi^+\rangle$. This makes sense, since by definition the correlator of a stabilizer evaluated on the stabilized state achieves the maximum value of 1.

The CHSH violation predicted by quantum theory has profound consequences, as it implies that one of the three assumptions (6.3), (6.4) and (6.5) that led to the derivation of the CHSH inequality does not hold for quantum theory. The quantum theory we consider in this thesis is the standard non-relativistic quantum theory, which describes quantum systems and measurements in terms of tensor-product Hilbert spaces and local Kraus operators acting on the corresponding Hilbert space. These features, combined with the partial trace rule, ensure that the local statistics of a system only depend on its reduced density operator. Therefore, no superluminal communication is allowed between parties and in particular the conditions of parameter independence (6.4) and of free will (6.5) are satisfied.

From the above argument, we conclude that quantum mechanics is a non-local theory, i.e. it does not satisfy the locality assumption in (6.3), and its predictions cannot be reproduced by any local theory. This concludes the proof of Bell's theorem.

Another important consequence of Bell's theorem are Bell inequalities. These can seen as means to experimentally test if Nature behaves according to local theories or not. The numerous experiments demonstrating the violation of Bell inequalities have proved beyond reasonable doubt that Nature is non-local. In particular, we mention the first successful results in this direction by Aspect et al [ADR82]. Recent and more sophisticated experiments have confirmed the existence of non-local correlations in *loophole-free* Bell tests [Hen+15; Giu+15; Sha+15], i.e. conducted without making any assumption that could lead to a description of the non-local correlation through an LHV model.

6.2 Local, Quantum, No-signaling and Causal Correlations

In this section we wish to clarify the relations existing between different types of correlations, starting from what we have seen in the proof of Bell's theorem.

First of all, we can derive the so called *no-signaling constraints* [Bru+14; HR19] from the parameter-independence (6.4) and free-will (6.5) assumptions used in Bell's theorem:

$$\begin{aligned} p(a|x,y) &= \int d\lambda\, p(a|x,y,\lambda)p(\lambda|x,y) \\ &\overset{(6.5)}{=} \int d\lambda\, p(a|x,y,\lambda)p(\lambda) \\ &\overset{(6.4)}{=} \int d\lambda\, p(a|x,\lambda)p(\lambda) \\ &= p(a|x), \end{aligned} \tag{6.23}$$

and similarly one gets

$$p(b|x,y) = p(b|y). \tag{6.24}$$

Note that another way to write the no-signaling constraint in (6.23) is $\sum_b p(a,b|x,y) = \sum_b p(a,b|x,y')$ for every a,x,y and y'. The no-signaling constraints state that the probability distribution of the outcomes of one party is independent of the inputs of the other party.

The justification of the no-signaling constraints for spacelike separated parties comes from the *causality constraint* of special relativity, according to which one party cannot communicate with another party by sending a superluminal signal, i.e. a signal that travels faster than the speed of light. Indeed, the constraints on the probability distributions of a two-party Bell scenario imposed by causality coincide with (6.23) and (6.24).

The no-signaling constraints are generalized as follows in an N-party Bell scenario [MAG06]:

$$\begin{aligned} &\sum_{a_j} p(a_1,\dots,a_j,\dots,a_N|x_1,\dots,x_j,\dots,x_N) \\ &= \sum_{a_j} p(a_1,\dots,a_j,\dots,a_N|x_1,\dots,x_j',\dots,x_N) \\ &\forall\, j \in \{1,\dots,N\},\ \{a_1,\dots,a_N\}\setminus\{a_j\},\ \{x_1,\dots,x_j,x_j',\dots,x_N\}, \end{aligned} \tag{6.25}$$

stating that the probability distribution of the outcomes of any subset of parties is independent of the inputs of the complementary set of parties. Note that the constraints in (6.25) explicitly express this statement only for subsets of one party each, but the general statement can be deduced from (6.25) [HR19].

Interestingly, the multiparty no-signaling constraints (6.25) do not precisely capture the causality constraints for certain configurations of parties in the Minkowski spacetime (when $N \geq 3$). In other words, one can arrange the parties in spacetime such that the constraints on their probability distributions purely derived from causality are a strict subset of the no-signaling constraints in (6.25) [HR19]. By labelling $\mathcal{NS}$ the set of all possible correlations obeying the no-signaling constraints (6.25) and analogously $\mathcal{R}$ the set of correlations obeying the causality constraints of relativity, we have that: $\mathcal{NS} \subset \mathcal{R}$. We remark that this situation occurs only when the Bell scenario is composed of $N \geq 3$ parties, while for $N = 2$ we have that $\mathcal{NS} \equiv \mathcal{R}$ as stated above.

Considering again the bipartite Bell scenario, the set $\mathcal{Q}$ of quantum correlations is defined by those probability distributions that can be expressed as:

$$p(a, b|x, y) = \mathrm{Tr}\left[\rho_{AB} M_{a|x} \otimes M_{b|y}\right], \tag{6.26}$$

where ρ_{AB} is a quantum state on the joint Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and $M_{a|x}, M_{b|y}$ are POVM elements (c.f. section 2.2) relative to outcomes a, b given the inputs x, y.

Finally, the set $\mathcal{L}$ of local correlations is characterized by probability distributions that can be expressed in terms of an LHV model (6.6).

It is proved that every local correlation is also a quantum correlation, and that every quantum correlation satisfies the no-signaling constraints, as anticipated [Bru+14]. However, with the violation of the CHSH inequality (6.9), we have seen that there are quantum correlations outside the set of local correlations. Moreover, there are no-signaling correlations which are not quantum correlations. For instance, there are no-signaling correlations whose CHSH value S_{CHSH} achieves the algebraic bound of the expression: $S_{\mathrm{CHSH}} = 4$. Conversely, it is shown [Bru+14] that any quantum correlation leads to a CHSH value upper bounded by $2\sqrt{2}$, which is called the *Tsirelson bound*.

Due to these observations, the following strict inclusions hold: $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$.

6.3 From Bell Violation to Security

Whenever a set of probability distributions, e.g. $p(a, b|x, y)$ in the bipartite Bell scenario, violates a Bell inequality, we talk about *Bell violation* and we call the correlations generated by such distributions *non-local*. In this section we clarify the connection between Bell violation and the security of device-independent (DI) quantum cryptographic protocols.

The security of DI protocols, such as DIQKD and DIRG, is guaranteed irrespective of the trustworthiness of the devices used in their implementation. In a DI protocol, each party holds a device modelled as black box producing an output upon receiving an input from the party. By repeating this operation for several rounds, the parties collect a series of outcomes, each related to the input that generated it.

A fraction of the collected outputs forms the secret key shared by the parties in DIQKD and DICKA protocols, or the secret random bitstring in DIRG protocols. The remaining outputs are used to test a Bell inequality with a Bell experiment like the one described in section 6.1.

Performing a Bell test during the execution of a device-independent (DI) protocol is crucial to ensure its security. Indeed, upon observing a Bell violation, the parties can certify that the random outcomes collected during the execution of the protocol are (at least partially) secret, i.e. unknown to a potential eavesdropper (Eve). What is the link between Bell violation and the privacy of the parties' outcomes?

Firstly, observing a Bell violation rules out the possibility that the outcomes collected by the parties have been generated by an LHV strategy (6.6). In particular, this excludes the possibility that the outcomes have been predetermined by Eve by setting up the systems such that the probabilities $p(a|x,\lambda)$ and $p(b|y,\lambda)$ are deterministic functions of x, y and λ: $p(a|x,\lambda), p(b|y,\lambda) \in \{0,1\}$. This ensures that, even if the parties' systems were fabricated by Eve, she could not have predicted all the outcomes observed by the parties during the Bell experiment. This is a good starting point to have a secret string of random bits.

As we discussed in Bell's theorem proof (c.f. section 6.1), quantum theory allows for correlations violating a Bell inequality. Specifically, a Bell violation occurs only when the parties share a quantum entangled state and their measurements are described by non-commuting observables (e.g. $[A_0, A_1] \neq 0$) [Bru+14]. One can thus interpret Bell inequalities –and violation thereof– as device-independent entanglement witnesses [Pir+09].

An important property of entanglement, called *monogamy of entanglement* [CKW00; BKP06], states that if the quantum systems of two parties, say Alice and Bob, are strongly entangled, then a third quantum system shares little entanglement with them. Thanks to this property, upon observing a Bell violation, Alice and Bob are sure that Eve was poorly entangled with their systems and thus has little information on their outcomes. Hence the secrecy of the parties' outcomes is granted. Notably, the monogamy of correlations is not specific to quantum theory, rather it is present in any no-signaling theory leading to non-local correlations [Bru+14].

6.3.1 DIQKD Security under Coherent Attacks

Let us now formalize the intuition provided above on the security of DI protocols. Here we focus on DIQKD protocols, but analogous considerations hold for DICKA and DIRG protocols.

The Bell violation estimated by the parties while running a DIQKD protocol only describes, on average, the amount of non-locality characterizing one protocol round, and in particular a round devoted to the generation of the secret key. This is enough to make a security statement for one round of the protocol. In particular, given the observed Bell violation, one can bound the conditional von Neumann entropy $H(R_A|E)$ of Alice's raw key bit R_A given Eve's side information E, which we already encountered when computing the secret key rates of QKD protocols (c.f. chapter 3). The quantitative tradeoff between Bell violation and conditional entropy is illustrated in section 6.5 for the simplest DIQKD protocol.

However, the validity of the security statement for one round cannot be directly extended to the whole DI protocol and to all its outputs. The reason is that we consider the most general scenario where Eve performs coherent attacks, meaning that she can act differently in the various rounds and so can the devices. In fact, the security of DIQKD follows the same definitions and results reported in section 3.3 for the security of general QKD schemes, where the main quantity to be estimated is the smooth min-entropy $H^{\varepsilon}_{\min}(R^n_A|E)$ of Alice's bits R^n_A given the side information available to Eve (see (3.27)). Here, Eve's side information includes her quantum system correlated with the initial state distributed to the parties' devices, but also the additional side information generated by the untrusted devices during the process.

In standard QKD[2], we have discussed the existence of methods –such as the postselection technique (PST)– which reduce the security proof against coherent attacks to one against collective attacks, i.e. when the behaviour of the devices and the state distributed by Eve is the same in every round (c.f. subsection 3.3.3). In this case, one can focus on proving the security of one protocol round by using the AEP (c.f. (2.62)), which links the min-entropy of an i.i.d. state to the von Neumann entropy of one of its copies.

However, the methods used in standard QKD are not applicable to DIQKD. Recall, for instance, that the PST requires the knowledge of the Hilbert space dimension of the parties' systems, which is clearly not known in DIQKD.

Nevertheless, an important result named *entropy accumulation theorem* (EAT) [DFR16; Arn+18; DF19] allows us to link the security of the whole DIQKD scheme to the security of one round and can be seen as a generalization of the AEP valid for non-i.i.d. rounds. In particular, the protocol rounds considered by EAT are such

[2] In this context, standard QKD refers to non-DI QKD.

that the key bit $R_A^{(i)}$ generated in the i-th round can also depend on what happened in all the previous rounds, but not on the future rounds, which is a meaningful assumption in sequential DIQKD protocols. According to EAT, the amount of entropy accumulated during the described sequential processes, i.e. the smooth min-entropy $H_{\min}^{\varepsilon}(R_A^n|E)$, is at least n times the conditional von Neumann entropy of one round $H(R_A|E)$ evaluated over the observed Bell violation (up to correction factors of order $\sqrt{n}$).

Therefore, our discussion will now focus on quantitatively connecting the conditional von Neumann entropy of one protocol round with the Bell violation observed in the Bell test. In the next two sections we explore this relationship in the context of the simplest example of a DIQKD protocol.

Finally, we remark that these considerations similarly hold for DIRG protocols, where a secret random biststring is extracted from the collected outcomes of one party or more parties, who can be co-located –e.g. located in the same laboratory.

6.4 Device-independent QKD

In this section we summarize the assumptions that still hold in any bipartite DI protocol (the generalization to more parties is straightforward). We then illustrate the most common DIQKD protocol, which is based on the violation of the CHSH inequality [Cla+69]. In the next section we prove the protocol's security by deriving a lower bound on the conditional von Neumann entropy of one round as a function of the observed CHSH violation.

6.4.1 Assumptions

Despite the fact that in a DI scenario no assumption is made on the quantum state shared by the parties, nor on its dimension and measurement, there are still some unavoidable assumptions in place [Mur+19]. Here we list them:

1. Isolated laboratories: No information flows in or out Alice's and Bob's labs except for what is established by the protocol, i.e. the state distribution in each round and the public classical communication between Alice and Bob.

2. Isolated source: The preparation of the states is independent of the measurements performed on them.

3. Trusted classical post-processing: The classical communication is performed over a public authenticated channel and the data is processed with trusted computers.

4. Trusted random number generators: Alice and Bob independently possess a trusted random number generator whose outcomes are only known to the owner.

Note that the complete removal of any of the above assumptions would lead to a strategy where the key is leaked to Eve [Mur+19].

6.4.2 DIQKD Based on the CHSH Inequality

Consider the following DIQKD protocol whose security is based on testing the CHSH inequality [Pir+09; Arn+18]. Alice holds an uncharacterized device with two inputs $x \in \{0,1\}$ and two outputs for each input: $a_x \in \{-1,1\}$. Ideally, upon receiving an input, the device performs a measurement on Alice's portion of an entangled state that she shares with Bob and provides the outcome of the measurement. We emphasize, however, that we do not specify the implementation when proving the protocol's security. Similarly, Bob holds a device with three inputs $y \in \{0,1,2\}$ and two outputs per input $b_y \in \{-1,1\}$.

Before initiating the protocol, Alice and Bob agree on a set of parameters: the total number of rounds M, the probability $p_t \in (0,1)$ with which they perform a test round, the expected CHSH value $S_{\text{exp}} \in (2, 2\sqrt{2}]$ and its tolerated statistical fluctuation $\delta \in (0, 2\sqrt{2}-2)$.

The protocol comprises the following steps[3] [Pir+19]:

1. Alice and Bob perform a test round with probability p_t or a key-generation (KG) round with probability $1-p_t$. The information on which round to perform can be provided to them by a short preshared key (c.f. Remark 5.2). The total number of rounds is M.

2. In a test round Alice (Bob) randomly selects an input $x \in \{0,1\}$ ($y \in \{0,1\}$) on her (his) device and collects the output a_x (b_y), i.e. the parties test the CHSH inequality. In a KG round, Alice (Bob) selects the predefined input $x = 1$ ($y = 2$) and records the output –her (his) raw key bit– in the random variable R_A (R_B).

3. In parameter estimation (PE) the parties reveal the inputs and outputs of every test round to compute the observed CHSH value S:

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \, . \tag{6.27}$$

[3] We remark that there exist more sophisticated versions of the same scheme with an improved secret key rate [Arn+18]. However, since we are not interested in investigating the protocol's performance, we consider this simplified version.

If $S < S_{\exp} - \delta$, the protocol aborts. The parties additionally reveal a fraction of the KG outcomes to estimate the QBER E_{AB}:

$$E_{AB} = \Pr[R_A \neq R_B] \tag{6.28}$$

4. The parties perform one-way error correction (EC): Alice discloses some information on her raw key by communicating it to Bob via the classical public channel. With the information received from Alice, Bob computes a guess of her raw key. If the EC scheme fails, the protocol aborts.

5. The parties distil two secret keys from their error-corrected raw keys by applying a privacy amplification (PA) procedure.

In an ideal implementation of the above scheme, the CHSH inequality is maximally violated, implying that Eve has no information on the generated secret key (section 6.5). In order for this to happen, the parties can e.g. share the pure Bell state $|\Phi^+\rangle$ (6.15) in each round of the protocol. The measurements of Alice and Bob in the test rounds are given by (6.21) and are the same used to maximally violate the CHSH inequality in the example of section 6.1.

In the DIQKD protocol, Bob has an additional setting $y = 2$ that is only used for KG. In order for Bob to have his raw key bits R_B perfectly correlated with Alice's, he must measure the same observable $B_2 = Z$ that Alice measures in a KG round. Indeed, in a KG round Alice measures $A_1 = Z$ (according to (6.21)) and the outcomes of two local Z measurements on the Bell state $|\Phi^+\rangle$ are perfectly correlated.

As explained in the previous section, thanks to EAT the security proof of the described DIQKD protocol in the finite-key scenario is reduced to the computation of the conditional von Neumann entropy $H(R_A|E)$, relative to one protocol round, as a function of the observed CHSH violation S. Note that, since without violation ($S \leq 2$) the estimation of the entropy $H(R_A|E)$ would be $H(R_A|E) = 0$ (see section 6.5), from now one we refer to S as the CHSH *violation* rather than the CHSH *value*.

We point out that the security of the protocol is composable in the sense of the definition given in section 3.3. However this is true only as far as the devices are not reused in another run of the protocol [Pir+19; Mur+19].

In the asymptotic limit ($M \to \infty$) the finite-key effects become negligible and the asymptotic secret key rate constitutes an upper bound on the secret key rate achieved with finite resources [ARV19]. The asymptotic secret key rate of the described DIQKD protocol coincides with the one of standard QKD protocols (3.9) and reads:

$$r = H(R_A|E) - H(R_A|R_B). \tag{6.29}$$

The second term in (6.29) is due to the classical information leaked during EC and can be estimated analogously to standard QKD in terms of the QBER E_{AB} (see (3.25)). However, differently from standard QKD schemes, here the entropy $H(R_A|E)$ is estimated device-independently as a function of the observed CHSH violation. This is the content of the next section.

In a similar fashion, the asymptotic rate of secret bits generated by a DIRG protocol reads:

$$r = H(R_A|E), \tag{6.30}$$

where the term due to EC is removed since the only goal is to produce a secret random bitstring in one specific location.

6.5 Conditional Entropy Bound

We derive a tight analytical lower bound on the conditional von Neumann entropy $H(R_A|E)$, relative to the DIQKD protocol of section 6.4, for a given CHSH violation S. This result yields a lower bound on the protocol's secret key rate both in the finite-key and asymptotic regimes.

The analytical lower bound on $H(R_A|E)$ was first derived in [Pir+09]. This fundamental result allows for analytical expressions of the secret key rates (secret randomness generation rates) of all the DIQKD (DIRG) protocols based on the CHSH inequality or reducible to a CHSH violation (e.g. the DICKA protocol in [RMW19]). Indeed, there is no analytical DIQKD key rate which does not rely on the bound derived in [Pir+09].

There are other ways to lower bound $H(R_A|E)$ in terms of the violation of a given Bell inequality, which are employed when a tight analytical lower bound is not available. A common procedure is to numerically compute the min-entropy $H_{\min}(R_A|E)$ [NPA07; NPA08; NPS14; BSS14] and use the fact that the min-entropy is a lower bound of the von Neumann entropy (see Eq. 2.56). However the bounds derived in this way are fairly loose, leading to poorly-performing DIQKD schemes.

The critical result derived in [Pir+09] is the reduction of the state shared by Alice and Bob in one round of the protocol to a two-qubit state which is diagonal in the Bell basis (3.15). Note that this result is derived assuming i.i.d. rounds in the DIQKD protocol above, i.e. Eve performs collective attacks. Nevertheless, as we discussed, the result can be applied to proving the protocol's security in the most general scenario thanks to EAT.

Theorem 6.1 ([Pir+09]). *Let Alice and Bob perform the DIQKD protocol described in subsection 6.4.2. It is not restrictive to assume that, in each round, Eve distributes a mixture $\sum_\alpha p_\alpha \rho_\alpha$ of two-qubit states ρ_α, together with a flag $|\alpha\rangle$ (known to her) which determines the measurements performed on ρ_α given the parties' inputs. Without loss of generality, the measurements performed by Alice's and Bob's devices on ρ_α are rank-one binary projective measurements in the (x, y)-plane of the Bloch sphere. Moreover, each state ρ_α is diagonal in the Bell basis* (3.15) *and reads:*

$$\rho_\alpha = \sum_{i,j=0}^{1} \lambda_{ij}^\alpha |\psi_{ij}\rangle\langle\psi_{ij}| \quad \textit{with} \quad \lambda_{0j}^\alpha \geq \lambda_{1j}^\alpha \quad \forall\, j \in \{0, 1\}. \tag{6.31}$$

The proof of Theorem 6.1 is given in appendix A.3 and is rearranged in order to coherently fit with the more general result we prove in [Gra+20] (appendix H).

The second crucial ingredient to derive the bound on $H(R_A|E)$ is the analytical expression of the maximal CHSH violation $\mathcal{S}_\rho$ that can achieved on a given two-qubit state ρ. In other words, there exist measurements performed by Alice and Bob on ρ such that the observed CHSH violation is $S = \mathcal{S}_\rho$, and any other measurement setting leads to violations $S \leq \mathcal{S}_\rho$. This is a well-known result derived in [HHH95].

Theorem 6.2 ([HHH95]). *The maximum violation $\mathcal{S}_\rho$ of the CHSH inequality* (6.27)*, attained by a two-qubit state ρ, is given by:*

$$\mathcal{S}_\rho = 2\sqrt{t_0 + t_1} \tag{6.32}$$

where t_0 and t_1 are the largest and second-to-the-largest eigenvalues of the matrix $T_\rho T_\rho^T$, where T_ρ is the correlation matrix of ρ, with elements: $[T_\rho]_{ij} = \mathrm{Tr}[\rho(\sigma_i \otimes \sigma_j)]$ for $i, j = 1, 2, 3$ (σ_i are the Pauli matrices).

For the state ρ_α in (6.31), the maximal CHSH violation reads:

$$\mathcal{S}_\alpha = 2\sqrt{2} \max\left\{\sqrt{(\lambda_{00}^\alpha - \lambda_{11}^\alpha)^2 + (\lambda_{01}^\alpha - \lambda_{10}^\alpha)^2}, \sqrt{(\lambda_{00}^\alpha - \lambda_{10}^\alpha)^2 + (\lambda_{01}^\alpha - \lambda_{11}^\alpha)^2}\right\}. \tag{6.33}$$

We are now ready to derive the lower bound on the conditional entropy $H(R_A|E)$ in terms of the observed CHSH violation S. The derivation provided in this thesis, although based on the same concepts used in [Pir+09], presents further details in order to better guide the reader in the various steps. Moreover, the last step of the proof leading to the final result substantially differs from [Pir+09] as it employs a completely different approach.

To start with, Theorem 6.1 says that we can restrict the computation of the conditional entropy of interest over a mixture of states ρ_α of the form (6.31). We emphasize that the total information available to Eve includes the knowledge of the value α stored in a random variable Ξ, therefore we must compute the conditional entropy $H(R_A|E_{\text{tot}})$, where $E_{\text{tot}} = E\Xi$.

More specifically, the aim is to derive a tight lower bound $F(S)$ of $H(R_A|E_{\text{tot}})$ where F is a function of the observed CHSH violation S. The bound is tight if for every violation S there exist a quantum state and a set of measurements that achieve that violation and whose conditional entropy is exactly given by $F(S)$.

By the argument above[4], we can be express the conditional entropy $H(R_A|E_{\text{tot}})$ as follows:

$$\begin{aligned} H(R_A|E_{\text{tot}}) &= \sum_\alpha p_\alpha H(R_A|E\Xi = \alpha) \\ &= \sum_\alpha p_\alpha H(R_A|E)_{\rho_\alpha}, \end{aligned} \tag{6.34}$$

where $H(R_A|E)_{\rho_\alpha}$ is the conditional entropy of Alice's raw key bit given that Eve distributed the state ρ_α. Similarly, the observed violation S can be written as:

$$S = \sum_\alpha p_\alpha S_\alpha, \tag{6.35}$$

where S_α is the violation that the parties would observe if they were given the state ρ_α in each round.

We can then focus on deriving a tight lower bound on $H(X|E)_{\rho_\alpha}$:

$$H(R_A|E)_{\rho_\alpha} \geq F(S_\alpha), \tag{6.36}$$

where F is a convex function of the violation S_α. Note that the tightness of the bound (6.36) is crucial to obtain a tight bound on $H(R_A|E_{\text{tot}})$. Indeed, by combining (6.34), (6.35), (6.36) and the convexity of F, we get the desired lower bound on $H(R_A|E_{\text{tot}})$ as a function of the observed violation S:

$$H(R_A|E_{\text{tot}}) \geq F(S). \tag{6.37}$$

Remark 6.1. *The task is thus reduced to minimizing the conditional entropy $H(R_A|E)_{\rho_\alpha}$ over all the states ρ_α of the form* (6.31) *(Theorem 6.1), whose CHSH violation S_α is upper bounded by* (6.33) *(Theorem 6.2). In doing so we obtain* (6.36).

We start by providing Eve with the maximum amount of side information (as in every QKD protocol) by assuming that the state on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is pure, i.e.

[4] As a matter of fact, the quantum state on which $H(R_A|E_{\text{tot}})$ is computed is a c.q. state derived from (A.22), which is given in the proof of Theorem 6.1. Recall the formula to compute the conditional entropy of c.q. states: (2.49).

Eve holds the purifying system of ρ_α. Considering that ρ_α is written in its spectral decomposition in (6.31), we have the following pure state on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$:

$$|\phi^\alpha_{ABE}\rangle = \sum_{i,j=0}^{1} \sqrt{\lambda^\alpha_{ij}}\, |\psi_{ij}\rangle \otimes |e_{ij}\rangle\,, \tag{6.38}$$

where $\{|e_{ij}\rangle\}_{i,j=0}^{1}$ is an orthonormal basis in $\mathcal{H}_E$.

We then decompose the entropy $H(R_A|E)_{\rho_\alpha}$ according to the definition of conditional von Neumann entropy:

$$H(R_A|E)_{\rho_\alpha} = H(E|R_A)_{\rho_\alpha} + H(R_A)_{\rho_\alpha} - H(E)_{\rho_\alpha}. \tag{6.39}$$

Due to the fact that the state on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is pure, we can directly compute $H(E)_{\rho_\alpha}$ as follows:

$$H(E)_{\rho_\alpha} = H(AB)_{\rho_\alpha} = H(\{\lambda^\alpha_{ij}\}), \tag{6.40}$$

where the entropy on the r.h.s. is the Shannon entropy of the probability distribution defined by the eigenvalues λ^α_{ij} of ρ_α. Indeed, the eigenvalues of a density operator sum to one and are non-negative, due to the normalization and positivity of the density operator.

Note that the entropies in (6.39) are computed on the quantum state $\rho^\alpha_{R_A E}$ obtained by applying Alice's projective measurement corresponding to input $x = 1$ (the input for KG) on the pure state $|\phi^\alpha_{ABE}\rangle$ and by tracing out Bob's system. According to Theorem 6.1, Alice's measurement is described by a quantum operation $\mathcal{E}_{R_A}$ which projects on the eigenstates $\{|a\rangle\}_{a=0}^{1}$ of a generic observable in the (x, y)-plane: $A = \cos(\varphi)X + \sin(\varphi)Y$, with $\varphi \in [0, 2\pi]$. The eigenstates of A are given by:

$$|a\rangle_{R_A} = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a e^{\mathbb{i}\varphi}\, |1\rangle), \tag{6.41}$$

and the corresponding measurement outcomes are defined as $a = 0, 1$ ($a = 0$ corresponds to eigenvalue $+1$ and $a = 1$ to eigenvalue -1). The state $\rho^\alpha_{R_A E}$ thus reads:

$$\begin{aligned}
\rho^\alpha_{R_A E} &= (\mathcal{E}_{R_A} \otimes \mathrm{id}_E)\, \mathrm{Tr}_B\, [|\phi^\alpha_{ABE}\rangle\langle\phi^\alpha_{ABE}|] \\
&\overset{(6.38)}{=} \sum_{a=0,1} |a\rangle\langle a|_{R_A} \otimes \sum_{i,j,k,l=0,1} \sqrt{\lambda^\alpha_{ij}\lambda^\alpha_{kl}}\, \mathrm{Tr}_B[\langle a|\psi_{ij}\rangle\, \langle\psi_{kl}|a\rangle]|e_{ij}\rangle\langle e_{kl}|_E \\
&=: \frac{1}{2} \sum_{a=0,1} |a\rangle\langle a|_{R_A} \otimes \rho^{\alpha,a}_E,
\end{aligned} \tag{6.42}$$

where we defined the normalized conditional state of Eve $\rho^{\alpha,a}_E$, given that Alice's raw key bit is equal to a.

The matrix representing $\rho_E^{\alpha,a}$ in the orthonormal basis $|e_{ij}\rangle$ is given by the following Hermitian matrix[5]:

$$\rho_E^{\alpha,a} = \begin{bmatrix} \lambda_{00}^{\alpha} & 0 & (-1)^a\sqrt{\lambda_{00}^{\alpha}\lambda_{01}^{\alpha}}\cos\varphi & (-1)^{a+1}\sqrt{\lambda_{00}^{\alpha}\lambda_{11}^{\alpha}}\,\mathbb{i}\sin\varphi \\ & \lambda_{10}^{\alpha} & (-1)^a\sqrt{\lambda_{10}^{\alpha}\lambda_{01}^{\alpha}}\,\mathbb{i}\sin\varphi & (-1)^{a+1}\sqrt{\lambda_{10}^{\alpha}\lambda_{11}^{\alpha}}\cos\varphi \\ & & \lambda_{01}^{\alpha} & 0 \\ & & & \lambda_{11}^{\alpha} \end{bmatrix}, \tag{6.43}$$

with non-zero eigenvalues that are independent of a and given by:

$$\eta_{\pm}(\varphi) = \frac{1}{2}\left[1 \pm \sqrt{(\lambda_{00}^{\alpha}-\lambda_{10}^{\alpha})^2 + (\lambda_{01}^{\alpha}-\lambda_{11}^{\alpha})^2 + 2(\lambda_{00}^{\alpha}-\lambda_{10}^{\alpha})(\lambda_{01}^{\alpha}-\lambda_{11}^{\alpha})\cos(2\varphi)}\right]. \tag{6.44}$$

From (6.42), one immediately deduces that the reduced state on $\mathcal{H}_{R_A}$ is: $\rho_{R_A} = (1/2)\sum_{a=0,1}|a\rangle\langle a|$, hence its entropy is maximal:

$$H(R_A)_{\rho_\alpha} = 1. \tag{6.45}$$

Moreover, by exploiting the fact that the state $\rho_{R_A E}^{\alpha}$ in (6.42) is a c.q. state, we can recast the expression for the entropy $H(E|R_A)_{\rho_\alpha}$ as follows (c.f. (2.49)):

$$H(E|R_A)_{\rho_\alpha} = \frac{1}{2}\left(H(\rho_E^{\alpha,0}) + H(\rho_E^{\alpha,1})\right). \tag{6.46}$$

Now, the von Neumann entropy of the states $\rho_E^{\alpha,a}$ (for $a = 0,1$) is simply given by the Shannon entropy of their eigenvalues (6.44). The entropy $H(E|R_A)_{\rho_\alpha}$ is thus given by:

$$H(E|R_A)_{\rho_\alpha} = h(\eta_+(\varphi)), \tag{6.47}$$

where we used the definition of binary entropy (2.43) and the fact that the eigenvalues of a quantum state sum to one.

Note that the entropy in (6.47) depends on the angle φ which determines the direction of Alice's KG measurement in the (x,y)-plane of the Bloch sphere. Since in a DI scenario we do not have any information on the measurement direction, we have to consider the worst-case scenario, i.e. the direction that minimizes Eve's uncertainty represented by $H(E|R_A)_{\rho_\alpha}$. The function in (6.47) is clearly minimized for $\varphi = 0$ and simplifies to:

$$H(E|R_A)_{\rho_\alpha} = h(\lambda_{00}^{\alpha} + \lambda_{01}^{\alpha}), \tag{6.48}$$

[5] The missing entries are fixed by the fact that the matrix is Hermitian.

By substituting the results (6.40), (6.45) and (6.48) into (6.39), we can express the entropy $H(R_A|E)_{\rho_\alpha}$ to be minimized as follows:

$$H(R_A|E)_{\rho_\alpha} = 1 - H(\{\lambda_{ij}^\alpha\}) + h(\lambda_{00}^\alpha + \lambda_{01}^\alpha). \tag{6.49}$$

We can now formulate the optimization problem (stated in Remark 6.1) whose solution is the lower bound on $H(R_A|E)_{\rho_\alpha}$ (6.36). The optimization problem reads as follows:

$$\begin{aligned} F(S_\alpha) := \min_{\{\lambda_{ij}^\alpha\}} \, & 1 - H(\{\lambda_{ij}^\alpha\}) + h(\lambda_{00}^\alpha + \lambda_{01}^\alpha) \\ \text{sub. to} \quad & \mathcal{S}_\alpha \geq S_\alpha \ ; \ \lambda_{0j}^\alpha \geq \lambda_{1j}^\alpha \ ; \ \sum_{i,j=0,1} \lambda_{ij}^\alpha = 1, \end{aligned} \tag{6.50}$$

and its detailed solution is given in appendix A.4. We remark that our solution is based on a completely different approach with respect to the original derivation in [Pir+09]. Indeed, our derivation is inspired by similar proofs contained in our recent work [Gra+20] where we extend the results of this section to multiparty scenarios. For this, the analytical solution of the optimization in (6.50) provided in appendix A.4 can be regarded as a new result exclusive to this thesis.

The solution of the above optimization is given by:

$$F(S_\alpha) = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{S_\alpha}{2}\right)^2 - 1}\right), \tag{6.51}$$

which is a convex function as required by (6.37). Hence, by employing (6.51) in (6.37), we finally obtain the lower bound on the conditional von Neumann entropy of Alice's raw key bit as a function of the observed CHSH violation S:

$$H(R_A|E_{\text{tot}}) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{S}{2}\right)^2 - 1}\right). \tag{6.52}$$

By employing the derived bound e.g. in the asymptotic secret key rate (6.29) of the described DIQKD protocol, one can obtain a lower bound on the achievable key rate in terms of the observed CHSH violation S. We stress the fact that the bound in (6.52) plays a crucial role in obtaining an analytical expression for the secret key rate of any DIQKD protocol based on the CHSH inequality.

6.5.1 Privacy Certification in Standard- and DI-QKD

The conditional entropy bound in (6.52) can be seen as a quantitative certification of the privacy of Alice's key bit, in the context of a DIQKD protocol based on the CHSH inequality. It is interesting to compare this result with the analogous privacy certification (conditional entropy bound) used in a standard QKD protocol, namely the BB84 protocol studied in section 3.2.

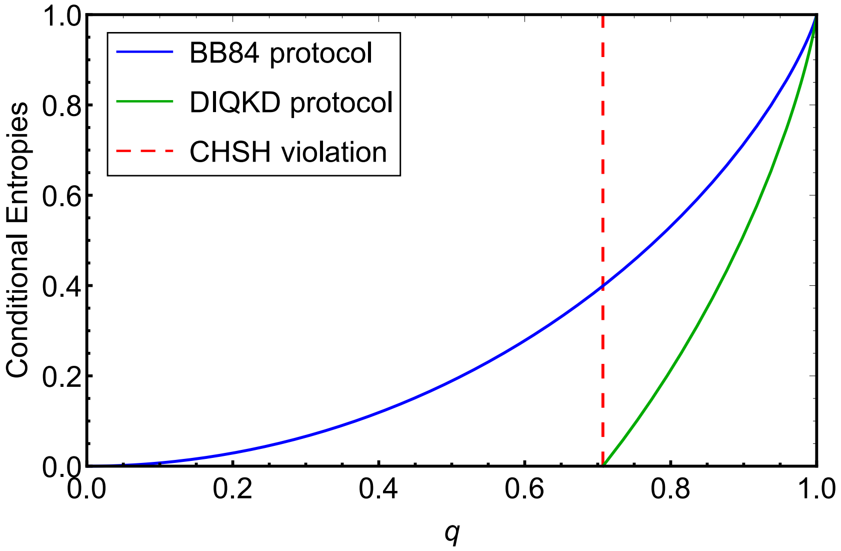

Fig. 6.2.: Conditional von Neumann entropy $H(R_A|E)$ certified by a CHSH-based DIQKD protocol (green line, Eq. 6.54) and by a BB84 protocol (blue line, Eq. 6.55), as a function of the mixing parameter q of the depolarized Bell state (6.53) shared by Alice and Bob. We observe that, opposed to the BB84 protocol, the conditional entropy of the DIQKD protocol is non-zero only when the parties share a state that leads to a CHSH violation.

In order to carry out a fair comparison, we set equal grounds for the DIQKD protocol and the BB84 protocol. In particular, we have seen that the ideal resource state distributed in each round to Alice and Bob is the Bell state $|\Phi^+\rangle$ for both protocols (see (6.15) and (3.7)). In a more realistic scenario, the pure state $|\Phi^+\rangle$ undergoes a depolarizing channel (c.f. subsection 2.5.1) generating the following mixed state:

$$\rho_{AB} = q|\Phi^+\rangle\langle\Phi^+|+(1-q)\frac{\mathrm{id}_A \otimes \mathrm{id}_B}{4}. \qquad (6.53)$$

We thus assume that in both protocols the state in (6.53) is distributed to Alice and Bob in every round. Then, in the DIQKD protocol the observed Bell violation reads $S = 2\sqrt{2}q$ when the parties perform the measurements given in (6.21) which are optimal[6] for the Bell state $|\Phi^+\rangle$.

[6] Note that the maximally mixed state in (6.53) does not contribute to the violation S.

This leads to the following conditional entropy bound (6.52) for the DIQKD protocol:

$$H(R_A|E)_{\mathrm{DIQKD}} = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{2q^2 - 1}\right). \tag{6.54}$$

In the entanglement-based BB84 protocol described in section 3.2, Alice and Bob perform measurements in the Z basis for key generation and in the X basis to estimate Eve's knowledge. The QBER in the X basis, given that they share the state in (6.53), reads: $E_X = (1 - q)/2$. This leads to the following conditional entropy bound (3.24) for the BB84 protocol:

$$H(R_A|E)_{\mathrm{BB84}} = 1 - h\left(\frac{1 - q}{2}\right). \tag{6.55}$$

We emphasize that DIQKD removes most of the assumptions on the measurement devices that typically hold in a BB84 protocol, where the additional assumptions need to be verified experimentally. However, the price to pay is a reduced capability of certifying the privacy of Alice's bit compared to the BB84 protocol, given that the parties share the same quantum state.

This is clear from figure 6.2, where we plot the conditional entropy bound of the DIQKD protocol (6.54) and of the BB84 protocol (6.55) as a function of the mixing parameter q of the depolarizing channel. Indeed, in the BB84 protocol Eve's uncertainty on Alice's bit is non-zero as soon as a fraction of the shared state is an entangled state. Conversely, in the DIQKD protocol Eve's uncertainty is only certified in the presence of a CHSH violation, which requires a much larger fraction of entanglement in the shared state ($q > 1/\sqrt{2}$).

6.6 Entropy Bounds for Multipartite Device-independent Cryptography

As anticipated in the previous section, we recently generalized Theorems 6.1 and 6.2 to multiparty DI scenarios [Gra+20] (also in appendix H). Our results allow for the derivation of analytical bounds on conditional entropies of interest for DIRG and DICKA protocols.

Consider a DI scenario with N parties that are denoted Alice$_1$, ..., Alice$_N$ for simplicity. In performing a DI protocol, the parties test a generic full-correlator Bell inequality [Bel04; WW01] with two dichotomic observables $A_x^{(i)}$ ($x = 0, 1$) per party ($i = 1, \ldots, N$). We call this an $(N, 2, 2)$ Bell scenario. A full-correlator Bell inequality is an inequality whose correlators always involve every party, i.e. they are of the form:

$$\left\langle A_{x_1}^{(1)} \cdots A_{x_N}^{(N)} \right\rangle. \tag{6.56}$$

From the observed Bell violation, the parties can certify the privacy of their outcomes by computing an appropriate conditional von Neumann entropy and thus determine the asymptotic rate of secret random bits generated by their DIRG or DICKA protocol.

In order to illustrate the generalized state reduction valid for an arbitrary $(N, 2, 2)$ Bell scenario, we first define the generalization of the Bell basis (3.15) in an N-qubit space [Epp+17].

Definition 6.1. *The GHZ basis is composed of the following 2^N states:*

$$|\psi_{\sigma,\vec{u}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\,|\vec{u}\rangle + (-1)^{\sigma}\,|1\rangle\,|\bar{\vec{u}}\rangle\right), \tag{6.57}$$

where $\sigma \in \{0,1\}$ while $\vec{u} \in \{0,1\}^{N-1}$ and $\bar{\vec{u}} = \vec{1} \oplus \vec{u}$ are $(N-1)$-bit strings.

We can now state our generalization of Theorem 6.1 to an $(N, 2, 2)$ Bell scenario.

Theorem 6.3 ([Gra+20])**.** *Consider N parties testing an $(N, 2, 2)$ full-correlator Bell inequality. It is not restrictive to assume that, in each round, Eve distributes a mixture $\sum_{\alpha} p_{\alpha}\rho_{\alpha}$ of N-qubit states ρ_{α}, together with a flag $|\alpha\rangle$ (known to her) which determines the measurements performed on ρ_{α} given the parties' inputs. Without loss of generality, the measurements performed by each device on ρ_{α} are rank-one binary projective measurements in the (x, y)-plane of the Bloch sphere. Moreover, each state ρ_{α} is diagonal in the GHZ basis, except for some purely imaginary off-diagonal terms:*

$$\rho_{\alpha} = \sum_{\vec{u}\in\{0,1\}^{N-1}} \lambda^{\alpha}_{0\vec{u}}|\psi_{0,\vec{u}}\rangle\langle\psi_{0,\vec{u}}|+\lambda^{\alpha}_{1\vec{u}}|\psi_{1,\vec{u}}\rangle\langle\psi_{1,\vec{u}}|+\mathbb{i}s^{\alpha}_{\vec{u}}\left(|\psi_{0,\vec{u}}\rangle\langle\psi_{1,\vec{u}}|-|\psi_{1,\vec{u}}\rangle\langle\psi_{0,\vec{u}}|\right). \tag{6.58}$$

Finally, N arbitrary off-diagonal terms $s^{\alpha}_{\vec{u}}$ can be assumed to be zero. Independently, N pairs of the form $(\lambda^{\alpha}_{0\vec{u}}, \lambda^{\alpha}_{1\vec{u}})$ can be arbitrarily ordered (e.g. $\lambda^{\alpha}_{0\vec{u}} \geq \lambda^{\alpha}_{1\vec{u}}$).

We remark that Theorem 6.3 reduces to Theorem 6.1 when one considers the CHSH Bell scenario ($N = 2$).

The second main tool to derive conditional entropy bounds is an analytical expression for the maximal violation of the considered Bell inequality achievable by a given state (e.g. Theorem 6.2 in section 6.5). In [Gra+20] we derive such a result for a specific $(N, 2, 2)$ full-correlator inequality, namely the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [Mer90; Ard92; BK93]. The MABK inequality is a multiparty generalization of the CHSH inequality and is obtained on the following MABK operator.

Definition 6.2. *The MABK operator M_N is defined by recursion [Col+02; RMW18]:*

$$\begin{aligned} M_2 &= G_{\text{CHSH}}(A_0^{(1)}, A_1^{(1)}, A_0^{(2)}, A_1^{(2)}) \\ &\equiv A_0^{(1)} \otimes A_0^{(2)} + A_0^{(1)} \otimes A_1^{(2)} + A_1^{(1)} \otimes A_0^{(2)} - A_1^{(1)} \otimes A_1^{(2)} \\ M_N &= \frac{1}{2} G_{\text{CHSH}}(M_{N-1}, \overline{M_{N-1}}, A_0^{(N)}, A_1^{(N)}), \end{aligned} \tag{6.59}$$

where $A_x^{(i)}$ $(i = 0, 1)$ is the x-th binary observable of Alice$_i$ and where $\overline{M_l}$ is the operator obtained from M_l by replacing every observable $A_x^{(i)}$ with $A_{1-x}^{(i)}$.

Then the N-partite MABK inequality reads as follows:

$$\langle M_N \rangle = \text{Tr}[M_N \rho] \leq \begin{cases} 2, & \text{classical bound} \\ 2^{N/2}, & \text{GME threshold} \\ 2^{(N+1)/2} & \text{quantum bound} \end{cases} \tag{6.60}$$

where M_N is the MABK operator and a violation of the GME threshold implies that the parties share a genuine multipartite entangled (GME) state (c.f. Definition 2.4).

We now present the upper bound on the maximal N-partite MABK violation derived in [Gra+20]. This result can be seen as a generalization of Theorem 6.2 since the latter is recovered for $N = 2$.

Theorem 6.4 ([Gra+20])**.** *The maximum violation $\mathcal{M}_\rho$ of the N-partite MABK inequality* (6.60)*, attained by rank-one projective measurements on a given N-qubit state ρ, satisfies*

$$\mathcal{M}_\rho \leq 2\sqrt{t_0 + t_1} \tag{6.61}$$

where t_0 and t_1 are the largest and second-to-the-largest eigenvalues of the matrix $T_\rho T_\rho^T$, where T_ρ is the correlation matrix of ρ.

The correlation matrix of an N-qubit state can be defined as follows.

Definition 6.3. *The correlation matrix T_ρ of an N-qubit state ρ is defined by the matrix elements $[T_\rho]_{ij} = \text{Tr}[\rho \sigma_{\nu_1} \otimes \ldots \otimes \sigma_{\nu_N}]$ such that:*

$$\begin{aligned} i &= 1 + \sum_{k=1}^{\lceil N/2 \rceil} 3^{\lceil N/2 \rceil - k}(\nu_k - 1) \\ j &= 1 + \sum_{k=\lceil N/2 \rceil + 1}^{N} 3^{N-k}(\nu_k - 1) \end{aligned} \tag{6.62}$$

where $\nu_1, \ldots, \nu_N \in \{1, 2, 3\}$, $\sigma_1 = X$, $\sigma_2 = Y$ and $\sigma_3 = Z$ are the Pauli matrices and $\lceil x \rceil$ returns the smallest integer greater or equal to x.

We remark that the upper bound on the maximal MABK violation in Theorem 6.4 is only tight on certain classes of states, differently from its bipartite counterpart, Theorem 6.2. Nevertheless, it still enables us to derive *tight* conditional entropy bounds, as we discuss below. Opposed to Theorem 6.2, Theorem 6.4 also restricts the measurements on each qubit to rank-one projective measurements (defined by combinations of Pauli operators) in agreement with the result of Theorem 6.3, thus excluding the identity as a viable observable. Note that for $N = 2$ the identity would not lead to any violation [HHH95], hence Theorem 6.4 effectively reduces to Theorem 6.2.

To the best of our knowledge, Theorem 6.4 is the first result of such kind valid for an N-partite Bell inequality. Recently a similar bound was derived in the $N = 3$ case [SS19]. However, our bound is proved to be tight on a larger set of states and is valid for an arbitrary number of parties N.

6.6.1 Conditional Entropy Bounds for Three Parties

Equipped with the results of Theorems 6.3 and 6.4, we are able to obtain analytical bounds on conditional von Neumann entropies that are relevant for the security of certain DI protocols [Gra+20].

Specifically, we consider the $(3, 2, 2)$ Bell scenario where Alice, Bob and Charlie test the tripartite MABK inequality in order to certify the privacy of some of their outcomes, by deriving lower bounds on suitable conditional von Neumann entropies. In particular, we obtain bounds on the conditional von Neumann entropies $H(R_A|E)$ and $H(R_A R_B|E)$ as a function of the observed MABK violation. The bounds derivation is similar to the one described in section 6.5 for two parties, although it presents additional difficulties due to the increased number of parties and outcomes. The details can be found in appendix H, where our work [Gra+20] is reported.

We recall that the entropy $H(R_A|E)$ determines the asymptotic rate of secret random bits generated at Alice's location by a multiparty DIRG or DICKA protocol[7] [DFR16; BRC20]. Similarly, the bound on the entropy $H(R_A R_B|E)$ can represent the rate at which co-located parties generate DI global randomness from Alice and Bob's outcomes [DFR16; WBA18].

In figure 6.3 we plot the derived lower bounds on $H(R_A|E)$ and $H(R_A R_B|E)$ as a function of the observed MABK violation. The analytical expressions corresponding to the plotted curves can be found in appendix H. Some comments are due.

Firstly, the lower bound on $H(R_A|E)$ is tight and in [Gra+20] we provide the family of states that attains the bound for every value of the violation. In [Gra+20]

[7] In a DICKA protocol, the asymptotic conference key rate is given by $H(R_A|E)$ from which one subtracts the information leaked during error correction.

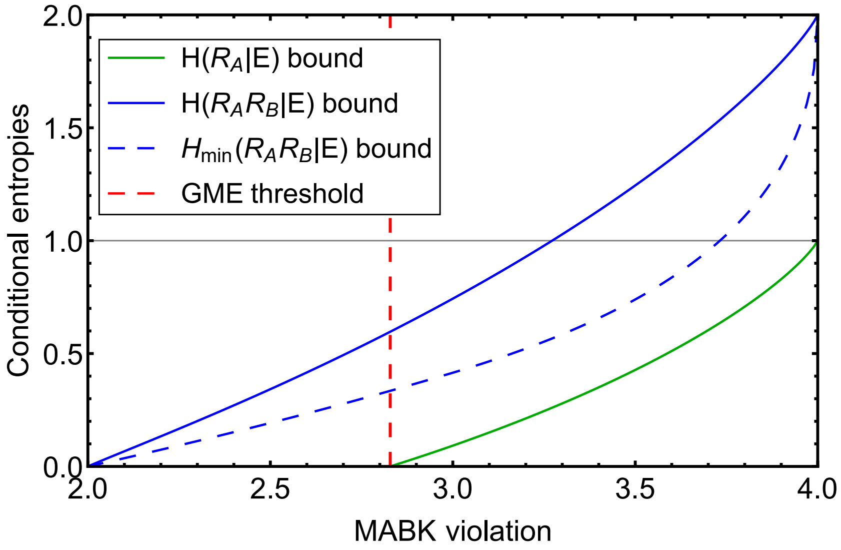

Fig. 6.3.: Lower bounds on the conditional von Neumann entropies $H(R_A|E)$ and $H(R_AR_B|E)$ and on the conditional min-entropy $H_{\text{min}}(R_AR_B|E)$ as a function of the MABK violation observed by three parties. We notice that Eve has full information on Alice's outcome R_A for violations below the GME threshold (green line). Moreover, bounding Eve's uncertainty on Alice and Bob's outcomes with the suitable von Neumann entropy (blue solid line) brings a substantial advantage compared to bounding the correspondent min-entropy (blue dashed line). The analytical expressions relative to the plotted curves can be found in [Gra+20].

we additionally present a tight lower bound on $H(R_A|E)$ when an arbitrary number of parties N test the N-partite MABK inequality.

From figure 6.3 we observe that the lower bound on $H(R_A|E)$ is null for violations of the tripartite MABK inequality below the GME threshold. This characteristic is shared by the N-party lower bound on $H(R_A|E)$, which is null for violations below the N-partite GME threshold.

Given that the bounds on $H(R_A|E)$ are tight, this implies that GME is necessary to certify the privacy of a party's outcome in any DI scenario based on the MABK inequality. Being the latter a prerequisite of any DICKA protocol (not necessarily based on the MABK inequality), it is an open question whether GME is necessary for a successful implementation of a DICKA protocol.

The lower bound on the von Neumann entropy $H(R_AR_B|E)$ is plotted in figure 6.3 together with a tight analytical lower bound on the correspondent min-entropy $H_{\text{min}}(R_AR_B|E)$, derived in [WBA18][8]. There is a significant improvement in certifying the privacy of Alice and Bob's outcomes, from a given MABK violation, with our bound on the von Neumann entropy, as opposed to using the more accessible

[8] We remark that the min-entropy is often used to lower bound the von Neumann entropy in DI protocols, since it can be directly estimated from the observed statistics of the Bell test [NPA07; NPA08; NPS14; BSS14] and since Eq. (2.56) holds.

min-entropy. This has a direct impact on the performance of DI (global) randomness generation protocols, since it increases the fraction of generated random bits proved to be secret.

The last observation demonstrates the potential of our analytical approach in bounding the von Neumann entropies of interest in DI protocols. In particular, the developed techniques could pave the way for similar results valid for the Bell inequalities employed in the existing DICKA protocols [RMW19; HKB19]. In this context, the derivation of tight analytical bounds on the von Neumann entropy would translate to tight security proofs, which are still missing, and to increased protocol performance.

6.7 Device-independent Conference Key Agreement

In this section we argue on the potential applicability of the conditional entropy bounds of section 6.6 to the security proofs of DI conference key agreement (DICKA) protocols. In particular, we investigate the relationship between the structure of full-correlator Bell inequalities and the task of DICKA. We conclude the chapter by providing an example of multipartite Bell inequality suited to DICKA protocols [HKB19].

6.7.1 Full-correlator Bell inequalities and DICKA

All the results presented in section 6.6 stem from the consideration of a Bell scenario with two distinctive features: every party can measure two binary observables and the Bell inequality is only composed of full-correlators. These two features can be exploited –as in [Gra+20]– to drastically simplify the state shared by the parties without loss of generality and in a DI fashion. While the first feature allows the reduction to qubits, the second enables further simplifications on the multi-qubit state shared by the parties (for a reference, see section 6.5).

Here we would like to provide an argument suggesting that any multipartite full-correlator Bell inequality with two binary measurements per party –e.g. the MABK inequality– seems to be incompatible with the task of DICKA. We stress the fact that this is still an open question in the scientific community and there is not yet a formal proof which confirms or disproves the above statement. More details on this argument can be found in [Gra+20].

The secret conference key rate yielded by a generic N-partite DICKA protocol performed by Alice$_1$, …, Alice$_N$, in the asymptotic limit, reads [RMW18; HKB19]:

$$r_{\mathrm{DICKA}} = H(R_{A_1}|E) - \max_{2\leq i\leq N} H(R_{A_1}|R_{A_i}). \tag{6.63}$$

The second term in (6.63) is due to EC (see subsection 3.4.1) and represents the fact that Alice$_i$ for $i = 2, \dots, N$ corrects her raw key to match Alice$_1$'s raw key. The conditional entropy $H(R_{A_1}|E)$ quantifies Eve's uncertainty on Alice$_1$'s key bits, which compose the secret conference key shared by all the parties after EC and PA. As we discussed in the previous section, the entropy $H(R_{A_1}|E)$ can be bounded when the parties observe a violation of an N-partite Bell inequality.

In light of the key rate expression (6.63), a DICKA protocol is successful (it can yield a positive key rate) when the following two events take place. The test-round data leads to a significant violation of a multiparty Bell inequality ($H(R_{A_1}|E)$ is large) and the parties' raw keys are sufficiently correlated ($H(R_{A_1}|R_{A_i})$ are small).

In the DIQKD protocol based on the CHSH inequality and illustrated in subsection 6.4.2, one of the two test inputs of Alice is also used for key generation (KG), while Bob has a third additional input only devoted to KG. This fact is necessary in any DIQKD or DICKA protocol [Hol+19; HKB19]. In a DICKA protocol, we consider that Alice$_1$ plays the role of Alice, i.e. she is the only party without an input (observable) exclusively dedicated to KG.

If even Alice$_1$ had an additional setting only for KG, Eve –who manufactures the devices– would be able to distinguish a test round from a KG round on all the devices. Then, she could equip the devices with a maximally entangled state and suitable test-round measurements so that the parties would observe a maximal violation of the Bell inequality under test. Additionally, Eve could preprogram the devices to always output the same bit when the parties use their KG inputs, so that they would also have perfectly correlated raw keys. In doing so, Eve would be able to learn the whole conference key without being noticed.

The above argument implies that in an honest implementation of a DICKA protocol, the distributed quantum state and the chosen Bell inequality are such that the parties can have highly correlated outputs *while* violating the Bell inequality. Ideally, in an error-free implementation, it should be possible to maximally violate the Bell inequality and at the same time observe perfect correlations of the parties' raw keys. Indeed, this would maximize the protocol's asymptotic secret key rate (6.63) to: $r_{\mathrm{DICKA}} = 1$.

Let us now consider a DICKA protocol based on the violation of a full-correlator Bell inequality with two binary observables per party. Here we heuristically argue that, for such DICKA protocols, it is forbidden to simultaneously have maximal Bell violation in the test rounds and perfect correlations in the KG rounds.

Given that the Bell inequality under consideration has two binary observables per party, we can restrict the analysis to multi-qubit states (c.f. section 6.5). Then, we recall from subsection 3.4.1 that the only multi-qubit state leading to perfectly correlated outcomes is the GHZ state (3.31) where every party measures the Pauli operator Z. If a party instead measures the operator X or Y, she would obtain a completely uncorrelated outcome. Therefore, we assume that the parties share a GHZ state and in the KG rounds every party measures the observable Z. In particular, this fixes one of Alice$_1$'s test-round observables to be Z.

In [WW01], the authors show that every full-correlator Bell inequality with two binary observables per party is maximally violated by the GHZ state. However, we argue that in order to achieve maximal violation, the measurements must be chosen such that the resulting inequality (after simplifications) is only composed of expectation values of GHZ stabilizers (e.g. Eq. 6.22). Indeed, they acquire the extremal value 1 when evaluated on the GHZ state. Moreover, the stabilizers appearing in the inequality cannot contain the identity operator since that would not generate maximal violation. We identify these stabilizers as "full-stabilizers".

Unfortunately, all the observables of every N-partite GHZ state full-stabilizer (with N odd) are either the X or Y Pauli operators [TG05]. Therefore, in order to maximally violate the inequality, Alice$_1$'s test-round observables lie in the (x, y)-plane of the Bloch sphere and have null Z component. This requirement collides with the fact that one of Alice$_1$'s two observables is fixed to Z in order to have perfect correlations in KG rounds. A similar argument can be made for the N even case[9].

Apparently, perfect correlations and maximal Bell violation are mutually exclusive conditions in any DICKA protocol based on a full-correlator Bell inequality with two binary observables per party, even for an ideal implementation of the protocol.

We emphasize that this argument, even if proven to be true, does not rule out the existence of implementations where the parties observe an adequate Bell violation while having reasonably correlated raw keys. However, it is an open question whether such implementations exist and lead to non-zero conference key rates.

We point out that in [Hol+19] the authors have already discussed the apparent incompatibility of the tripartite MABK inequality with the task of DICKA. Indeed, they show that there exists no implementation such that the parties' outcomes are perfectly correlated and concurrently the MABK inequality is violated above the GME threshold, which is a necessary condition to ensure the privacy of the established key (c.f. subsection 6.6.1).

In conclusion, the conditional entropy bounds presented in section 6.6 are not likely to find direct application in the security of DICKA protocols. Nevertheless, since in DIRG the requirement of perfect correlations is dropped, they can still be employed in tight security proofs of DIRG protocols. Moreover, the techniques that

[9] The $N = 2$ case includes the CHSH inequality that *can* be violated with Alice measuring Z, as we have seen in section 6.4.2. However this is a degenerate case due to the low number of parties, as discussed in [Gra+20].

led to the entropy bounds can inspire similar derivations which are relevant for the Bell inequalities used in current DICKA protocols [RMW19; HKB19].

6.7.2 A Bell Inequality tailored to DICKA

We conclude the chapter by presenting a multipartite Bell inequality specifically designed to achieve both perfect correlations and maximal violation in an error-free implementation of a DICKA protocol. The Bell inequality is characterized by two binary observables per party, like in all the other cases discussed in this thesis. For the argument of the previous subsection, the inequality is not exclusively composed of full-correlators.

The inequality under consideration has been recently introduced in [HKB19] for the general case of N parties and its structure allows it to be maximally violated by an N-partite GHZ state where one of Alice$_1$'s optimal observables is Z. In this way, Alice$_1$'s outcomes are perfectly correlated with the other parties' outcomes, when every party measures Z in the KG rounds and the parties share a GHZ state[10].

Here we focus on the $N=3$ case for simplicity, where we denote the parties as Alice$_1$, Alice$_2$ and Alice$_3$ with observables $A^{(i)}_{x_i}$ for $i=1,2,3$ and $x_i=0,1$. The Bell inequality in this case reads:

$$\langle A^{(1)}_1 A^{(2)}_+ A^{(3)}_+ \rangle - \langle A^{(1)}_0 A^{(2)}_- \rangle - \langle A^{(1)}_0 A^{(3)}_- \rangle - \langle A^{(2)}_- A^{(3)}_- \rangle \leq 1, \tag{6.64}$$

where we defined non-normalized observables $A^{(j)}_\pm = (A^{(j)}_0 \pm A^{(j)}_1)/2$ for $j=2,3$. The maximal quantum violation is given by $3/2$ and is achieved on the tripartite GHZ state (2.27). The density operator relative to the tripartite GHZ state $|\mathrm{GHZ}_3\rangle$ can be expressed in terms of all its stabilizers, similarly to (6.16), as follows [TG05]:

$$\begin{aligned} |\mathrm{GHZ}_3\rangle\langle \mathrm{GHZ}_3 |= \frac{1}{8} & (\mathrm{id}\otimes\mathrm{id}\otimes\mathrm{id} + Z\otimes Z\otimes \mathrm{id} + Z\otimes\mathrm{id}\otimes Z + \mathrm{id}\otimes Z\otimes Z \\ & + X\otimes X\otimes X - X\otimes Y\otimes Y - Y\otimes X\otimes Y - Y\otimes Y\otimes X)\,. \end{aligned} \tag{6.65}$$

The observables of Alice$_2$ and Alice$_3$, $A^{(j)}_x = \vec{\alpha}^{(j)}_x \cdot \vec{\sigma}$ (where $j=2,3$ and $\vec{\sigma} = (X,Y,Z)$), are qubit projective measurements[11] whose directions in the Bloch sphere

[10] We recall that all the parties except for Alice$_1$ are equipped with a third measurement setting only used for KG.

[11] We can restrict to qubit projective measurements since the Bell inequality has two inputs with binary outputs for each party.

are identified by the unit vectors $\vec{\alpha}_x^{(j)}$. Then, the non-normalized observables $A_+^{(j)}$ and $A_-^{(j)}$ read:

$$A_\pm^{(j)} = \vec{\alpha}_\pm^{(j)} \cdot \vec{\sigma} \quad , \quad \vec{\alpha}_\pm^{(j)} := \frac{\vec{\alpha}_0^{(j)} \pm \vec{\alpha}_1^{(j)}}{2} \tag{6.66}$$

and are characterized by orthogonal measurement directions $\vec{\alpha}_+^{(j)} \perp \vec{\alpha}_-^{(j)}$ and by normalizations which depend on each other: $\left|\vec{\alpha}_+^{(j)}\right|^2 + \left|\vec{\alpha}_-^{(j)}\right|^2 = 1$. These constraints must be taken into account when looking for the optimal observables leading to a maximal violation of (6.64).

Starting from the form of the inequality in (6.64), we can easily guess the optimal measurements to be performed on the GHZ state. In doing so, we follow the principle (see Eq. 6.22) that the resulting inequality should be only composed of correlators of the GHZ stabilizers (6.65). Note that the terms in (6.64) which are not full-correlators allow us to use the GHZ stabilizers containing the Z and the identity operator, without introducing the identity as one of the parties' observables. In this way we can impose that one of Alice$_1$'s optimal observables is Z, which is necessary to achieve perfect correlations with the other parties in the KG rounds.

For the arguments above, we choose the following optimal observables:

$$\begin{aligned} A_0^{(1)} &= Z \quad , \quad A_1^{(1)} = X \\ A_-^{(j)} &= -\frac{1}{2}Z \quad , \quad A_+^{(j)} = \frac{\sqrt{3}}{2}X \quad (j = 2, 3), \end{aligned} \tag{6.67}$$

where $A_+^{(j)}$ and $A_-^{(j)}$ have orthogonal directions and Alice$_1$'s optimal observable $A_0^{(1)}$ is the Z operator. By substituting the optimal observables in (6.64) we obtain the maximal quantum violation:

$$\frac{3}{4}\langle XXX\rangle + \frac{1}{2}\langle ZZ\rangle + \frac{1}{2}\langle ZZ\rangle - \frac{1}{4}\langle ZZ\rangle = \frac{3}{2} > 1 \tag{6.68}$$

where all the terms of the inequality are indeed proportional to correlators of the GHZ stabilizers, which yield the value 1 when evaluated on the GHZ state.

The authors in [HKB19] investigate the performance of the DICKA protocol based on the illustrated inequality. The security of the protocol is proven by bounding the single-round von Neumann entropy $H(R_A|E)$ as a function of the violation with rather loose numerical techniques [NPA08; MPA11]. This inevitably leads to a poor performance of the conference key rate. A solution to this problem would be to derive a tight analytical bound on $H(R_A|E)$ similarly to what we did in [Gra+20] and possibly using similar techniques. The bound would guarantee a tight security analysis and hence a better performance.

Finally, we mention that the only other DICKA protocol proposed so far [RMW19] is based on a Bell inequality that can be seen as a particular case of the one introduced in [HKB19] and analysed here in the tripartite case. In particular, the inequality used in [RMW19] is recovered when one imposes that Alice$_i$ for $i \geq 3$ has only one measurement setting at her disposal used for testing, instead of two.

The DICKA protocol proposed in [RMW19] also lacks a tight security proof, and would benefit from a tight analytical bound on $H(R_A|E)$ like the one we derived in [Gra+20].

7 Overview of Results

In this chapter we summarize the scientific contributions resulting from our doctoral research that led to the publication of scientific papers. The original publications are attached in appendices B to H.

Finite-key effects in multipartite quantum key distribution protocols (Appendix B)

In this work [GKB18] we systematically generalize the security definitions of a quantum key distribution (QKD) protocol (c.f. Definitions 3.1-3.3) to the multipartite scenario, thereby introducing the concept of ε-security of a quantum conference key agreement (CKA) protocol.

We devise an N-partite version of the BB84 protocol (N-BB84) where Alice, Bob$_1, \ldots,$ Bob$_{N-1}$ ideally share the N-partite GHZ state (3.31) in every round and generate their raw key bits by measuring in the Z basis. They measure in the X basis in m test rounds and compute the error rate $E_X = \Pr[X_A \neq \prod_{i=1}^{N-1} X_{B_i}]$ (see section 3.4). They also estimate the quantum bit error rate (QBER) in the Z basis E_{AB_i} by using m key-generation rounds.

We prove that the protocol, when combined with an ideal error correction (EC) scheme, is $(2\varepsilon + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}})$-secure, with $\varepsilon = \sqrt{(N-1)\varepsilon_z + \varepsilon_x}$ (ε_z and ε_x are input parameters), as long as the length ℓ of the secret key generated by privacy amplification is upper bounded by (compare with (3.27)):

$$\ell \leq n \left[1 - h\left(E_X + 2\xi(\varepsilon_x, n, m)\right) - \max_{1\leq i\leq N-1} h\left(E_{AB_i} + 2\xi(\varepsilon_z, n, m)\right)\right] - \log\frac{2(N-1)}{\varepsilon_{\mathrm{EC}}} - \log\frac{1-2(N-1)\varepsilon}{2\varepsilon_{\mathrm{PA}}}, \tag{7.1}$$

where n is the number of raw-key bits, $h(p)$ is the binary entropy and $\xi(\varepsilon, n, m)$ is due to statistical fluctuations and reads:

$$\xi(\varepsilon, n, m) := \sqrt{\frac{(n+m)(m+1)}{8nm^2} \ln\frac{1}{\varepsilon}}. \tag{7.2}$$

In a similar fashion, we prove the security of the N-partite six-state protocol (N-six-state) introduced in [Epp+17] and derive its secret key length expression. We compare the secret key rates achieved by the N-BB84 and N-six-state protocols under the action of the depolarizing channel (c.f. section 2.5), taking into account the effects due to finite resources. As expected, the N-six-state protocol outperforms the N-BB84 protocol in the asymptotic limit of infinitely many rounds due to a more complete characterization of the eavesdropper's information. However, for lower number of rounds, the N-BB84 protocol provides higher secret key rates thanks to its tighter security analysis.

Practical decoy-state method for twin-field quantum key distribution (Appendix C)

The maximum distance achieved by point-to-point QKD protocols is fundamentally limited by channel losses and their secret key rates cannot scale better than linearly with the channel transmittance, as proven by the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound (5.1). Twin-field (TF) QKD is arguably the simplest solution to overcome such limitations by placing an untrusted measuring station (relay) in the middle of the quantum channel, where the key is established by single-photon interference events.

In this paper [GC19] we investigate the performance of the improved TF-QKD protocol introduced in [CAL19] (c.f. section 5.3), whose security is based on the estimation of detection statistics (yields) of Fock states sent by the two parties to the relay. The yields estimation is carried out through the decoy-state method (c.f. section 4.2). We derive analytical bounds on several yields appearing in the key rate formula (5.25) assuming that each party uses either two, three or four decoy intensity settings, which are the most relevant cases from an experimental point of view. The bounds enable a closed analytical expression of the secret key rate, which is particularly useful when optimizing the protocol's performance over a large set of parameters, e.g. in the finite-key regime.

By optimizing the secret key rate over the input parameters, we show that the use of two decoy intensity settings per party is enough to beat the PLOB bound. We also show that the secret key rate achieved with four decoy intensity settings is almost indistinguishable from the ideal key rate attained with an infinite number of decoy intensity settings.

Asymmetric twin-field quantum key distribution (Appendix D)

Our work in [GNC19] represents a follow-up publication of [GC19] where we address the asymmetric-loss scenario for the same TF-QKD protocol [CAL19] investigated in the previous paper. Indeed, it is common practice to initially analyse the performance of QKD protocols with an intermediate relay, such as TF-QKD, in a simplified symmetric scenario where the channel losses for the two parties are equal and thus are their optimal laser intensities. However, in a realistic situation the parties might be placed at different distances from the relay and their lasers might be affected by random and independent intensity fluctuations. Therefore, in view of field implementations of TF-QKD, it is crucial to assess its performance in the presence of asymmetric losses and for independent laser intensities of the two parties.

For the above reasons, we derive new analytical bounds on the relevant yields of the TF-QKD scheme in [CAL19] allowing the parties to have independent decoy intensities (a simple example is given in section 5.4). Based on the results of the previous paper [GC19], we consider the cases of two, three or four decoy intensity settings per party. With the derived bounds, we optimize the secret key rate for asymmetric losses and show that a secret key can be extracted even when the losses are highly asymmetric. Moreover, we show that the protocol is considerably robust against independent intensity fluctuations of the parties' lasers.

Conference key agreement with single-photon interference (Appendix E)

Inspired by our works on TF-QKD, in [GKB19] we devise a new CKA where N parties establish a secret conference key by relying on single-photon interference events occurring in a central untrusted relay. We prove the protocol's security according to the definitions introduced in [GKB18] and derive the expression of its conference key length.

The conditional state of the parties' qubits, given that a single-photon interference event occurred, is approximately given by a W-class state (5.38), i.e. a coherent superposition of product states where one qubit is in state $|1\rangle$ of the computational basis and the others are in state $|0\rangle$. This feature makes our protocol the first CKA based on a W-class state instead of a GHZ state, as in the N-partite BB84 and six-state protocols (c.f. section 3.4). Moreover, since only one of the N photons sent by the parties to the central relay is required to arrive in order to have single-photon interference, our CKA is much more robust against high losses –i.e. long distances– than any other CKA protocol based on the GHZ state.

We analyse the protocol's performance in the finite-key regime and for a realistic channel model. In particular, we introduce a generalization of the PLOB bound suited to the multipartite scenario and show that our protocol can overcome it for sufficiently high losses (similarly to TF-QKD surpassing the PLOB bound). Furthermore, we compare the conference key rate achieved by our CKA with that obtained by composing bipartite TF-QKD schemes among pairs of parties on the same experimental setup used for the CKA protocol. In this context, we show that our truly multipartite CKA can be advantageous for certain parameter regimes.

Experimental quantum conference key agreement (Appendix F)

In [Pro+20] we take part to the first experimental realization of a quantum CKA, in collaboration with the EMQL research group in Edinburgh. The experiment enables four parties to establish a secret conference key by implementing the multipartite BB84 protocol we introduce in [GKB18].

In every successful protocol round, the parties receive a four-party GHZ state from a quantum server. The server is composed of two sources of entangled photons pairs at telecommunication wavelength ($1550\,\mathrm{nm}$) supplied by the same mode-locked laser. In each source, photon pairs are produced by type-II spontaneous parametric down conversion embedded in a polarization-based Sagnac interferometer equipped with a half-wave plate and a polarizing beam splitter (PBS)[1]. The interference of the photon pairs in the Sagnac interferometer generates polarization-entangled photons pairs, whose state is described by the Bell state $|\Phi^+\rangle$. Then, one photon from each source interferes in a PBS such that the resulting state of the four photons, post-selected on the events where each output contains a photon (which occurs with probability $1/2$), is the four-party GHZ state.

After interfering one photon per source in the PBS, the four signals are coupled to single-mode fibers of total length up to $50\,\mathrm{km}$ and sent to the four parties. Each party measures the incoming photon either in the Z basis $\{|H\rangle, |V\rangle\}$ for key generation or in X basis $\{(|H\rangle + |V\rangle)/\sqrt{2}, (|H\rangle - |V\rangle)/\sqrt{2}\}$ for parameter estimation, where $|H\rangle$ and $|V\rangle$ represent the horizontal and vertical polarizations of the photon. Only the events with coincident detections in all four detectors are retained, since those correspond to the post-selection of a GHZ state.

Once the distribution of quantum states is completed, the parties perform one-way EC from Alice to the other parties, with a low-density parity-check code (LDPC) adapted to the multipartite scenario. LDPC codes disclose a fixed amount of information only depending on the largest QBER between Alice and any other party, thus reducing the amount of information revealed in multiparty EC (see discussion in section 3.4).

Finally the parties perform privacy amplification by applying an appropriate Toeplitz matrix –a two-universal hash function– on their error-corrected raw keys. As a result, the parties hold an $\varepsilon_{\mathrm{tot}}$-secure conference key of 1.15×10^6 bits, with $\varepsilon_{\mathrm{tot}} = 1.8 \times 10^{-8}$. The established key is used to encrypt an image with one-time pad in order to securely share it among the four parties.

[1] In a polarizing beam splitter, light polarized horizontally is transmitted while light polarized vertically is reflected.

Quantum Conference Key Agreement: A Review (Appendix G)

In this manuscript [Mur+20] we address the quantum cryptographic task of conference key agreement (CKA), also known as multipartite quantum key distribution. While a composition of bipartite quantum key distribution protocols can accomplish the task, genuine multipartite protocols exploiting multipartite quantum correlations can potentially be more efficient and represent a defining feature of future quantum networks. In [Mur+20] we review the existing quantum CKA protocols based on multipartite entanglement, both in the device-dependent and the device-independent scenario.

Analytical entropic bounds for multiparty device-independent cryptography (Appendix H)

Multipartite device-independent (DI) cryptographic protocols include DI randomness generation (DIRG) and DI conference key agreement (DICKA) protocols. The security of DI protocols relies on the ability to carefully bound an appropriate conditional von Neumann entropy as a function of the violation of a multipartite Bell inequality, as discussed in section 6.3.

In [Gra+20] we consider N parties testing a generic full-correlator Bell inequality with two inputs and two outcomes per party. In this context, we significantly simplify the general form of the quantum state shared by the parties in every protocol round, without loss of generality (Theorem 6.3). We then consider a particular Bell inequality, namely the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [Mer90; Ard92; BK93], and derive an upper bound on the maximal MABK violation attained by a given N-qubit state (Theorem 6.4).

With the above results, we derive analytical bounds on the conditional von Neumann entropies that enter the security proofs of tripartite DI protocols based on the MABK inequality. We stress the fact that tighter bounds on the conditional entropies enhance the protocol's noise tolerance and relax the strict experimental requirements typical of DI protocols. In particular, we obtain a tight bound on the conditional entropy of a single party's outcome when three parties test the MABK inequality and extend the bound to N parties. We also derive a bound on the joint conditional entropy of two parties' outcomes and show that our result drastically improves a previous bound on the same quantity (c.f subsection 6.6.1).

Based on our results, we raise interesting open questions on the necessity of genuine multipartite entanglement and the employability of full-correlator Bell inequalities in DICKA protocols.

Conclusion and Outlook

8

The fruitful combination of concepts and ideas from different fields of study, as well as the practical implications for the security of our data, have made quantum cryptography a very active research topic in recent years. In this context a major role is played by quantum key distribution (QKD), which enables information-theoretic secure communication between two users. In a world evermore demanding for connectedness, the need for an equally-secure communication established among several users is going to be satisfied by quantum conference key agreement (CKA).

CKA is only one aspect of a wider vision on how quantum communication will change our lives, with the quantum internet as its most ambitious representative [Kim08; WEH18]. Within this view, future quantum networks will provide on-demand entanglement to any subset of users in the network, allowing the execution of quantum-enabled tasks unachievable with classical means.

Our research, which culminated with this thesis, has contributed to driving the transition of quantum-secured communication beyond the two-user paradigm, from bipartite QKD to CKA.

As a matter of fact, we extended the composable security definitions of QKD to the multipartite scenario [GKB18] allowing the analysis of CKA schemes in the finite-key regime. We introduced two novel CKA protocols [GKB18; GKB19], proved their security and benchmarked their performance with other multipartite QKD schemes and with the iteration of bipartite QKD protocols. We additionally demonstrated the practicality of the first protocol [GKB18] by collaborating to its experimental implementation [Pro+20], which represents the only CKA experiment performed so far. In the context of device-independent (DI) quantum cryptography, we developed theoretical tools allowing the derivation of tight conditional entropy bounds that are crucial for the security of multipartite DI protocols [Gra+20].

The extensive work on multipartite key distribution schemes helped us to develop a comprehensive view of the topic, which supported the creation of the first review on quantum conference key agreement [Mur+20].

Nevertheless, we also investigated the promising bipartite TF-QKD approach, which has arguably become the new benchmark for far-distance QKD. By deriving analytical formulas for certain detection probabilities in realistic scenarios, we showed that TF-QKD is a major candidate for being implemented in near-future quantum networks.

Despite the contributions of this thesis, there is still much to be done in order to concretely make CKA protocols the ultimate solution for secure multi-user communication. Here we briefly outline the research directions stimulated from the results presented in this thesis.

The tools developed in [Gra+20] lay the ground for the derivation of further tight conditional entropy bounds for multipartite DI cryptographic protocols. We remark that a careful estimation of these entropies is of paramount importance for the experimental feasibility of DI protocols, as it increases noise tolerance and relaxes the experimental requirements. Of particular interest are the existing DI conference key agreement (DICKA) protocols [RMW19; HKB19]. Indeed, they currently lack a tight bound on the relevant conditional entropy, which severely penalizes their performance. Based on the results of [Gra+20], one could aim to develop a theoretical framework which enables the derivation of tight conditional entropy bounds for the existing and for future DICKA protocols. This would optimize the security analyses of DICKA protocols and boost their potential application in the upcoming quantum networks.

Another research line that stems from [Gra+20] is the characterization of the essential requirements for DICKA. To be more specific, in [Gra+20] we showed that genuine multipartite entanglement (GME) shared by all the participants is necessary if the inequality being tested is the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [Mer90; Ard92; BK93]. It is unclear, however, if the task of DICKA necessarily needs to rely on GME states. Moreover, in [Gra+20] we raised doubts about the employability of full-correlator Bell inequalities for DICKA protocols. Such open questions could trigger the search for definitive answers which we believe would shed light on novel fundamental aspects of multipartite quantum correlations. In doing so, one could obtain prescriptions that a Bell inequality should fulfil in order to be used in a DICKA protocol, and suggest new DICKA protocols based on Bell inequalities satisfying these conditions.

From an experimental point of view, our CKA experiment [Pro+20] only represents the first step towards a fully fledged CKA which can serve the needs of secure multi-user communication. We point out two aspects that should be addressed to meet such a goal. Firstly, one should increase the generation rate of the distributed multipartite entangled state in order to speed up the resulting secure communication. Additionally, the future field implementation of CKA should be performed in the existing telecommunication infrastructure. This would remove the need for dedicated fiber networks linking the users. Finally, the recent developments in photonic detector efficiencies [Li+18; Zha+19a] and parametric down-conversion sources [Fed+07; Gra+18] open the possibility for an all-photonic implementation of DI cryptographic schemes, paving the way for the application of this technology to future metropolitan quantum networks.

In conclusion, we hope that our doctoral research has supported the on-going process transforming QKD and CKA protocols into concrete cryptographic solutions, and at the same time has stimulated further fundamental research on the flourishing field of quantum cryptography.

Bibliography

[Abo+18] M. H. Abobeih, J. Cramer, M. A. Bakker, et al. “One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment”. In: *Nature Communications* 9.1 (2018), p. 2552 (cit. on p. 74).

[AKB14] Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß. “Measurement-device-independent quantum key distribution with quantum memories”. In: *Phys. Rev. A* 89 (1 Jan. 2014), p. 012301 (cit. on p. 56).

[AGM06] Antonio Acín, Nicolas Gisin, and Lluis Masanes. “From Bell’s Theorem to Secure Quantum Key Distribution”. In: *Phys. Rev. Lett.* 97 (12 Sept. 2006), p. 120405 (cit. on p. 77).

[Ard92] M. Ardehali. “Bell inequalities with a magnitude of violation that grows exponentially with the number of particles”. In: *Phys. Rev. A* 46 (9 Nov. 1992), pp. 5375–5378 (cit. on pp. 99, 113, 116).

[Arn+18] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. “Practical device-independent quantum cryptography via entropy accumulation”. In: *Nature Communications* 9.1 (2018), p. 459 (cit. on pp. 77, 87, 89).

[ARV19] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. “Simple and Tight Device-Independent Security Proofs”. In: *SIAM Journal on Computing* 48.1 (2019), pp. 181–225. eprint: `https://doi.org/10.1137/18M1174726` (cit. on p. 90).

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. “Experimental Test of Bell’s Inequalities Using Time-Varying Analyzers”. In: *Phys. Rev. Lett.* 49 (25 Dec. 1982), pp. 1804–1807 (cit. on p. 83).

[ATL15] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. “All-photonic quantum repeaters”. In: *Nature Communications* 6.1 (2015), p. 6787 (cit. on p. 56).

[ATM15] Koji Azuma, Kiyoshi Tamaki, and William J. Munro. “All-photonic intercity quantum key distribution”. In: *Nature Communications* 6.1 (2015), p. 10171 (cit. on p. 56).

[BSS14] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. “More randomness from the same data”. In: *New Journal of Physics* 16.3 (Mar. 2014), p. 033011 (cit. on pp. 91, 102).

[BKP06] Jonathan Barrett, Adrian Kent, and Stefano Pironio. “Maximally Nonlocal and Monogamous Quantum Correlations”. In: *Phys. Rev. Lett.* 97 (17 Oct. 2006), p. 170409 (cit. on p. 86).

[BK93] A. V. Belinskiĭ and D. N. Klyshko. "Interference of light and Bell's theorem". In: *Phys. Rev. A* 36 (8 1993), pp. 653–693 (cit. on pp. 99, 113, 116).

[Bel64] J. S. Bell. "On the Einstein Podolsky Rosen paradox". In: *Physics Physique Fizika* 1 (3 Nov. 1964), pp. 195–200 (cit. on p. 78).

[Bel04] J. S. Bell. *Speakable and Unspeakable in Quantum Mechanics. Collected Papers on Quantum Philosophy*. Cambridge University Press, 2004 (cit. on pp. 78, 98).

[BB89] C. H. Bennett and G. Brassard. "Experimental Quantum Cryptography: The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype is Working]". In: *SIGACT News* 20.4 (Nov. 1989), pp. 78–80 (cit. on p. 43).

[BB84] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984, pp. 175–179 (cit. on pp. 1, 27, 133).

[Ben+92] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. "Experimental quantum cryptography". In: *Journal of Cryptology* 5.1 (1992), pp. 3–28 (cit. on p. 43).

[Ben+83] Charles H. Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. "Quantum Cryptography, or Unforgeable Subway Tokens". In: *Advances in Cryptology*. Ed. by David Chaum, Ronald L. Rivest, and Alan T. Sherman. Boston, MA: Springer US, 1983, pp. 267–275 (cit. on p. 1).

[Ber+13] H. Bernien, B. Hensen, W. Pfaff, et al. "Heralded entanglement between solid-state qubits separated by three metres". In: *Nature* 497.7447 (2013), pp. 86–90 (cit. on p. 74).

[Boa+18] Alberto Boaron, Gianluca Boso, Davide Rusca, et al. "Secure Quantum Key Distribution over 421 km of Optical Fiber". In: *Phys. Rev. Lett.* 121 (19 Nov. 2018), p. 190502 (cit. on p. 43).

[Bra05] G. Brassard. "Brief history of quantum cryptography: a personal perspective". In: *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*. 2005, pp. 19–23 (cit. on p. 1).

[Bra+00] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. "Limitations on Practical Quantum Cryptography". In: *Phys. Rev. Lett.* 85 (6 Aug. 2000), pp. 1330–1333 (cit. on p. 46).

[Bri+98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication". In: *Phys. Rev. Lett.* 81 (26 Dec. 1998), pp. 5932–5935 (cit. on p. 56).

[BFK09] A. Broadbent, J. Fitzsimons, and E. Kashefi. "Universal Blind Quantum Computation". In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. 2009, pp. 517–526 (cit. on p. 1).

[BRC20] P. J. Brown, S. Ragy, and R. Colbeck. "A Framework for Quantum-Secure Device-Independent Randomness Expansion". In: *IEEE Transactions on Information Theory* 66.5 (2020), pp. 2964–2987 (cit. on p. 101).

[Bru+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. “Bell nonlocality”. In: *Rev. Mod. Phys.* 86 (2 Apr. 2014), pp. 419–478 (cit. on pp. 78, 84–86).

[Bru98] Dagmar Bruß. “Optimal Eavesdropping in Quantum Cryptography with Six States”. In: *Phys. Rev. Lett.* 81 (14 Oct. 1998), pp. 3018–3021 (cit. on pp. 1, 40).

[CP19] R. Laurenza C. Ottaviani C. Lupo and S. Pirandola. “Modular network for high-rate quantum conferencing”. In: *Communications Physics* 2.118 (2019) (cit. on p. 38).

[CW79] J.Lawrence Carter and Mark N. Wegman. “Universal classes of hash functions”. In: *Journal of Computer and System Sciences* 18.2 (1979), pp. 143–154 (cit. on p. 35).

[CKR09] Matthias Christandl, Robert König, and Renato Renner. “Postselection Technique for Quantum Channels with Applications to Quantum Cryptography”. In: *Phys. Rev. Lett.* 102 (2 Jan. 2009), p. 020504 (cit. on p. 37).

[Cla+69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. “Proposed Experiment to Test Local Hidden-Variable Theories”. In: *Phys. Rev. Lett.* 23 (15 Oct. 1969), pp. 880–884 (cit. on pp. 78, 81, 88).

[CKW00] Valerie Coffman, Joydip Kundu, and William K. Wootters. “Distributed entanglement”. In: *Phys. Rev. A* 61 (5 Apr. 2000), p. 052306 (cit. on p. 86).

[Col07] Roger Colbeck. *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, University of Cambridge. Also available at: arXiv:quant-ph/0911.3814. 2007 (cit. on p. 77).

[CK11] Roger Colbeck and Adrian Kent. “Private randomness expansion with untrusted devices”. In: *Journal of Physics A: Mathematical and Theoretical* 44.9 (Feb. 2011), p. 095305 (cit. on p. 77).

[Col+02] Daniel Collins, Nicolas Gisin, Sandu Popescu, David Roberts, and Valerio Scarani. “Bell-Type Inequalities to Detect True n-Body Nonseparability”. In: *Phys. Rev. Lett.* 88 (17 Apr. 2002), p. 170405 (cit. on p. 100).

[Com] European Commission. *The Quantum Flagship*. `https://qt.eu`. [Online] (cit. on pp. 1, 43).

[Cui+19] Chaohan Cui, Zhen-Qiang Yin, Rong Wang, et al. “Twin-Field Quantum Key Distribution without Phase Postselection”. In: *Phys. Rev. Applied* 11 (3 Mar. 2019), p. 034053 (cit. on pp. 57, 58).

[CAL19] Marcos Curty, Koji Azuma, and Hoi-Kwong Lo. “Simple security proof of twin-field type quantum key distribution protocol”. In: *npj Quantum Information* 5.1 (2019), p. 64 (cit. on pp. 2, 57, 58, 61–68, 110, 111).

[Das+19] Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki. *Universal limitations on quantum key distribution over a network*. 2019. arXiv: `1912.03646 [quant-ph]` (cit. on p. 39).

[DJR05] Thomas Decker, Dominik Janzing, and Martin Rótteler. “Implementation of group-covariant positive operator valued measures by orthogonal measurements”. In: *Journal of Mathematical Physics* 46.1 (2005), p. 012104. eprint: `https://doi.org/10.1063/1.1827924` (cit. on p. 10).

[DW05] Igor Devetak and Andreas Winter. “Distillation of secret key and entanglement from quantum states”. In: *Proc. R. Soc. A* 461 (2053 Jan. 2005) (cit. on p. 30).

[Dia+16] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. “Practical challenges in quantum key distribution”. In: *npj Quantum Information* 2.1 (2016), p. 16025 (cit. on pp. 1, 43).

[Dix+08] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate”. In: *Opt. Express* 16.23 (Nov. 2008), pp. 18790–18797 (cit. on p. 43).

[Dua+01] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. “Long-distance quantum communication with atomic ensembles and linear optics”. In: *Nature* 414.6862 (2001), pp. 413–418 (cit. on p. 56).

[DF19] F. Dupuis and O. Fawzi. “Entropy Accumulation With Improved Second-Order Term”. In: *IEEE Transactions on Information Theory* 65.11 (2019), pp. 7596–7612 (cit. on p. 87).

[DFR16] Frederic Dupuis, Omar Fawzi, and Renato Renner. *Entropy accumulation*. 2016. arXiv: `1607.01796 [quant-ph]` (cit. on pp. 87, 101).

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. “Three qubits can be entangled in two inequivalent ways”. In: *Phys. Rev. A* 62 (6 Nov. 2000), p. 062314 (cit. on p. 72).

[Eke91] A. K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Phys. Rev. Lett.* 67 (6 1991), pp. 661–663 (cit. on p. 1).

[EKB16a] Michael Epping, Hermann Kampermann, and Dagmar Bruß. “Large-scale quantum networks based on graphs”. In: *New Journal of Physics* 18.5 (May 2016), p. 053036 (cit. on p. 38).

[EKB16b] Michael Epping, Hermann Kampermann, and Dagmar Bruß. “Robust entanglement distribution via quantum network coding”. In: *New Journal of Physics* 18.10 (Oct. 2016), p. 103052 (cit. on p. 38).

[Epp+17] Michael Epping, Hermann Kampermann, Chiara Macchiavello, and Dagmar Bruß. “Multi-partite entanglement can speed up quantum key distribution in networks”. In: *New Journal of Physics* 19.9 (Sept. 2017), p. 093012 (cit. on pp. 38–41, 73, 99, 109, 149).

[Fed+07] Alessandro Fedrizzi, Thomas Herbst, Andreas Poppe, Thomas Jennewein, and Anton Zeilinger. “A wavelength-tunable fiber-coupled source of narrowband entangled photons”. In: *Opt. Express* 15.23 (Nov. 2007), pp. 15377–15386 (cit. on p. 116).

[FGS13] Serge Fehr, Ran Gelles, and Christian Schaffner. “Security and composability of randomness expansion from Bell inequalities”. In: *Phys. Rev. A* 87 (1 Jan. 2013), p. 012335 (cit. on p. 77).

[Fit17] Joseph F. Fitzsimons. “Private quantum computation: an introduction to blind quantum computing and related protocols”. In: *npj Quantum Information* 3.1 (June 2017), p. 23 (cit. on p. 1).

[Ger+11] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, et al. “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”. In: *Nature Communications* 2.1 (2011), p. 349 (cit. on p. 49).

[Giu+15] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, et al. “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons”. In: *Phys. Rev. Lett.* 115 (25 Dec. 2015), p. 250401 (cit. on p. 84).

[Gol+11] S. Goldstein, T. Norsen, D. Victor Tausk, and N. Zanghi. “Bell’s theorem”. In: *Scholarpedia* 6.10 (2011). revision #91049, p. 8378 (cit. on p. 78).

[Got+04] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. “Security of quantum key distribution with imperfect devices”. In: *Quant. Inf. Comput.* 4 (5 2004), pp. 325–360 (cit. on pp. 46, 54).

[Gra+18] Francesco Graffitti, Peter Barrow, Massimiliano Proietti, Dmytro Kundys, and Alessandro Fedrizzi. “Independent high-purity photons created in domain-engineered crystals”. In: *Optica* 5.5 (May 2018), pp. 514–517 (cit. on p. 116).

[GC19] Federico Grasselli and Marcos Curty. “Practical decoy-state method for twin-field quantum key distribution”. In: *New Journal of Physics* 21.7 (July 2019), p. 073001 (cit. on pp. 2, 66, 68, 69, 110, 111, 173, 207).

[GKB19] Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. “Conference key agreement with single-photon interference”. In: *New Journal of Physics* 21.12 (Dec. 2019), p. 123002 (cit. on pp. 2, 38, 69, 70, 74, 75, 111, 115, 241).

[GKB18] Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. “Finite-key effects in multipartite quantum key distribution protocols”. In: *New Journal of Physics* 20.11 (Nov. 2018), p. 113014 (cit. on pp. 2, 38–41, 43, 109, 111, 112, 115, 149, 261).

[Gra+20] Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß. *Analytical entropic bounds for multiparty device-independent cryptography*. 2020. arXiv: `2004.14263 [quant-ph]` (cit. on pp. 3, 92, 96, 98–103, 105, 107, 108, 113, 115, 116, 137, 138, 143, 289).

[GNC19] Federico Grasselli, Álvaro Navarrete, and Marcos Curty. “Asymmetric twin-field quantum key distribution”. In: *New Journal of Physics* 21.11 (Nov. 2019), p. 113032 (cit. on pp. 2, 67–69, 110, 207).

[GHZ89] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*. Vol. 37. Springer Science & Business Media B.V., 1989, pp. 69–72 (cit. on p. 13).

[GT09] Otfried Gühne and Géza Tóth. “Entanglement detection”. In: *Physics Reports* 474.1 (2009), pp. 1–75 (cit. on p. 12).

[HPE19] F. Hahn, A. Pappa, and J. Eisert. “Quantum network routing and local complementation”. In: *npj Quantum Information* 5.1 (2019), p. 76 (cit. on p. 38).

[Hen+15] B. Hensen, H. Bernien, A. E. Dréau, et al. “Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres”. In: *Nature* 526.7575 (2015), pp. 682–686 (cit. on p. 84).

[HKB19] Timo Holz, Hermann Kampermann, and Dagmar Bruß. *A Genuine Multipartite Bell Inequality for Device-independent Conference Key Agreement*. 2019. arXiv: `1910.11360 [quant-ph]` (cit. on pp. 77, 103, 104, 106–108, 116).

[Hol+19] Timo Holz, Daniel Miller, Hermann Kampermann, and Dagmar Bruß. “Comment on “Fully device-independent conference key agreement””. In: *Phys. Rev. A* 100 (2 Aug. 2019), p. 026301 (cit. on pp. 82, 104, 105).

[HR19] Paweł Horodecki and Ravishankar Ramanathan. “The relativistic causality versus no-signaling paradigm for multi-party correlations”. In: *Nature Communications* 10.1 (Apr. 2019), p. 1701 (cit. on pp. 78, 84, 85).

[HHH95] R. Horodecki, P. Horodecki, and M. Horodecki. “Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition”. In: *Physics Letters A* 200.5 (1995), pp. 340–344 (cit. on pp. 92, 101, 138).

[Hua+15] Duan Huang, Dakai Lin, Chao Wang, et al. “Continuous-variable quantum key distribution with 1 Mbps secure key rate”. In: *Opt. Express* 23.13 (June 2015), pp. 17511–17519 (cit. on p. 43).

[Hut+95] B. Huttner, N. Imoto, N. Gisin, and T. Mor. “Quantum cryptography with coherent states”. In: *Phys. Rev. A* 51 (3 Mar. 1995), pp. 1863–1869 (cit. on p. 46).

[Hwa03] Won-Young Hwang. “Quantum Key Distribution with High Loss: Toward Global Secure Communication”. In: *Phys. Rev. Lett.* 91 (5 Aug. 2003), p. 057901 (cit. on p. 47).

[KLM07] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007 (cit. on p. 5).

[Kim08] H. J. Kimble. “The quantum internet”. In: *Nature* 453.7198 (2008), pp. 1023–1030 (cit. on pp. 1, 38, 115).

[KRS09] R. Konig, R. Renner, and C. Schaffner. “The Operational Meaning of Min- and Max-Entropy”. In: *IEEE Transactions on Information Theory* 55.9 (2009), pp. 4337–4347 (cit. on pp. 21–24).

[Kru+19] V. Krutyanskiy, M. Meraner, J. Schupp, et al. “Light-matter entanglement over 50 km of optical fibre”. In: *npj Quantum Information* 5.1 (2019), p. 72 (cit. on p. 38).

[Li+18] Hao Li, Xiaoyan Yang, Lixing You, et al. “Improving detection efficiency of superconducting nanowire single-photon detector using multilayer antireflection coating”. In: *AIP Advances* 8.11 (2018), p. 115022. eprint: `https://doi.org/10.1063/1.5034374` (cit. on p. 116).

[Lia+18] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, et al. “Satellite-Relayed Intercontinental Quantum Network”. In: *Phys. Rev. Lett.* 120 (3 Jan. 2018), p. 030501 (cit. on p. 43).

[Lia+17] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (2017), pp. 43–47 (cit. on p. 43).

[Lim+14] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. “Concise security bounds for practical decoy-state quantum key distribution”. In: *Phys. Rev. A* 89 (2 Feb. 2014), p. 022307 (cit. on pp. 48, 49).

[LB05] Yuan Liang Lim and Almut Beige. “Multiphoton entanglement through a Bell-multiport beam splitter”. In: *Phys. Rev. A* 71 (6 June 2005), p. 062311 (cit. on p. 70).

[LL18] Jie Lin and Norbert Lütkenhaus. “Simple security analysis of phase-matching measurement-device-independent quantum key distribution”. In: *Phys. Rev. A* 98 (4 Oct. 2018), p. 042332 (cit. on p. 57).

[Liu+19] Yang Liu, Zong-Wen Yu, Weijun Zhang, et al. “Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending”. In: *Phys. Rev. Lett.* 123 (10 Sept. 2019), p. 100505 (cit. on pp. 43, 57, 62, 66).

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement-Device-Independent Quantum Key Distribution”. In: *Phys. Rev. Lett.* 108 (13 Mar. 2012), p. 130503 (cit. on pp. 49–51, 53, 54).

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. “Decoy State Quantum Key Distribution”. In: *Phys. Rev. Lett.* 94 (23 June 2005), p. 230504 (cit. on pp. 46, 47).

[Luc+18] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. “Overcoming the rate-distance limit of quantum key distribution without quantum repeaters”. In: *Nature* 557.7705 (2018), pp. 400–403 (cit. on pp. 2, 57, 58, 62).

[Lyd+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, et al. “Hacking commercial quantum cryptography systems by tailored bright illumination”. In: *Nature Photonics* 4.10 (2010), pp. 686–689 (cit. on p. 49).

[MZZ18] Xiongfeng Ma, Pei Zeng, and Hongyi Zhou. “Phase-Matching Quantum Key Distribution”. In: *Phys. Rev. X* 8 (3 Aug. 2018), p. 031043 (cit. on p. 57).

[MAG06] Ll. Masanes, A. Acin, and N. Gisin. “General properties of nonsignaling theories”. In: *Phys. Rev. A* 73 (1 Jan. 2006), p. 012112 (cit. on p. 84).

[MPA11] Lluís Masanes, Stefano Pironio, and Antonio Acín. “Secure device-independent quantum key distribution with causally independent measurement devices”. In: *Nature Communications* 2.1 (2011), p. 238 (cit. on pp. 77, 107).

[Mat07] Ryutaroh Matsumoto. “Multiparty quantum-key-distribution protocol without use of entanglement”. In: *Phys. Rev. A* 76 (6 Dec. 2007), p. 062316 (cit. on p. 39).

[Maz+14] Paweł Mazurek, Andrzej Grudka, Michał Horodecki, et al. “Long-distance quantum communication over noisy networks without long-time quantum memory”. In: *Phys. Rev. A* 90 (6 Dec. 2014), p. 062311 (cit. on p. 56).

[Mer90] N. David Mermin. “Extreme quantum entanglement in a superposition of macroscopically distinct states”. In: *Phys. Rev. Lett.* 65 (15 Oct. 1990), pp. 1838–1840 (cit. on pp. 99, 113, 116).

[Mil82] Frank Miller. *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. 1882 (cit. on p. 26).

[Min+19] M. Minder, M. Pittaluga, G. L. Roberts, et al. “Experimental quantum key distribution beyond the repeaterless secret key capacity”. In: *Nature Photonics* 13.5 (2019), pp. 334–338 (cit. on pp. 57, 62, 66).

[Mun+12] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and Kae Nemoto. “Quantum communication without the necessity of quantum memories”. In: *Nature Photonics* 6.11 (2012), pp. 777–781 (cit. on p. 56).

[Mur+19] G Murta, S B van Dam, J Ribeiro, R Hanson, and S Wehner. “Towards a realization of device-independent quantum key distribution”. In: *Quantum Science and Technology* 4.3 (July 2019), p. 035011 (cit. on pp. 88–90).

[Mur+20] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. *Quantum Conference Key Agreement: A Review*. 2020. arXiv: `2003.10186 [quant-ph]` (cit. on pp. 3, 38, 113, 115, 273).

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations”. In: *New Journal of Physics* 10.7 (July 2008), p. 073013 (cit. on pp. 91, 102, 107).

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. “Bounding the Set of Quantum Correlations”. In: *Phys. Rev. Lett.* 98 (1 Jan. 2007), p. 010401 (cit. on pp. 91, 102).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010 (cit. on pp. 5, 8, 17, 26, 27).

[NPS14] O Nieto-Silleras, S Pironio, and J Silman. “Using complete measurement statistics for optimal device-independent randomness evaluation”. In: *New Journal of Physics* 16.1 (Jan. 2014), p. 013035 (cit. on pp. 91, 102).

[Nie+18] Olmo Nieto-Silleras, Cédric Bamps, Jonathan Silman, and Stefano Pironio. “Device-independent randomness generation from several Bell estimators”. In: *New Journal of Physics* 20.2 (Feb. 2018), p. 023049 (cit. on p. 77).

[Pan+14] Christiana Panayi, Mohsen Razavi, Xiongfeng Ma, and Norbert Lütkenhaus. “Memory-assisted measurement-device-independent quantum key distribution”. In: *New Journal of Physics* 16.4 (Apr. 2014), p. 043005 (cit. on p. 56).

[Par12] M. G. A. Paris. “The modern tools of quantum mechanics”. In: *The European Physical Journal Special Topics* 203.1 (2012), pp. 61–86 (cit. on p. 17).

[Pat+14] K. A. Patel, J. F. Dynes, M. Lucamarini, et al. “Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks”. In: *Applied Physics Letters* 104.5 (2014), p. 051123. eprint: `https://doi.org/10.1063/1.4864398` (cit. on p. 43).

[Pau27] W. Pauli. “Zur Quantenmechanik des magnetischen Elektrons”. In: *Zeitschrift für Physik* 43.9 (1927), pp. 601–623 (cit. on p. 10).

[Per06] Asher Peres. *Quantum Theory: Concepts and Methods*. Springer, Dordrecht, 2006 (cit. on p. 10).

[Per+11] Alberto Peruzzo, Anthony Laing, Alberto Politi, Terry Rudolph, and Jeremy L. O’Brien. “Multimode quantum interference of photons in multiport integrated devices”. In: *Nature Communications* 2.1 (Mar. 2011), p. 224 (cit. on p. 70).

[Pir+19] S. Pirandola, U. L. Andersen, L. Banchi, et al. *Advances in Quantum Cryptography*. 2019. arXiv: `1906.01645 [quant-ph]` (cit. on pp. 28, 43, 50, 89, 90).

[Pir19a] Stefano Pirandola. “End-to-end capacities of a quantum communication network”. In: *Communications Physics* 2.1 (2019), p. 51 (cit. on p. 39).

[Pir19b] Stefano Pirandola. *General upper bounds for distributing conferencing keys in arbitrary quantum networks*. 2019. arXiv: `1912.11355 [quant-ph]` (cit. on p. 39).

[Pir+17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. “Fundamental limits of repeaterless quantum communications”. In: *Nature Communications* 8.1 (2017), p. 15043 (cit. on p. 55).

[PWD18] A Pirker, J Wallnöfer, and W Dür. “Modular architectures for quantum networks”. In: *New Journal of Physics* 20.5 (May 2018), p. 053054 (cit. on p. 38).

[Pir+10] S. Pironio, A. Acín, S. Massar, et al. “Random numbers certified by Bell’s theorem”. In: *Nature* 464.7291 (2010), pp. 1021–1024 (cit. on p. 77).

[Pir+09] Stefano Pironio, Antonio Acín, Nicolas Brunner, et al. “Device-independent quantum key distribution secure against collective attacks”. In: *New Journal of Physics* 11.4 (Apr. 2009), p. 045021 (cit. on pp. 77, 86, 89, 91, 92, 96, 137, 138).

[PM13] Stefano Pironio and Serge Massar. “Security of practical private randomness generation”. In: *Phys. Rev. A* 87 (1 Jan. 2013), p. 012336 (cit. on p. 77).

[Pro+20] Massimiliano Proietti, Joseph Ho, Federico Grasselli, et al. *Experimental quantum conference key agreement*. 2020. arXiv: `2002.01491 [quant-ph]` (cit. on pp. 2, 43, 112, 115, 116, 261).

[Ren08] Renato Renner. “Security of Quantum Key Distribution”. In: *International Journal of Quantum Information* 06.01 (2008), pp. 1–127 (cit. on pp. 5, 30, 35, 37, 136).

[Ren07] Renato Renner. “Symmetry of large physical systems implies independence of subsystems”. In: *Nature Physics* 3.9 (2007), pp. 645–649 (cit. on p. 37).

[RMW18] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. “Fully device-independent conference key agreement”. In: *Phys. Rev. A* 97 (2 Feb. 2018), p. 022307 (cit. on pp. 100, 103).

[RMW19] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner. “Reply to “Comment on ‘Fully device-independent conference key agreement’ ””. In: *Phys. Rev. A* 100 (2 Aug. 2019), p. 026302 (cit. on pp. 39, 77, 91, 103, 106, 108, 116).

[Ros11] Cesare Rossetti. *Rudimenti di meccanica quantistica*. Levrotto & Bella, 2011 (cit. on p. 5).

[Roz+19] Filip Rozp ędek, Raja Yehia, Kenneth Goodenough, et al. “Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission”. In: *Phys. Rev. A* 99 (5 May 2019), p. 052330 (cit. on p. 74).

[Rus+18] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden. “Finite-key analysis for the 1-decoy state QKD protocol”. In: *Applied Physics Letters* 112.17 (2018), p. 171104. eprint: `https://doi.org/10.1063/1.5023340` (cit. on p. 48).

[San+11] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. “Quantum repeaters based on atomic ensembles and linear optics”. In: *Rev. Mod. Phys.* 83 (1 Mar. 2011), pp. 33–80 (cit. on p. 56).

[Sca+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, et al. “The security of practical quantum key distribution”. In: *Rev. Mod. Phys.* 81 (3 Sept. 2009), pp. 1301–1350 (cit. on pp. 1, 28, 33, 37, 43).

[SG01a] Valerio Scarani and Nicolas Gisin. “Quantum Communication between N Partners and Bell’s Inequalities”. In: *Phys. Rev. Lett.* 87 (11 Aug. 2001), p. 117901 (cit. on p. 77).

[SG01b] Valerio Scarani and Nicolas Gisin. “Quantum key distribution between N partners: Optimal eavesdropping and Bell’s inequalities”. In: *Phys. Rev. A* 65 (1 Dec. 2001), p. 012311 (cit. on p. 77).

[SR08a] Valerio Scarani and Renato Renner. “Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing”. In: *Phys. Rev. Lett.* 100 (20 May 2008), p. 200501 (cit. on p. 30).

[SR08b] Valerio Scarani and Renato Renner. “Security Bounds for Quantum Cryptography with Finite Resources”. In: *Theory of Quantum Computation, Communication, and Cryptography*. Ed. by Yasuhito Kawano and Michele Mosca. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 83–95 (cit. on p. 30).

[Sha+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, et al. “Strong Loophole-Free Test of Local Realism”. In: *Phys. Rev. Lett.* 115 (25 Dec. 2015), p. 250402 (cit. on p. 84).

[SS19] Mohd Asad Siddiqui and Sk Sazim. “Tight upper bound for the maximal expectation value of the Mermin operators”. In: *Quantum Information Processing* 18.5 (Mar. 2019), p. 131 (cit. on p. 101).

[Spa+13] Nicolò Spagnolo, Chiara Vitelli, Lorenzo Aparo, et al. “Three-photon bosonic coalescence in an integrated tritter”. In: *Nature Communications* 4.1 (Mar. 2013), p. 1606 (cit. on p. 70).

[SO94] Alan Stuart and J. Keith Ord. *Kendall’s Advanced Theory of Statistics, Volume 1, Distribution Theory*. Edward Arnold Publishers, 1994 (cit. on p. 63).

[Tak+17] Hideki Takenaka, Alberto Carrasco-Casado, Mikio Fujiwara, et al. “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite”. In: *Nature Photonics* 11.8 (2017), pp. 502–508 (cit. on p. 43).

[TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. “Fundamental rate-loss tradeoff for optical quantum key distribution”. In: *Nature Communications* 5.1 (2014), p. 5235 (cit. on p. 55).

[Tak+19] Masahiro Takeoka, Eneet Kaur, Wojciech Roga, and Mark M. Wilde. *Multipartite entanglement and secret key distribution in quantum networks*. arXiv:1912.10658. 2019 (cit. on p. 39).

[Tch+19] Anna Tchebotareva, Sophie L. N. Hermans, Peter C. Humphreys, et al. “Entanglement between a Diamond Spin Qubit and a Photonic Time-Bin Qubit at Telecom Wavelength”. In: *Phys. Rev. Lett.* 123 (6 Aug. 2019), p. 063601 (cit. on p. 38).

[Tec] Inside Quantum Technology. *Quantum Key Distribution (QKD) Markets: 2019-2028*. `https://www.insidequantumtechnology.com/product/quantum-key-distribution-qkd-markets-2019-2028`. [Online] (cit. on pp. 1, 43).

[TCR09] M. Tomamichel, R. Colbeck, and R. Renner. “A Fully Quantum Asymptotic Equipartition Property”. In: *IEEE Transactions on Information Theory* 55.12 (2009), pp. 5840–5847 (cit. on p. 22).

[Tom+11a] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. “Leftover Hashing Against Quantum Side Information”. In: *IEEE Transactions on Information Theory* 57.8 (2011), pp. 5524–5535 (cit. on p. 22).

[Tom+11b] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. “Leftover Hashing Against Quantum Side Information”. In: *IEEE Transactions on Information Theory* 57.8 (2011), pp. 5524–5535 (cit. on pp. 37, 136).

[Tom16] Marco Tomamichel. *Quantum Information Processing with Finite Resources*. SpringerBriefs in Mathematical Physics, 2016 (cit. on pp. 21–23).

[Tom+12] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. “Tight finite-key analysis for quantum cryptography”. In: *Nature Communications* 3.1 (2012), p. 634 (cit. on pp. 34, 136).

[TR11] Marco Tomamichel and Renato Renner. “Uncertainty Relation for Smooth Entropies”. In: *Phys. Rev. Lett.* 106 (11 Mar. 2011), p. 110506 (cit. on p. 41).

[TG05] Géza Tóth and Otfried Gühne. “Entanglement detection in the stabilizer formalism”. In: *Phys. Rev. A* 72 (2 Aug. 2005), p. 022340 (cit. on pp. 82, 105, 106).

[Val02] Angel G Valdenebro. “Assumptions underlying Bell s inequalities”. In: *European Journal of Physics* 23.5 (Sept. 2002), pp. 569–577 (cit. on p. 78).

[VV14] Umesh Vazirani and Thomas Vidick. “Fully Device-Independent Quantum Key Distribution”. In: *Phys. Rev. Lett.* 113 (14 Sept. 2014), p. 140501 (cit. on p. 77).

[Ver26] G. S. Vernam. “Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications”. In: *Transactions of the American Institute of Electrical Engineers* XLV (1926), pp. 295–301 (cit. on p. 26).

[Wan+19] Shuang Wang, De-Yong He, Zhen-Qiang Yin, et al. “Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System”. In: *Phys. Rev. X* 9 (2 June 2019), p. 021046 (cit. on pp. 43, 57, 62, 66).

[Wan05] Xiang-Bin Wang. “Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography”. In: *Phys. Rev. Lett.* 94 (23 June 2005), p. 230503 (cit. on pp. 47, 48).

[WYH18] Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu. “Twin-field quantum key distribution with large misalignment error”. In: *Phys. Rev. A* 98 (6 Dec. 2018), p. 062323 (cit. on p. 57).

[Wat+07] Shun Watanabe, Ryutaroh Matsumoto, Tomohiko Uyematsu, and Yasuhito Kawano. “Key rate of quantum key distribution with hashed two-way classical communication”. In: *Phys. Rev. A* 76 (3 Sept. 2007), p. 032312 (cit. on p. 133).

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. “Quantum internet: A vision for the road ahead”. In: *Science* 362.6412 (2018). eprint: `https://science.sciencemag.org/content/362/6412/eaam9288.full.pdf` (cit. on pp. 1, 38, 115).

[Wei+13] Zhengchao Wei, Weilong Wang, Zhen Zhang, et al. “Decoy-state quantum key distribution with biased basis choice”. In: *Scientific Reports* 3.1 (2013), p. 2453 (cit. on pp. 46, 48).

[WW01] R. F. Werner and M. M. Wolf. “All-multipartite Bell-correlation inequalities for two dichotomic observables per site”. In: *Phys. Rev. A* 64 (3 Aug. 2001), p. 032112 (cit. on pp. 98, 105).

[Wie83] Stephen Wiesner. “Conjugate Coding”. In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88 (cit. on p. 1).

[WBA18] Erik Woodhead, Boris Bourdoncle, and Antonio Acín. “Randomness versus nonlocality in the Mermin-Bell experiment with three parties”. In: *Quantum* 2 (Aug. 2018), p. 82 (cit. on pp. 101, 102).

[WZ82] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (1982), pp. 802–803 (cit. on p. 26).

[Wu+16] Yadong Wu, Jian Zhou, Xinbao Gong, et al. “Continuous-variable measurement-device-independent multipartite quantum communication”. In: *Phys. Rev. A* 93 (2 Feb. 2016), p. 022325 (cit. on p. 38).

[Xu+15] F. Xu, M. Curty, B. Qi, and H. Lo. “Measurement-Device-Independent Quantum Cryptography”. In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 148–158 (cit. on p. 49).

[YM98] A. Yao and D. Mayers. “Quantum Cryptography with Imperfect Apparatus”. In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. Los Alamitos, CA, USA: IEEE Computer Society, Nov. 1998, p. 503 (cit. on p. 77).

[Yin+16] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, et al. “Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber”. In: *Phys. Rev. Lett.* 117 (19 Nov. 2016), p. 190501 (cit. on p. 43).

[ZZH97] Marek Żukowski, Anton Zeilinger, and Michael A. Horne. “Realizable higher-dimensional two-particle entanglements via multiport beam splitters”. In: *Phys. Rev. A* 55 (4 Apr. 1997), pp. 2564–2579 (cit. on p. 70).

[Zha+19a] Weijun Zhang, Qi Jia, Lixing You, et al. “Saturating Intrinsic Detection Efficiency of Superconducting Nanowire Single-Photon Detectors via Defect Engineering”. In: *Phys. Rev. Applied* 12 (4 Oct. 2019), p. 044040 (cit. on p. 116).

[Zha+19b] Yichen Zhang, Zhengyu Li, Ziyang Chen, et al. “Continuous-variable QKD over 50 km commercial fiber”. In: *Quantum Science and Technology* 4.3 (May 2019), p. 035006 (cit. on p. 43).

[ZSG18] Zhaoyuan Zhang, Ronghua Shi, and Ying Guo. “Multipartite Continuous Variable Quantum Conferencing Network with Entanglement in the Middle”. In: *Applied Sciences* 8.8 (2018) (cit. on p. 38).

[Zha+08] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems”. In: *Phys. Rev. A* 78 (4 Oct. 2008), p. 042333 (cit. on p. 49).

[Zho+19] Xiaoqing Zhong, Jianyong Hu, Marcos Curty, Li Qian, and Hoi-Kwong Lo. “Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution”. In: *Phys. Rev. Lett.* 123 (10 Sept. 2019), p. 100506 (cit. on pp. 57, 66).

Proofs

A

In this appendix we prove some statements made in the main text, whose articulated proof would have altered the cohesion and flow of the text.

A.1 Eve's Uncertainty is Non-increasing under Symmetrization

Part of the proof in this section is inspired by [Wat+07].

In computing the secret key rate of the BB84 protocol [BB84] in section 3.2, we argue that w.l.o.g. the state ρ_{AB} distributed to Alice and Bob by Eve is replaced by (3.13):

$$\begin{aligned}\tilde{\rho}_{AB} = \frac{1}{4}\,[&\rho_{AB} + (Z \otimes Z)\rho_{AB}(Z \otimes Z) + (X \otimes X)\rho_{AB}(X \otimes X) \\ &+(Y \otimes Y)\rho_{AB}(Y \otimes Y)]\,.\end{aligned} \tag{A.1}$$

This scenario can be viewed as Eve preparing one of the four states

$$\rho_{AB},\ \ (Z \otimes Z)\,\rho_{AB}\,(Z \otimes Z),\ \ (X \otimes X)\,\rho_{AB}\,(X \otimes X),\ \ (Y \otimes Y)\,\rho_{AB}\,(Y \otimes Y) \tag{A.2}$$

depending on the outcome $t = 1, 2, 3, 4$ of a random variable stored in the register T, which Eve is aware of. Since Eve holds the purifying system E of every state in (A.2), the state prepared by Eve is:

$$\tilde{\rho}_{ABET} = \frac{1}{4}\sum_t |\phi^t_{ABE}\rangle\,\langle\phi^t_{ABE}| \otimes |t\rangle\langle t|_T, \tag{A.3}$$

where $\{|\phi^t_{ABE}\rangle\}_{t=1}^4$ are pure states. Finally, we assume that Eve holds the purifying system T' of the state in (A.3). Thus the global state is pure and reads:

$$|\phi_{ABETT'}\rangle = \frac{1}{2}\sum_t |\phi^t_{ABE}\rangle \otimes |t\rangle_T \otimes |t\rangle_{T'}\,. \tag{A.4}$$

Note that (A.4) is a purification of (A.3), where both registers T and T' are held by Eve. The above argument holds only if it's not disadvantageous for Eve. In other words, Eve's uncertainty on Alice's key, quantified by the conditional entropy $H(R_A|E)$, must be non-increasing. Therefore, we must verify that:

$$H(R_A|E)_\rho \geq H(R_A|E_{\text{tot}})_{\tilde{\rho}}, \tag{A.5}$$

where Eve's quantum system $E_{\text{tot}} = ETT'$ contains: the quantum side information E, the outcome of the random variable T, and the purifying system T'.

Proof. In order to prove (A.5), we start by using the strong subadditivity property (c.f. section 2.6):

$$H(R_A|E_{\text{tot}})_{\tilde{\rho}} \leq H(R_A|ET)_{\tilde{\rho}} \tag{A.6}$$

where the r.h.s. entropy is computed on the following state:

$$\begin{aligned}\tilde{\rho}_{R_A ET} &= (\mathcal{E}_{R_A} \otimes \text{id}_{ET}) \operatorname{Tr}_B [\tilde{\rho}_{ABET}] \\ &= \frac{1}{4} (\mathcal{E}_{R_A} \otimes \text{id}_{ET}) \operatorname{Tr}_B \left[\sum_t |\phi^t_{ABE}\rangle \langle \phi^t_{ABE}| \otimes |t\rangle\langle t|_T \right] \\ &=: \frac{1}{4} \sum_t \rho^t_{R_A E} \otimes |t\rangle\langle t|_T, \end{aligned} \tag{A.7}$$

where the quantum map

$$\mathcal{E}_{R_A}(\sigma) = \sum_{a=0}^{1} |a\rangle\langle a| \langle a| \sigma |a\rangle$$

represents the measurement performed by Alice for key generation, i.e. a projection onto the Z basis. Being the state in Eq. (A.7) a c.q. state, its entropy simplifies to:

$$H(R_A|ET)_{\tilde{\rho}} = \frac{1}{4} \sum_t H(R_A|E)_{\rho^t}. \tag{A.8}$$

The last part of the proof shows that $H(R_A|E)_{\rho^t}$ is actually independent of t and equal to conditional entropy of the original state $H(R_A|E)_\rho$. This is clear if the state $\rho^t_{R_A E}$ is made explicit. From Eq. (A.7) we have that:

$$\rho^t_{R_A E} = (\mathcal{E}_{R_A} \otimes \text{id}_{ET}) \operatorname{Tr}_B \left[|\phi^t_{ABE}\rangle \langle \phi^t_{ABE}| \right], \tag{A.9}$$

where $|\phi^t_{ABE}\rangle$ is the purification of one of the four states in (A.2) prepared by Eve according to the random variable T. For definiteness, let's fix that state to be $(X \otimes X)\, \rho_{AB}\, (X \otimes X)$, although an analogous reasoning holds for any other state in Eq. (A.2). By writing ρ_{AB} in its spectral decomposition:

$$\rho_{AB} = \sum_\lambda \lambda |\lambda\rangle\langle\lambda|, \tag{A.10}$$

we can immediately explicit $|\phi^t_{ABE}\rangle$ as follows:

$$|\phi^t_{ABE}\rangle = \sum_\lambda \sqrt{\lambda}\, |\lambda^t\rangle_{AB} \otimes |e_\lambda\rangle_E, \tag{A.11}$$

where the eigenstates of the operator $(X \otimes X)\, \rho_{AB}\, (X \otimes X)$ read: $|\lambda^t\rangle = (X \otimes X)\, |\lambda\rangle$. By substituting (A.11) into (A.9) and by making explicit the map $\mathcal{E}_{R_A}$ we obtain the following chain of equalities:

$$
\begin{aligned}
\rho^t_{R_AE} &= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_B \left[\langle a|\, |\lambda^t\rangle \, \langle\sigma^t|\, |a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_B \left[\langle a|\, (X \otimes X)|\lambda\rangle\langle\sigma|(X \otimes X)\, |a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_B \left[\langle \bar{a}|\, |\lambda\rangle\langle\sigma||\bar{a}\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |\bar{a}\rangle\langle \bar{a}| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_B \left[\langle a|\, |\lambda\rangle\langle\sigma||a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&=: \sum_{a=0}^{1} |\bar{a}\rangle\langle \bar{a}| \otimes \rho^a_E,
\end{aligned}
\tag{A.12}
$$

where in the third equality we used the cyclic property of the trace and the fact that Alice measures in the Z basis $\{|0\rangle\, , |1\rangle\}$, hence the Pauli operator X flips its eigenstates: $X\, |a\rangle = |\bar{a}\rangle$. In the fourth equality we relabelled the classical outcomes: $a \leftrightarrow \bar{a}$. Finally, by comparing (A.12) with the state ρ_{R_AE} obtained in an analogous way from the original state ρ_{AB}:

$$
\begin{aligned}
\rho_{R_AE} &= (\mathcal{E}_{R_A} \otimes \mathrm{id}_E)\ \mathrm{Tr}_B \left[|\phi_{ABE}\rangle\langle\phi_{ABE}|\right] \\
&= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\, \mathrm{Tr}_B \left[\langle a|\, |\lambda\rangle \, \langle\sigma|\, |a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \rho^a_E,
\end{aligned}
\tag{A.13}
$$

we observe that $\rho^t_{R_AE}$ and ρ_{R_AE} are the same state up to a permutation of the classical outcomes, thus their conditional entropies coincide:

$$
H(R_A|E)_{\rho^t} = H(R_A|E)_\rho \quad \forall\, t. \tag{A.14}
$$

In conclusion, by combining Eqs. (A.14), (A.8) and (A.6), we prove the claim in Eq. (A.5). This concludes the proof. □

A.2 Finite-key Security of QKD

Here we prove Lemma 3.1, following the lines of [Ren08; Tom+12]. For clarity, we report the Lemma's statement.

Lemma 3.1 *The general QKD protocol described in subsection 3.3.1 is $\varepsilon_{\mathrm{tot}}$-secure, with* $\varepsilon_{\mathrm{tot}} \geq \varepsilon_{\mathrm{EC}} + \varepsilon + \varepsilon_{\mathrm{PA}}$.

Proof. We start by showing that the protocol is $\varepsilon_{\mathrm{EC}}$-correct.

Recall that at the end of EC, Alice and Bob apply a two-universal hash function on their raw keys R_A^n and $\hat{R_A^n}$, obtaining hashes h_A and h_B of length $\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil$. The defining feature of two-universal hash functions is that the probability that two outputs of length $\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil$ coincide, given that the inputs are different, is small, namely: $2^{-\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil}$. In formulas, we have that:

$$\Pr[h_A = h_B, R_A^n \neq \hat{R_A^n}] \leq \Pr[h_A = h_B | R_A^n \neq \hat{R_A^n}] \leq 2^{-\lceil \log(1/\varepsilon_{\mathrm{EC}}) \rceil} \leq \varepsilon_{\mathrm{EC}}. \tag{A.15}$$

Then we observe that the keys s_A and s_B always coincide when the protocol aborts, thus $\Pr[s_A \neq s_B, h_A \neq h_B] = 0$. By employing (A.15) in the following expression, we prove that the protocol is $\varepsilon_{\mathrm{EC}}$-correct:

$$\Pr[s_A \neq s_B] = \Pr[s_A \neq s_B, h_A = h_B] \leq \Pr[R_A^n \neq \hat{R_A^n}, h_A = h_B] \leq \varepsilon_{\mathrm{EC}}. \tag{A.16}$$

In order to prove the secrecy, we make use of the quantum leftover hash lemma [Ren08; Tom+11b], which provides the following upper bound:

$$\frac{1}{2}\left\| \rho_{S_A E_{\mathrm{tot}}|\Omega} - \omega_{S_A} \otimes \rho_{E_{\mathrm{tot}}} \right\| \leq \varepsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(R_A^n|CE)}}, \tag{A.17}$$

where ℓ is the length of Alice's key after PA and where we emphasize E_{tot} being the total information available to Eve. This comprises her purifying system E, the classical communication C occurred during EC and the knowledge F of the hash function used in PA: $E_{\mathrm{tot}} = FCE$.

We now employ the following chain-rule for the min-entropy [Tom+12]:

$$\begin{aligned} H_{\min}^{\varepsilon}(R_A^n|CE) &\geq H_{\min}^{\varepsilon}(R_A^n|E) - \log|C| \\ &= H_{\min}^{\varepsilon}(R_A^n|E) - \mathrm{leak}_{\mathrm{EC}} - \log\frac{2}{\varepsilon_{\mathrm{EC}}}, \end{aligned} \tag{A.18}$$

where $\log|C|$ quantifies all the information revealed during EC and is given by $\mathrm{leak}_{\mathrm{EC}} + \log(2/\varepsilon_{\mathrm{EC}})$ (see the protocol's description).

By inserting Eq. (A.18) into (A.17) we obtain the following chain of inequalities:

$$\begin{aligned}\frac{1}{2}\left\|\rho_{S_A E_{\mathrm{tot}}|\Omega} - \omega_{S_A} \otimes \rho_{E_{\mathrm{tot}}}\right\| &\leq \varepsilon + \frac{1}{2}\sqrt{2^{\ell-(H^{\varepsilon}_{\min}(R^n_A|E)-\mathrm{leak}_{\mathrm{EC}}-\log(2/\varepsilon_{\mathrm{EC}}))}} \\ &\leq \varepsilon + \frac{1}{2}\sqrt{2^{\log(2\,\varepsilon_{\mathrm{PA}})^2}} \\ &= \varepsilon + \varepsilon_{\mathrm{PA}}, \end{aligned} \tag{A.19}$$

where we used the key length expression (3.27) in the second inequality. We have thus proven that the protocol is $\varepsilon_{\mathrm{sec}}$-secret, with $\varepsilon_{\mathrm{sec}} \geq \varepsilon + \varepsilon_{\mathrm{PA}}$. By combining this with the correctness proof, we have shown that the protocol is $\varepsilon_{\mathrm{tot}}$-secure, with $\varepsilon_{\mathrm{tot}} \geq \varepsilon + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}}$. This concludes the proof. □

A.3 State Reduction in the CHSH Scenario

Here we present the proof of Theorem 6.1, whose statement is reported for clarity.

Theorem 6.1 ([Pir+09]). *Let Alice and Bob perform the DIQKD protocol described in subsection 6.4.2. It is not restrictive to assume that, in each round, Eve distributes a mixture $\sum_\alpha p_\alpha \rho_\alpha$ of two-qubit states ρ_α, together with a flag $|\alpha\rangle$ (known to her) which determines the measurements performed on ρ_α given the parties' inputs. Without loss of generality, the measurements performed by Alice's and Bob's devices on ρ_α are rank-one binary projective measurements in the (x, y)-plane of the Bloch sphere. Moreover, each state ρ_α is diagonal in the Bell basis* (3.15) *and reads:*

$$\rho_\alpha = \sum_{i,j=0}^{1} \lambda^\alpha_{ij} |\psi_{ij}\rangle\langle\psi_{ij}| \quad \textit{with} \quad \lambda^\alpha_{0j} \geq \lambda^\alpha_{1j} \quad \forall j \in \{0, 1\}. \tag{A.20}$$

Proof. The proof follows the same principles of the original proof in [Pir+09], however we apply some modifications and add details in a way which is coherent with its generalization valid for N parties that we prove in [Gra+20] (appendix H). **Reduction to qubits:** Firstly we reduce the state shared by Alice and Bob in one round to a convex combination of two-qubit states.

Recall that the statistics of a general quantum measurement (POVM, c.f. section 2.2) is reproduced by a projective measurement in a larger Hilbert space, due to the Naimark theorem. Since in a DI scenario the Hilbert space dimensions are not fixed, we can assume without loss of generality (w.l.o.g.) that Alice and Bob perform binary projective measurements on their share of the quantum state.

Now we make use of a preliminary result derived in [Pir+09], which we extend and detail in [Gra+20]. The result states that the Hilbert space on which Alice's two projective measurements, corresponding to inputs $x = 0, 1$, are acting can be decomposed into the following direct sum (indicated by $\oplus$) of Hilbert spaces:

$$\mathcal{H} = \oplus_{\alpha} \mathcal{H}_{\alpha}^{2} \ , \tag{A.21}$$

where every subspace $\mathcal{H}_{\alpha}^{2}$ is two-dimensional (qubit space) and both Alice's measurements act within $\mathcal{H}_{\alpha}^{2}$ as rank-one projective measurements[1]. Therefore, from Alice's perspective, the measurement process in one round consists of a projection in one of the two-dimensional subspaces $\mathcal{H}_{\alpha}^{2}$, followed by a projective measurement in that subspace selected according to her input. For this reason, we can think that Eve is effectively distributing to Alice a direct sum of qubits at every round. Moreover, since Eve fabricates the measurement devices, she can preprogram the projective measurements that Alice can select on every qubit. By repeating the same argument for Bob, we deduce that Eve effectively distributes a direct sum of two-qubit states in each round.

Now, consider that it cannot be detrimental for Eve to learn the value α corresponding to the two-qubit space selected in a particular round by Alice's and Bob's measurements. Hence, we can assume that Eve directly sends to the parties the two-qubit state ρ_{α} relative to the two-qubit space the parties would select. Since the selection of the two-qubit space can be random, Eve sends a statistical mixture of states ρ_{α}. Furthermore, since she could have preprogrammed the devices to perform specific measurements upon selecting a given subspace, together with the state ρ_{α} she sends a flag $|\alpha\rangle$ to Alice and Bob's devices to instruct them on which measurement to perform on the state ρ_{α}. In conclusion, in every round Eve prepares the following mixture of two-qubit states ρ_{α}:

$$\rho_{AB\Xi} = \textstyle\sum_{\alpha} p_{\alpha} \rho_{\alpha} \otimes |\alpha\rangle\langle\alpha|_{\xi_A} \otimes |\alpha\rangle\langle\alpha|_{\xi_B}, \tag{A.22}$$

where the two ancillae $\Xi := \{\xi_A, \xi_B\}$ fix the qubit measurements that Alice and Bob can select on ρ_{α}. This can be modelled for instance by defining Alice's qubit measurement A_x as follows (and similarly Bob's):

$$A_x = \sum_{\alpha} (\Pi_{+1}^{x,\alpha} - \Pi_{-1}^{x,\alpha}) \otimes |\alpha\rangle\langle\alpha|_{\xi_A}, \tag{A.23}$$

[1] Note that a binary projective measurement on a qubit can also be of rank-two and corresponds to the identity as observable. In this case one outcome has probability 1 to occur and the other outcome never occurs. This possibility was originally neglected in [Pir+09] since measuring the identity cannot lead to a CHSH violation, as pointed out by [HHH95]. However, the identity might lead to violations of multipartite Bell inequalities such as the MABK inequality we consider in [Gra+20]. In [Gra+20] we show how one can restrict to rank-one projective measurements, thus excluding the identity, without loss of generality.

where $\Pi_{\pm 1}^{x,\alpha}$ are the projectors on the eigenvalues ± 1 of the qubit projective measurement defined by Alice's choice of input x and by the particular state ρ_α she is measuring.

We now fix α and proceed in specifying the form of the two-qubit state ρ_α (we omit the symbol α in the following). At the moment, we can only say that ρ_α is a normalized positive Hermitian operator acting on the four-dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Symmetrization of the marginal distributions: We define the planes individuated by the two measurements of Alice and of Bob to be the (x, y)-plane of the Bloch sphere. We can now assume w.l.o.g. that the marginal distributions of the outcomes, $p(a|x)$ and $p(b|y)$, are symmetrized. In other words, the expectation values of the corresponding observables are null:

$$\langle A_x \rangle = \langle B_y \rangle = 0 \quad \forall\, x, y \in \{0, 1\}, \tag{A.24}$$

where A_x and B_y are the observables of Alice and Bob, respectively, defining rank-one binary projective measurements in the (x, y)-plane. If (A.24) were not true, Alice and Bob could enforce it by agreeing on flipping their outcomes with probability 1/2 in every round. This classical procedure would not change the observed CHSH value (6.27) nor the QBER, since either both parties flip or none of them does. Additionally, it would require classical communication between Alice and Bob, known to Eve.

Given that the experiment statistics satisfies (A.24), we can assume that it is Eve herself who flips the outcomes in place of the parties. However, instead of doing this classically on the outcomes of the devices, she could provide Alice and Bob with a suitable state which already embodies the symmetry of the outcomes distributions. By calling ρ the generic state she initially prepares, the state she distributes that satisfies (A.24) is given by:

$$\bar{\rho} = \frac{1}{2} \left[\rho + Z_A \otimes Z_B \, \rho \, Z_A^\dagger \otimes Z_B^\dagger \right], \tag{A.25}$$

where Z_A, Z_B are Pauli operators on Alice's and Bob's qubits. As a matter of fact, the outcome of a measurement in the (x, y)-plane is flipped if one first applies the Z operator.

We remark that it is safe to assume that Eve distributes the state (A.25) since this is not disadvantageous to her. Indeed, her uncertainty on Alice's raw key bit R_A, quantified by the conditional von Neumann entropy $H(R_A|E)$, does not increase when she sends the state $\bar{\rho}$ instead of ρ. The proof of this fact follows the same lines of the proof given in section A.1, hence we omit it.

By expressing the initial generic state ρ in the Bell basis (3.15):

$$\rho = \sum_{i,j,k,l=0}^{1} \rho_{(ij),(kl)} \left|\psi_{ij}\right\rangle \left\langle\psi_{kl}\right| \quad \rho_{(ij),(kl)} \in \mathbb{C}, \tag{A.26}$$

and by substituting it into (A.25), we observe that all the coherences relative to Bell states such that $j \neq l$ are set to zero:

$$\bar{\rho} = \sum_{i,j,k=0}^{1} \rho_{(ij),(kj)} \left|\psi_{ij}\right\rangle \left\langle\psi_{kj}\right| . \tag{A.27}$$

The matrix representation of the state in (A.27) in the Bell basis is thus block-diagonal and reads as follows, upon relabelling the coefficients[2]:

$$\bar{\rho} = \begin{bmatrix} \lambda_{00} & r_0 + \mathbb{i}s_0 & 0 & 0 \\ r_0 - \mathbb{i}s_0 & \lambda_{10} & 0 & 0 \\ 0 & 0 & \lambda_{01} & r_1 + \mathbb{i}s_1 \\ 0 & 0 & r_1 - \mathbb{i}s_1 & \lambda_{11} \end{bmatrix}, \tag{A.28}$$

where λ_{ij}, r_j and s_j are real numbers.

Exploiting the orientation of the local reference frames: The state in (A.28) can be further reduced by carefully choosing the orientation of the parties' local reference frames. Indeed, although we already fixed the measurement directions of Alice and Bob to lie in the (x, y)-plane, we can still choose the orientation of the axes with respect to the measurement directions by applying rotations $R(\theta)$ along the z direction on the qubit spaces. In particular, the state distributed by Eve can be rotated w.l.o.g. as follows:

$$\bar{\rho}_+ = R_A(\theta_A) \otimes R_B(\theta_B)\, \bar{\rho}\, R_A^\dagger(\theta_A) \otimes R_B^\dagger(\theta_B), \tag{A.29}$$

where the rotation $R_A(\theta_A)$ acts on Alice's Hilbert space and is given by:

$$R_A(\theta_A) = \cos\left(\frac{\theta_A}{2}\right) \mathrm{id}_A + \mathbb{i} \sin\left(\frac{\theta_A}{2}\right) Z_A, \tag{A.30}$$

and similarly for Bob. The resulting rotated state $\bar{\rho}_+$ is still block-diagonal and reads:

$$\bar{\rho}_+ = \begin{bmatrix} \lambda'_{00} & r_0 + \mathbb{i}s'_0 & 0 & 0 \\ r_0 - \mathbb{i}s'_0 & \lambda'_{10} & 0 & 0 \\ 0 & 0 & \lambda'_{01} & r_1 + \mathbb{i}s'_1 \\ 0 & 0 & r_1 - \mathbb{i}s'_1 & \lambda'_{11} \end{bmatrix}, \tag{A.31}$$

[2] Recall that $\bar{\rho}$ is a Hermitian operator, hence the matrix representing it must be Hermitian.

where the new matrix coefficients are given by:

$$\lambda'_{ij} = \frac{1}{2}\left[\lambda_{0j} + \lambda_{1j} + (-1)^i(\lambda_{0j} - \lambda_{1j})\cos[\theta_j(\theta_A, \theta_B)] + 2(-1)^i s_j \sin[\theta_j(\theta_A, \theta_B)]\right] \tag{A.32}$$

$$s'_j = s_j \cos[\theta_j(\theta_A, \theta_B)] - \frac{1}{2}(\lambda_{0j} - \lambda_{1j})\sin[\theta_j(\theta_A, \theta_B)], \tag{A.33}$$

where the angle $\theta_j(\theta_A, \theta_B)$ is defined as:

$$\theta_j(\theta_A, \theta_B) := \theta_A + (-1)^j\theta_B. \tag{A.34}$$

From (A.33) we deduce that by choosing the rotation angles such that both the following conditions are verified[3]:

$$\theta_A + (-1)^j\theta_B = \arctan\frac{2s_j}{\lambda_{0j} - \lambda_{1j}} \quad \text{for } j = 0, 1, \tag{A.35}$$

we can set the imaginary parts of the off-diagonal terms to zero: $s'_0 = s'_1 = 0$. Thus, w.l.o.g. we can assume that the state distributed by Eve is of the form:

$$\bar{\rho}_+ = \begin{bmatrix} \lambda_{00} & r_0 & 0 & 0 \\ r_0 & \lambda_{10} & 0 & 0 \\ 0 & 0 & \lambda_{01} & r_1 \\ 0 & 0 & r_1 & \lambda_{11} \end{bmatrix}. \tag{A.36}$$

Moreover, by applying further rotations on (A.36) defined by angles $\tilde{\theta}_A$ and $\tilde{\theta}_B$ such that:

$$\tilde{\theta}_A + (-1)^j\tilde{\theta}_B = \pi, \tag{A.37}$$

we can exchange the position of the two diagonal terms λ_{0j} and λ_{1j} in (A.36), for $j = 0, 1$ (see (A.32)). This implies that we can assume w.l.o.g. that the diagonal elements in (A.36) are ordered as follows:

$$\lambda_{00} \geq \lambda_{10} \quad , \quad \lambda_{01} \geq \lambda_{11}. \tag{A.38}$$

[3] Note that this is possible since we have two linear conditions for two independent variables.

Independence from the off-diagonal terms: Finally, let us construct the state $\bar{\rho}_-$ starting from $\bar{\rho}_+$ given in (A.36) by replacing r_j with $-r_j$:

$$\bar{\rho}_- := \begin{bmatrix} \lambda_{00} & -r_0 & 0 & 0 \\ -r_0 & \lambda_{10} & 0 & 0 \\ 0 & 0 & \lambda_{01} & -r_1 \\ 0 & 0 & -r_1 & \lambda_{11} \end{bmatrix}. \tag{A.39}$$

We observe that the two states $\bar{\rho}_+$ and $\bar{\rho}_-$ yield the same probability distribution of the outcomes:

$$p(a,b)_{\bar{\rho}_+} = \mathrm{Tr}\left[\Pi_a \Pi_b \bar{\rho}_+\right] = \mathrm{Tr}\left[\Pi_a \Pi_b \bar{\rho}_-\right] = p(a,b)_{\bar{\rho}_-}, \tag{A.40}$$

where the projectors Π_a and Π_b represent Alice and Bob's projective measurements in the (x,y)-plane relative to some non-specified inputs. The projectors can be parametrized by writing the corresponding observables A and B as convex combinations of the Pauli operators X and Y:

$$\begin{aligned} A &= \cos(\varphi_A)X + \sin(\varphi_A)Y \\ B &= \cos(\varphi_B)X + \sin(\varphi_B)Y, \end{aligned} \tag{A.41}$$

for some unknown angles φ_A, φ_B. The eigenstates of the observables in (A.41) read:

$$\begin{aligned} |a\rangle_A &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a e^{\mathbb{i}\varphi_A} |1\rangle) \\ |b\rangle_B &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b e^{\mathbb{i}\varphi_B} |1\rangle) \end{aligned} \tag{A.42}$$

where the measurement outcomes are defined as $a, b \in \{0,1\}$ ($a = 0$ corresponds to eigenvalue $+1$ and $a = 1$ to eigenvalue -1). Then the projectors Π_a and Π_b are simply given by $\Pi_a = |a\rangle\langle a|_A$ and $\Pi_b = |b\rangle\langle b|_B$.

Furthermore, the states $\bar{\rho}_+$ and $\bar{\rho}_-$ provide Eve with the same information, i.e. their conditional entropies coincide:

$$H(R_A|E)_{\bar{\rho}_+} = H(R_A|E)_{\bar{\rho}_-}. \tag{A.43}$$

Additionally, it is not disadvantageous for Eve to prepare the balanced mixture:

$$\rho_\alpha := \frac{\bar{\rho}_+ + \bar{\rho}_-}{2}, \tag{A.44}$$

rather than preparing one of the two states with certainty, if she knows which of the two states she prepared:

$$H(R_A|E)_{\rho_\alpha} \leq H(R_A|E)_{\bar{\rho}_+}. \tag{A.45}$$

The proofs of the observations (A.40), (A.43) and (A.45) follow by direct computation and are omitted. Nevertheless, the interested reader can find analogous proofs in the Supplementary Information of our recent work [Gra+20], valid for the general N-party scenario.

We conclude that it is not restrictive to assume that Eve distributes to the parties the mixture (A.22) of two-qubit states ρ_α together with ancillae that fix the parties' possible measurements. Each state ρ_α is given by (A.44) and is diagonal in the Bell basis:

$$\rho_\alpha = \begin{bmatrix} \lambda_{00} & 0 & 0 & 0 \\ 0 & \lambda_{10} & 0 & 0 \\ 0 & 0 & \lambda_{01} & 0 \\ 0 & 0 & 0 & \lambda_{11} \end{bmatrix}, \tag{A.46}$$

with the conditions (A.38) on the diagonal elements. This concludes the proof. □

A.4 Lower Bound on the Conditional Entropy: Analytical Proof

The security of the DIQKD protocol presented in subsection 6.4.2 is based on the ability to lower bound the conditional von Neumann entropy $H(R_A|E)_{\rho_\alpha}$ as a function of the CHSH violation S_α, as discussed in section 6.5. In that section, the conditional entropy is simplified to (6.49):

$$H(R_A|E)_{\rho_\alpha} = 1 - H(\{\lambda_{ij}^\alpha\}) + h(\lambda_{00}^\alpha + \lambda_{01}^\alpha), \tag{A.47}$$

and its lower bound is obtained by solving the following optimization problem:

$$\begin{aligned} F(S_\alpha) := \min_{\{\lambda_{ij}^\alpha\}} & \; 1 - H(\{\lambda_{ij}^\alpha\}) + h(\lambda_{00}^\alpha + \lambda_{01}^\alpha) \\ \text{sub. to} & \quad \mathcal{S}_\alpha \geq S_\alpha \; ; \; \lambda_{0j}^\alpha \geq \lambda_{1j}^\alpha \; ; \; \sum_{i,j=0,1} \lambda_{ij}^\alpha = 1 \end{aligned} \tag{A.48}$$

where $\mathcal{S}_\alpha$ is the maximal CHSH violation given in (6.33) and reported here for completeness:

$$\mathcal{S}_\alpha = 2\sqrt{2}\max\left\{\sqrt{(\lambda_{00}^\alpha - \lambda_{11}^\alpha)^2 + (\lambda_{01}^\alpha - \lambda_{10}^\alpha)^2}, \sqrt{(\lambda_{00}^\alpha - \lambda_{10}^\alpha)^2 + (\lambda_{01}^\alpha - \lambda_{11}^\alpha)^2}\right\}. \tag{A.49}$$

Here we analytically derive the solution of the optimization problem in (A.48). We start by assuming that the CHSH value S_α is such that $S_\alpha \geq 2$, i.e. we assume that the CHSH inequality is violated. Otherwise, Eve would have full information on Alice's raw key bit R_A and the lower bound on the conditional entropy would be zero.

Because of the symmetry of the problem, we assume w.l.o.g. that $\lambda_{01}^{\alpha} \geq \lambda_{00}^{\alpha}$. Indeed, for every solution of (A.48) with $\lambda_{00}^{\alpha} \geq \lambda_{01}^{\alpha}$, there exists an equivalent solution –that leads to the same minimum– with $\lambda_{01}^{\alpha} \geq \lambda_{00}^{\alpha}$: the equivalent solution is obtained by relabelling $\lambda_{01}^{\alpha} \leftrightarrow \lambda_{00}^{\alpha}$[4].

By noticing that the second term in (A.49) is larger than the first if and only if $\lambda_{01}^{\alpha} \geq \lambda_{00}^{\alpha}$, we can simplify the maximal CHSH violation to:

$$\mathcal{S}_\alpha = 2\sqrt{2}\sqrt{(\lambda_{00}^{\alpha} - \lambda_{10}^{\alpha})^2 + (\lambda_{01}^{\alpha} - \lambda_{11}^{\alpha})^2}. \tag{A.50}$$

Then, a necessary condition for $S_\alpha \geq 2$ can be derived by upper bounding (A.50) as follows:

$$2 \leq S_\alpha \leq \mathcal{S}_\alpha \leq 2\sqrt{2}\sqrt{(\lambda_{00}^{\alpha})^2 + (\lambda_{01}^{\alpha})^2} \leq 2\sqrt{2}\sqrt{\lambda_{01}^{\alpha}(\lambda_{01}^{\alpha} + \lambda_{00}^{\alpha})} \leq 2\sqrt{2}\sqrt{\lambda_{01}^{\alpha}}, \tag{A.51}$$

which implies the following necessary condition on λ_{01}^{α}:

$$\lambda_{01}^{\alpha} \geq \frac{1}{2}. \tag{A.52}$$

Consider the following class of states parametrized by $\nu \in [\frac{1}{2}, 1]$:

$$\tau(\nu) = (1-\nu)|\psi_{00}\rangle\langle\psi_{00}| + \nu|\psi_{01}\rangle\langle\psi_{01}|, \tag{A.53}$$

whose maximal CHSH violation (A.49) reads:

$$\mathcal{S}_\tau(\nu) = 2\sqrt{2}\sqrt{\nu^2 + (1-\nu)^2}. \tag{A.54}$$

It is straightforward to verify, by using the last expression, that

$$\mathcal{S}_\tau(\lambda_{01}^{\alpha}) \geq \mathcal{S}_\alpha \quad \forall\, \rho_\alpha, \tag{A.55}$$

where $\mathcal{S}_\alpha$ is given in (A.50). Moreover, the entropy (A.47) of the states (A.53) reads:

$$H(X|E)_\tau(\nu) = 1 - h(\nu), \tag{A.56}$$

where we used the binary entropy $h(x) = -x\log x - (1-x)\log(1-x)$.

By definition of the optimization problem (A.48), the solution of the optimization for a given S_α is upper bounded by the entropy of any particular state with $\mathcal{S}_\alpha = S_\alpha$. Thus for the states (A.53) we have:

$$F(S_\alpha) \leq H(R_A|E)_\tau(\nu_\alpha) \tag{A.57}$$

[4] Note that the relabelling does not modify the maximal CHSH violation (A.49).

where ν_α is fixed such that the maximal violation $\mathcal{S}_\tau(\nu_\alpha)$ of the state $\tau(\nu_\alpha)$ is exactly given by S_α:

$$\mathcal{S}_\tau(\nu_\alpha) = 2\sqrt{2}\sqrt{\nu_\alpha^2 + (1-\nu_\alpha)^2} = S_\alpha, \tag{A.58}$$

where we choose the solution $\nu_\alpha \geq 1/2$.

By proving the following result (with the assumption $\lambda_{01}^\alpha \geq \lambda_{00}^\alpha$ and (A.52)):

$$H(R_A|E)_{\rho_\alpha} \geq H(R_A|E)_\tau(\lambda_{01}^\alpha) \quad \forall\, \rho_\alpha \tag{A.59}$$

we obtain the solution of the optimization problem. In order to realize this, let us use the last expression on the state ρ_α^*, which is the solution of the minimization in (A.48):

$$\begin{aligned} F(S_\alpha) = H(R_A|E)_{\rho_\alpha^*} &\geq H(R_A|E)_\tau(\lambda_{01}^{\alpha,*}) \\ &\geq H(R_A|E)_\tau(\nu_\alpha). \end{aligned} \tag{A.60}$$

The last inequality in (A.60) is motivated by the following observations. (i) by applying (A.55) to the state ρ_α^*, we obtain $\mathcal{S}_\tau(\lambda_{01}^{\alpha,*}) \geq \mathcal{S}_{\alpha,*} \geq S_\alpha$, which combined with (A.58) implies that $\lambda_{01}^{\alpha,*} \geq \nu_\alpha$ since $\mathcal{S}_\tau(\nu)$ in (A.54) is monotonically increasing in the interval $\nu \in [\frac{1}{2}, 1]$. (ii) the entropy $H(R_A|E)\tau(\nu)$ in (A.56) is monotonically increasing in the interval $\nu \in [\frac{1}{2}, 1]$. The two observations lead to the second inequality in (A.60).

By combining (A.60) with (A.57), we obtain the desired lower bound:

$$\begin{aligned} F(S_\alpha) &= H(R_A|E)_\tau(\nu_\alpha) = 1 - h(\nu_\alpha) \\ &= 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{S_\alpha}{2}\right)^2 - 1}\right), \end{aligned} \tag{A.61}$$

where the last equality is obtained by reverting Eq. (A.58).

The bound (A.61) is *tight*. Indeed, for every violation S_α, there exists a state $\tau(\nu_\alpha)$ such that its entropy coincides with the bound and such that it can produce a violation equal to S_α, thanks to $\mathcal{S}_\tau(\nu_\alpha) = S_\alpha$ (A.58) and to the fact that the maximal CHSH violation (A.49) is achievable.

We are left to prove the inequality in (A.59), which can be made explicit by using (A.47) and (A.56):

$$D := h(\lambda_{01}^\alpha) - H(\{\lambda_{ij}^\alpha\}) + h(\lambda_{00}^\alpha + \lambda_{01}^\alpha) \geq 0. \tag{A.62}$$

We simplify the first two terms in D:

$$h(\lambda_{01}^{\alpha}) - H(\{\lambda_{ij}^{\alpha}\}) = -(1-\lambda_{01}^{\alpha})\log(1-\lambda_{01}^{\alpha}) + \sum_{(i,j)\neq(0,1)} \lambda_{ij}^{\alpha}\log\lambda_{ij}^{\alpha}. \tag{A.63}$$

Now we apply Jensen's inequality:

$$f(x+y) \geq \frac{f(2x)+f(2y)}{2} \quad \text{for} \quad f(x) = -x\log x, \tag{A.64}$$

to the last term in (A.62):

$$\begin{aligned} h(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha}) &= -(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha})\log(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha}) + f(\lambda_{10}^{\alpha}+\lambda_{11}^{\alpha}) \\ &\geq -(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha})\log(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha}) - \lambda_{10}^{\alpha}\log(2\lambda_{10}^{\alpha}) - \lambda_{11}^{\alpha}\log(2\lambda_{11}^{\alpha}) \\ &= -(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha})\log(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha}) - (1-\lambda_{00}^{\alpha}-\lambda_{01}^{\alpha}) \\ &\quad - \lambda_{10}^{\alpha}\log(\lambda_{10}^{\alpha}) - \lambda_{11}^{\alpha}\log(\lambda_{11}^{\alpha}). \end{aligned} \tag{A.65}$$

By combining (A.63) and (A.65) in (A.62) we get:

$$\begin{aligned} D &\geq -(1-\lambda_{01}^{\alpha})\log(1-\lambda_{01}^{\alpha}) - (\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha})\log(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha}) - (1-\lambda_{00}^{\alpha}-\lambda_{01}^{\alpha}) \\ &\quad + \lambda_{00}^{\alpha}\log\lambda_{00}^{\alpha} \\ &= -(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha})\log(\lambda_{00}^{\alpha}+\lambda_{01}^{\alpha}) - (1-\lambda_{01}^{\alpha})\log[2(1-\lambda_{01}^{\alpha})] + \lambda_{00}^{\alpha}\log(2\lambda_{00}^{\alpha}) \\ &=: g(\lambda_{01}^{\alpha}, \lambda_{00}^{\alpha}). \end{aligned} \tag{A.66}$$

In the last expression we defined the function $g(x,y)$:

$$g(x,y) = -(x+y)\log(x+y) - (1-x)\log[2(1-x)] + y\log(2y), \tag{A.67}$$

and we will analyse it in the ranges of interest for the variables $x = \lambda_{01}^{\alpha}$ and $y = \lambda_{00}^{\alpha}$, i.e.: $1/2 \leq x \leq 1$, $0 \leq y \leq 1-x$.

In these ranges the function in (A.67) is concave in x since its second derivative is always negative:

$$\frac{\partial^2 g(x,y)}{\partial x^2} = -\frac{1}{\ln(2)}\left(\frac{1}{1-x} + \frac{1}{x+y}\right) < 0. \tag{A.68}$$

Consider the points at the boundary $x+y=1$, for which we get $g(1-y,y)=0$. Thanks to the concavity of $g(x,y)$, it holds that:

$$g\left(p\frac{1}{2} + (1-p)(1-y), y\right) \geq pg\left(\frac{1}{2}, y\right) + (1-p)g(1-y,y), \quad 0 \leq p \leq 1$$

or equivalently that:

$$g(x,y) \geq \left(\frac{1-x-y}{\frac{1}{2}-y}\right) g\left(\frac{1}{2},y\right). \tag{A.69}$$

Note that in the parameter regimes of x and y it holds that

$$0 \leq \left(\frac{1-x-y}{\frac{1}{2}-y}\right) \leq 1. \tag{A.70}$$

We finally analyse the properties of $g(\frac{1}{2},y)$, which is convex in y since its second derivative is always positive:

$$\frac{\partial^2 g(\frac{1}{2},y)}{\partial y^2} = \frac{1}{y\ln(2)+y^2\ln(4)} > 0. \tag{A.71}$$

A convex function has a unique minimum if it exists in the parameter regime. In our case this is given by:

$$\frac{\partial g(\frac{1}{2},y)}{\partial y} = \log(2y) - \log(\frac{1}{2}+y) \overset{!}{=} 0 \quad \Leftrightarrow \quad y = \frac{1}{2} \tag{A.72}$$

for which $g(\frac{1}{2},\frac{1}{2}) = 0$ holds. Thus in general it holds:

$$g\left(\frac{1}{2},y\right) \geq 0. \tag{A.73}$$

By combining these considerations we prove the inequality in (A.62):

$$\begin{aligned} D &\overset{(A.66)}{\geq} g(\lambda_{01}^{\alpha},\lambda_{00}^{\alpha}) \\ &\overset{(A.69)}{\geq} \left(\frac{1-\lambda_{01}^{\alpha}-\lambda_{00}^{\alpha}}{\frac{1}{2}-\lambda_{00}^{\alpha}}\right) g\left(\frac{1}{2},\lambda_{00}^{\alpha}\right) \\ &\geq 0, \end{aligned} \tag{A.74}$$

where in the last inequality we used the fact that the pre-factor is positive (A.70) and that $g(\frac{1}{2},\lambda_{00}^{\alpha})$ is lower bounded by zero (A.73). This concludes the proof of inequality (A.59), thus completing the analytical solution of the optimization problem in (A.48).

B Finite-key effects in multipartite quantum key distribution protocols

Title:	Finite-key effects in multipartite quantum key distribution protocols
Authors:	Federico Grasselli, Hermann Kampermann and Dagmar Bruß
Journal:	New Journal of Physics
Impact factor:	3.783 (2018)
Date of submission:	24 July 2018
Publication status:	Published
Contribution by FG:	First author (input approx. 85%)

This publication corresponds to reference [GKB18]. A summary of its content is presented in chapter 7.

The research objective initially consisted in performing a finite-key analysis of the multipartite QKD protocol introduced in [Epp+17], and was set by my co-authors long before the project started. My co-authors also suggested me some relevant papers from which I could draw inspiration to achieve the project's goal and were available to discuss my initial doubts on some security aspects of QKD. I independently generalized the concepts of finite-key security to multipartite QKD protocols (apart from Lemma 3 kindly provided by Prof. Renato Renner) and I ideated the new N-partite BB84 protocol. I proved the finite-key security of both the N-BB84 protocol and of the N-six-state protocol introduced in [Epp+17]. I investigated the performance of the two protocols with self-produced numerical simulations and obtained the plots comparing their performances. I drew the conclusions of the research study and welcomed suggestions from my co-authors on potential future developments. I wrote the whole manuscript which was then proofread by my co-authors and improved thanks to their comments.

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
24 July 2018

REVISED
6 October 2018

ACCEPTED FOR PUBLICATION
29 October 2018

PUBLISHED
12 November 2018

Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Finite-key effects in multipartite quantum key distribution protocols

Federico Grasselli , **Hermann Kampermann** and **Dagmar Bruß**

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany

E-mail: federico.grasselli@hhu.de

Keywords: quantum key distribution, multipartite qkd, finite-key effects, security analysis, finite resources, uncertainty relation for smooth entropies, conference key agreement

Abstract

We analyze the security of two multipartite quantum key distribution (QKD) protocols, specifically we introduce an N-partite version of the BB84 protocol and we discuss the N-partite six-state protocol proposed by Epping *et al* (2017 *New J. Phys.* **19** 093012). The security analysis proceeds from the generalization of known results in bipartite QKD to the multipartite scenario, and takes into account finite resources. In this context we derive a computable expression for the achievable key rate of both protocols by employing the best-known strategies: the uncertainty relation and the postselection technique. We compare the performances of the two protocols both for finite resources and infinitely many signals.

Quantum key distribution (QKD) represents one of the primary applications of quantum information science. Since the proposal of the first QKD protocols [1, 2], major advancements have been achieved both on the theoretical and experimental side [3, 4]. A QKD protocol provides a systematic procedure through which two honest parties (Alice and Bob) generate a secret shared key, when connected by an insecure quantum channel and an authenticated insecure classical channel.

Recently the generalization of such protocols to multipartite schemes has been investigated [5, 6]. It has been shown that there are quantum-network configurations [5] or noise regimes [6] in which the execution of a multipartite scheme is advantageous with respect to establishing a multipartite secret key via many independent bipartite protocols. However, the analysis of multipartite QKD protocols has only been carried out in the unrealistic scenario of infinitely many signals exchanged through the quantum channel.

We compare the performances of two multipartite QKD protocols, which constitute the N-partite versions of the asymmetric BB84 [1] and the asymmetric six-state protocol [7], and will be denoted as N-BB84 and N-six-state protocol. While the N-six-state protocol was first proposed in [5], the N-BB84 constitutes a novel multipartite QKD protocol.

Our analysis is conducted in the practical case of a finite amount of resources (signals) at the N parties' disposal. The action of a potential eavesdropper (Eve) on the insecure quantum channel is not restricted at all, as she is allowed to perform any kind of attack (coherent attacks) on the exchanged signals. What is assumed is that the parties have access to true randomness and that the devices performing measurements on the quantum systems work according to their ideal functionality.

The article is structured as follows. In section 1 we extend notions and results of bipartite QKD security analysis to the multipartite scenario. In section 2 we review the N-six-state protocol and introduce the N-BB84 protocol. Then we obtain a computable expression for their secret key lengths in the case of finite resources. In section 3 we compare the achievable key rates of the two NQKD protocols in the presence of finite and infinite resources. We conclude the article in section 4.

1. Multipartite QKD: general framework and achievable key length

Throughout the article we refer to the parties involved in an N-partite QKD protocol (NQKD) in the following way: A for Alice, $\mathbf{B}$ for the set of $N-1$ Bobs, B_i for Bob in position i and E for the eavesdropper Eve. The definitions of distance and entropic quantities employed in this section are given in appendix A.

© 2018 The Author(s). Published by IOP Publishing Ltd on behalf of Deutsche Physikalische Gesellschaft

The aim of an NQKD protocol is to establish a common secret key, sometimes also referred to as conference key, between all N (trusted) parties. We consider the following general NQKD protocol. Although the protocol is presented in an entanglement-based view for clarity, there exists an equivalent prepare-and-measure scheme which requires the adoption of multipartite entangled states only for a small fraction of rounds (see the protocols in section 2).

The protocol starts with the distribution of a finite number of signals -described by genuinely multipartite entangled states- over the insecure quantum channel. All parties perform local measurements on their respective quantum systems, collecting classical data. A short preshared random key indicates to the parties the type of measurement to be performed on each individual state they hold (more on this in section 2).

In the parameter estimation (PE) step the parties reveal a random sample of the collected data, over the insecure classical channel. This allows them to estimate the noise occurring in the quantum channel and thus to determine the secret key length. At this point the raw keys held by the parties are partially correlated and partially secret. In order to correct the errors in the raw keys, A performs pairwise an information reconciliation procedure with every B_i. The procedure consists in some classical communication occurring between A and B_i, which allows B_i to compute a guess of A's raw key. We will refer to this procedure as error correction (EC). At last the shared raw key is turned into a secret key with privacy amplification (PA). Each party applies the same randomly chosen hash function to his/her raw key, where the final length of the key depends on the error rates observed in PE and the desired level of security. Finally all parties share the same secret key.

During the execution of the NQKD protocol, one or more of the described subprotocols might fail to produce the desired output, thus causing the abortion of the entire protocol. In the security analysis this is accounted for by the definition of robustness:

Definition 1 [8]. An NQKD protocol is ε_{rob}-robust on $\rho_{A\mathbf{B}}$ if, for inputs defined by $\rho_{A\mathbf{B}}$, the probability that the protocol aborts is at most ε_{rob}.

In order to study the effects of finite resources on an NQKD protocol, one needs to extend the concept of ε-security of a key [8] to the multipartite scenario:

Definition 2. [8, 9]. Let $\rho_{A\mathbf{B}E}$ be a density operator. Any NQKD protocol, which is ε_{rob}-robust on $\text{Tr}_E[\rho_{A\mathbf{B}E}]$, is said to be ε_{tot}-secure on $\rho_{A\mathbf{B}E}$ if the following inequality holds:

$$(1-\varepsilon_{\text{rob}})\frac{1}{2}\|\rho_{S_A\mathbf{S_B}E'}-\rho_{\mathbf{U}}\otimes\rho_{E'}\|\leqslant\varepsilon_{\text{tot}}, \tag{1.1}$$

where $\rho_{S_A\mathbf{S_B}E'}$ is the density operator describing the final keys held by the N parties and Eve's enlarged subsystem $\mathcal{H}_{E'}$ (including the information of the classical channels), while $\rho_{\mathbf{U}}$ is the uniform state on the key space of the N parties:

$$\rho_{\mathbf{U}}\equiv\sum_{s\in\mathcal{S}}\frac{1}{|\mathcal{S}|}\bigotimes_{i=1}^{N}|s\rangle\langle s| \tag{1.2}$$

with $\mathcal{S}$ the set of possible secret keys.

The total security parameter ε_{tot} quantifies the deviation of the NQKD protocol from an ideal protocol, i.e. one that either outputs a set of perfectly-correlated and fully-secret keys or aborts. In other words, an NQKD protocol is ε_{tot}-secure if it behaves like an ideal protocol except for probability ε_{tot}. With this definition, the parameter that actually accounts for the correctness and secrecy of the protocol when it does not abort, is: $\varepsilon_{\text{tot}}/(1-\varepsilon_{\text{rob}})$. An NQKD protocol may deviate from an ideal one if, for instance, its EC procedure fails to correct all the errors between A and $\mathbf{B}$'s strings. In particular, if the probability that at least one B_i holds a different string than A—after EC—is ε_{EC}, then the NQKD protocol is ε_{tot}-secure, with $\varepsilon_{\text{tot}}\geqslant\varepsilon_{\text{EC}}$. Formally, the EC failure probability is defined as:

Definition 3 [8]. Let $P_{X\mathbf{K}}$ be a probability distribution. Any set of EC protocols $\{\mathsf{EC}_i\}_{i=1}^{N-1}$, which is ε_{rob}-robust on $P_{X\mathbf{K}}$, is said to be ε_{EC}-secure on $P_{X\mathbf{K}}$ if the following holds:

$$(1-\varepsilon_{\text{rob}})\Pr[\exists\, i\in\{1,\ldots,N-1\}:\,\hat{k}_i\neq x]\leqslant\varepsilon_{\text{EC}}, \tag{1.3}$$

where the guess $\hat{k}_i$ is computed by B_i according to protocol EC_i, and the probability is computed for inputs $(x,\,\mathbf{k})$ chosen according to $P_{X\mathbf{K}}$, conditioned on the fact that no EC_i aborted. If $\{\mathsf{EC}_i\}_{i=1}^{N-1}$ is ε_{EC}-secure for any probability distribution, it is ε_{EC}-fully secure.

In this article we assume that the NQKD protocol may abort only during the EC procedure. Thus the abortion probability of the chosen set of EC procedures is also the abortion probability of the whole protocol[1].

The classical communication occurring during EC contains some information about the key. The amount of information about the key that is leaked to E from the insecure classical channel is quantified by the leakage:

Definition 4 [8]. Let $\{\mathsf{EC}_i\}_{i=1}^{N-1}$ be a set of EC protocols. The NQKD protocol adopting such a set of protocols for EC has leakage:

$$\mathrm{leak}^{\mathrm{NQKD}}_{\{\mathsf{EC}_i\}} \equiv \log_2|\mathcal{C}_{1,\ldots,N-1}| - \min_{x,\mathbf{k}} H_{\min}(P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}}), \tag{1.4}$$

where $\mathcal{C}_{1,\ldots,N-1}$ is the set of $(N-1)$-tuples representing all possible communication transcripts allowed by the chosen EC protocols, i.e.:

$$\mathcal{C}_{1,\ldots,N-1} = \{(c_1,\ldots,c_{N-1}) : P_{\mathbf{C}}(c_1,\ldots,c_{N-1}) \neq 0\}, \tag{1.5}$$

$P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}}$ is the transcripts' distribution conditioned on A and $\mathbf{B}$'s raw keys and $H_{\min}(P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}})$ is the min-entropy defined on a probability distribution (A.10), (A.11).

We now present our results on the achievable key length (theorem 1) and the minimum leakage (theorem 2) of a general $\varepsilon_{\mathrm{tot}}$-secure NQKD protocol, which constitute a generalization of analogous results [8, lemmas 6.4.1 and 6.3.4] valid for bipartite QKD. The general structure of the proofs is derived from the bipartite case, but deals with the new definitions of security and leakage (definitions 2, 3, 4) for multipartite schemes. As in the bipartite case, the security of an NQKD protocol can be inferred by correctness and secrecy (appendix B). While the correctness of a protocol is determined by its EC procedure, the secrecy is linked to the final-key length via the leftover hashing lemma [8, corollary 5.6.1]. In fact, in PA the parties map their shared key to another key which is short enough to be secret (i.e. unknown to the eavesdropper Eve). In theorem 1 we present the achievable key length of an $\varepsilon_{\mathrm{tot}}$-secure NQKD protocol for a general two-way EC procedure, while typically only the special case of one-way EC is addressed. This is achieved thanks to the result on the information leakage with two-way EC presented in appendix E [10]. A detailed version of the proofs of theorems 1 and 2 is presented in appendix B.

Theorem 1. *Let: $\bar{\varepsilon} > 0$, $\varepsilon_{\mathrm{EC}} > 0$, $\varepsilon_{\mathrm{PA}} > 0$, $\varepsilon_{\mathrm{rob}} \geqslant 0$ and $\rho_{A\mathbf{B}E}$ be a density operator. Let $\rho_{X\mathbf{K}E}$ be the output—prior to EC and PA—of an NQKD protocol applied to $\rho_{A\mathbf{B}E}$. If the two-way EC protocol $\{\mathsf{EC}_i\}_{i=1}^{N-1}$ is $\varepsilon_{\mathrm{EC}}$-secure and $\varepsilon_{\mathrm{rob}}$-robust on the distribution defined by $\rho_{X\mathbf{K}}$, and if $\mathsf{PP}_{\{\mathsf{EC}_i\},\mathcal{F}}$ is the post-processing protocol defined by the set of EC protocols and by the set of two-universal hash functions $\mathcal{F}$ with co-domain $\{0,1\}^{\ell}$ such that[2] the secret key length ℓ fulfills:*

$$\ell \leqslant H^{\bar{\varepsilon},\mathrm{P}}_{\min}(\rho_{XE}|E) - \mathrm{leak}^{\mathrm{NQKD}}_{\{\mathsf{EC}_i\}} - 2\log_2\frac{1-\varepsilon_{\mathrm{rob}}}{2\,\varepsilon_{\mathrm{PA}}}, \tag{1.6}$$

then the NQKD protocol is $\varepsilon_{\mathrm{tot}}$-secure on $\rho_{A\mathbf{B}E}$, where $\varepsilon_{\mathrm{tot}}$ is defined as: $\varepsilon_{\mathrm{tot}} = 2\bar{\varepsilon} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}}$.

If one restricts to one-way EC, the same result holds but with the $\bar{\varepsilon}$-environment of the min-entropy defined via the trace distance.

Theorem 2. *Given a probability distribution $P_{X\mathbf{K}}$, there exists a one-way EC protocol that is: $\varepsilon_{\mathrm{EC}}$-fully secure, $2(N-1)\varepsilon'$-robust on $P_{X\mathbf{K}}$, and has leakage:*

$$\mathrm{leak}^{\mathrm{NQKD}}_{\mathrm{EC}} \leqslant \max_i H^{\varepsilon'}_0(P_{XK_i}|K_i) + \log_2\frac{2(N-1)}{\varepsilon_{\mathrm{EC}}}. \tag{1.7}$$

The upper bound in theorem 2 is independent of the EC protocol, thus also bounds the leakage of an *optimal* one-way EC protocol which is $\varepsilon_{\mathrm{EC}}$-fully secure and $2(N-1)\varepsilon'$-robust on $P_{X\mathbf{K}}$.

2. N-BB84 and N-six-state protocol

Here we present the two NQKD protocols whose performance will be investigated in section 3. We introduce the N-BB84 protocol which is the N-partite version of the asymmetric BB84 protocol [1]:

[1] Note, however, that a higher global abortion probability for fixed security parameter $\varepsilon_{\mathrm{tot}}$ may lead to higher key rates.

[2] The $\bar{\varepsilon}$-environment of the min-entropy is defined via the purified distance, see appendix A.

N-BB84 protocol.

(i) Distribution of N-qubit GHZ states:

$$|\mathrm{GHZ}\rangle_N \equiv \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}) \tag{2.1}$$

for L rounds.

(ii) In 1st-type rounds each party measures in the Z-basis, in 2nd-type rounds—which occur with probability p[3]—each party measures in the X-basis. The total number of 2nd-type rounds is: $m = Lp$.

(iii) Parameter estimation:

(a) Computation of $Q_{AB_i}^m = (1 - \langle Z_A Z_{B_i}\rangle_m)/2$ for every B_i, where $Z_A Z_{B_i}$ is averaged over m 1st-type rounds randomly chosen by Alice. In the ideal situation: $Q_{AB_i}^m = 0$.

(b) Computation of $Q_X^m = (1 - \langle X^{\otimes N}\rangle_m)/2$, where $X^{\otimes N}$ is averaged over the 2nd-type rounds. Note that in the ideal situation: $Q_X^m = 0$ [5].

(iv) The secret key is obtained from the remaining data of $n = L - 2m$ 1st-type rounds.

(v) Classical post-processing:

(a) A sends the same EC information to every B_i.

(b) A and $\mathbf{B}$ apply the same two-universal hash function to their corrected data.

Remarks. Note that the frequencies $Q_{AB_i}^m$ and Q_X^m observed in the PE step are the fraction of discordant Z-outcomes between A and B_i and the frequency of the outcome -1 when the parties measure the operator $X^{\otimes N}$, respectively.

In an equivalent prepare-and-measure scheme, Alice directly produces the $(N - 1)$-qubit projection of the GHZ state according to her fictitious random outcome and distributes it to the Bobs. In particular, she prepares product states if the Z-basis is chosen and multipartite entangled states when the X-basis is picked. Thus the production of multipartite entangled states is only required for Lp rounds, while in all other rounds product states are prepared [5].

For the protocol's security to hold, the preshared secret key indicating to the parties the 2nd-type rounds needs to be refreshed at every new execution of the protocol. Therefore, the net amount of new secret key bits produced by one run of the protocol is obtained by subtracting $L \cdot h(p)$ bits from the final key length presented in section 2.1. We take into account this term for both protocols when investigating their performance in section 3.

We refer to [5] for a detailed description of the steps characterizing the N-six-state protocol. However, the only actual differences with respect to the N-BB84 protocol are that: in the 2nd-type rounds each party measures randomly in the X- or Y-basis and all parties jointly flip their Z-measurement outcomes with probability $1/2$. The bits to be flipped can be announced by Alice after the distribution and measurement of the states. These operations enable the implementation of the extended depolarization procedure [5] on the classical data, without adding further quantum gates.

The frequencies observed in the PE step of the N-six-state protocol are again $Q_{AB_i}^m$ and $Q_X^{m'}$[4], plus Q_Z^m, i.e. the fraction of rounds in which at least one Bob measured a different Z-outcome than A's. We will refer to the corresponding probabilities as: P_{AB_i}, P_X and P_Z.

The frequencies observed in the PE steps of both protocols enable to quantify the amount of noise occurring in the quantum channel. However, these statistics are collected on finite-size samples, thus they only represent an estimate of the channel's noise. In appendix C we quantitatively describe how the finite statistics of PE characterize the quantum channel's noise, for both NQKD protocols.

2.1. Computable key length

In order to employ the results of section 1 in a performance comparison of the two NQKD protocols one needs to characterize E's knowledge about the key. This is achieved by assigning the noise in the quantum channel to eavesdropping. This means, in practice, that one can bound the unknown entropies with quantities exclusively

[3] $L \cdot h(p)$ bits of preshared secure key are used to mark the 2nd-type rounds.

[4] Since the value of $X^{\otimes N}$ must be registered only when an even number of parties measured in the Y basis, $m' = m/2$. See [5] for further details.

depending on the noise affecting the quantum channel. In turn, the channel's noise is characterized by the finite PE statistics, as explained above.

As a result, we obtain a computable expression for the achievable key length of both protocols, that is an expression solely depending on the observed PE statistics, the desired level of security, and the total number of quantum signals.

The techniques we adopt to obtain a computable key length are the following. We employ the uncertainty relation (for smooth entropies) presented in [11] for the N-BB84 protocol, thus showing its first application to NQKD. For the N-six-state protocol we instead employ the Postselection technique (PS) [12] in combination with the asymptotic equipartition property [8], and we exploit the symmetries induced by the extended depolarization procedure.

We arrive at the computable key lengths of the N-BB84 and N-six-state protocol:

Theorem 3. *The N-BB84 protocol, with the optimal one-way EC protocol (which is $\varepsilon_{\mathrm{EC}}$-fully secure and $2(N-1)\varepsilon_{\mathrm{PE}}$ -robust) and where the secret key generated by two-universal hashing has length*

$$\ell = n\left[1 - h(Q_X^m + 2\xi(\varepsilon_x, n, m)) - \max_i h(Q_{AB_i}^m + 2\xi(\varepsilon_z, n, m))\right] - \log_2\frac{2(N-1)}{\varepsilon_{\mathrm{EC}}} - 2\log_2\frac{1-2(N-1)\varepsilon_{\mathrm{PE}}}{2\ \varepsilon_{\mathrm{PA}}}, \tag{2.2}$$

is $\varepsilon_{\mathrm{tot}}$-secure with $\varepsilon_{\mathrm{tot}} = 2\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}}$, where $\varepsilon_{\mathrm{PE}}$ is defined as (C.16):

$$\varepsilon_{\mathrm{PE}} \equiv \sqrt{(N-1)\varepsilon_z + \varepsilon_x} \tag{2.3}$$

and $\xi(\varepsilon, n, m)$ as (C.4):

$$\xi(\varepsilon, n, m) \equiv \sqrt{\frac{(n+m)(m+1)}{8nm^2}\ln\left(\frac{1}{\varepsilon}\right)}. \tag{2.4}$$

Theorem 4. *The N -six-state protocol, with the optimal one-way EC protocol (which is $\varepsilon_{\mathrm{EC}}$-fully secure and $2(N-1)\varepsilon_{\mathrm{PE}}$ -robust) and where the secret key generated by two-universal hashing has length*

$$\ell = n\inf_{\Gamma_{\mathrm{PE}}}\left[\left(1-\frac{P_Z}{2}-P_X\right)\log_2\left(1-\frac{P_Z}{2}-P_X\right) + \left(P_X-\frac{P_Z}{2}\right)\log_2\left(P_X-\frac{P_Z}{2}\right) + (1-P_Z)(1-\log_2(1-P_Z)) - 5\sqrt{\frac{\log_2(1/\bar{\varepsilon})}{n}} - \max_i h(P_{AB_i}) - \log_2(5)\sqrt{\frac{2\log_2(1/(2\varepsilon_{\mathrm{PE}}))}{n}}\right] - \log_2\frac{2(N-1)}{\varepsilon_{\mathrm{EC}}} - 2\log_2\frac{1-2(N-1)\varepsilon_{\mathrm{PE}}}{2\ \varepsilon_{\mathrm{PA}}} - 2(2^{2N}-1)\log_2(L+1), \tag{2.5}$$

is $\varepsilon_{\mathrm{tot}}$-secure with $\varepsilon_{\mathrm{tot}} = (L+1)^{(2^{2N}-1)}(2\bar{\varepsilon} + \varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}})$, where P_X, P_{AB_i} and P_Z are minimized over the set:

$$\Gamma_{\mathrm{PE}} \equiv \left\{P_{AB_i}, P_Z, P_X : \frac{1}{2}|Q_{AB_i}^m - P_{AB_i}| \leqslant \eta(\varepsilon_z, 2, m)\forall i \wedge \frac{1}{2}|Q_X^{m'} - P_X| \leqslant \eta(\varepsilon_x, 2, m') \wedge \frac{1}{2}|Q_Z^m - P_Z| \leqslant \eta(\varepsilon_z', 2, m)\right\}. \tag{2.6}$$

The parameters ε_x, ε_z, ε_z' are linked to $\varepsilon_{\mathrm{PE}}$ via (C.18):

$$\varepsilon_{\mathrm{PE}} \equiv \varepsilon_z' + (N-1)\varepsilon_z + \varepsilon_x \tag{2.7}$$

while $\eta(\varepsilon, d, m)$ is defined as (C.19):

$$\eta(\varepsilon, d, m) \equiv \sqrt{\frac{\ln(1/\varepsilon) + d\ln(m+1)}{8m}}. \tag{2.8}$$

For the derivation of theorems 3 and 4, we refer to appendix D.

3. Performance comparison

We compare the performances of the two NQKD protocols by studying their secret key rates, i.e. the fraction of shared secret bits per transmitted quantum signal (ℓ/L). For this purpose we investigate the computable key lengths (2.2) and (2.5)—corrected with the term '$-L\cdot h(p)$' that accounts for the preshared secret key- for a given number of parties N and a fixed total security parameter $\varepsilon_{\mathrm{tot}}$.

In order to carry out a fair comparison, we assume that the PE statistics of both protocols are generated by the same error model.

3.1. Error model

We assume that in every distribution round white noise acted on the ideal state and that the action of the noise is the same in every round[5]. The total distributed state over all rounds is a product state: $\rho_{A\mathbf{B}}^{\otimes L}$, where the single-round state is given by:

$$\rho_{A\mathbf{B}} = (1-\nu)|\mathrm{GHZ}\rangle_N\langle\mathrm{GHZ}|_N + \nu\,\frac{\mathrm{id}_{A\mathbf{B}}}{2^N}, \tag{3.1}$$

where ν is the noise parameter and $|\mathrm{GHZ}\rangle_N$ is the GHZ state of N qubits (2.1).

The state (3.1) can be seen as the result of the action of a depolarizing channel on the whole N-qubit system, such that it is diagonal in the GHZ basis [5] and the probabilities P_{AB_i} (of A and B_i having discordant Z-outcomes), P_X (of having the outcome -1 when the parties measured $X^{\otimes N}$) and P_Z (of having at least one Bob with a different Z-outcome than A's) are given by:

$$P_{AB_i} = \nu/2 \quad \forall\, i, \tag{3.2}$$

$$P_X = P_{AB}, \tag{3.3}$$

$$P_Z = \frac{2^N-2}{2^{N-1}}P_{AB}. \tag{3.4}$$

For ease of notation we will drop the index i in the probabilities P_{AB_i}. We assume that the frequencies $Q_{AB_i}^m$, Q_X^m and Q_Z^m observed in the PE step of both protocols are linked by the same relations (3.3), (3.4) that hold for the corresponding probabilities.

3.2. Infinite resources

In the asymptotic limit of infinitely many rounds ($L\to\infty$), all the correction terms due to finite statistics vanish, as well as all the correction terms due to the ε-security of the key. For instance, the PE frequencies coincide with their corresponding probabilities.

For the assumed error model, the asymptotic key rates of the N-six-state protocol ($r_{6-\mathrm{state}}$) and the N-BB84 protocol (r_{BB84}) read:

$$\begin{aligned} r_{6\text{-state}}(P_{AB}, N) = {} & \left(1-\frac{P_Z}{2}-P_{AB}\right)\log_2\left(1-\frac{P_Z}{2}-P_{AB}\right) \\ & + \left(P_{AB}-\frac{P_Z}{2}\right)\log_2\left(P_{AB}-\frac{P_Z}{2}\right) + (1-P_Z)(1-\log_2(1-P_Z)) - h(P_{AB}), \end{aligned} \tag{3.5}$$

$$r_{\mathrm{BB84}}(P_{AB}) = 1-2h(P_{AB}), \tag{3.6}$$

where P_Z is fixed by (3.4) and the rates have been maximized over the probability p of performing 2nd-type rounds. For $N=2$ the rate (3.5) reduces to the asymptotic rate of the bipartite six-state protocol [3], while (3.6) is independent of N—for fixed P_{AB}—and coincides with the asymptotic bipartite BB84 rate [3]. The reason for which (3.6) does not depend on N is that the N-BB84 protocol—unlike the N-six-state—does not completely characterize the state shared by all the parties, thus its asymptotic rate only depends on P_{AB} and P_X. For the highly symmetric error model introduced in section 3.1, it holds: $P_X = P_{AB} = \nu/2$ which is independent of the number of parties involved.

In figure 1 we plot the asymptotic rate of both protocols as a function of the probability of discordant raw key bits between A and B_i (P_{AB}), for various numbers of parties N. By noting that the N-six-state protocol outperforms the N-BB84 for equal P_{AB} and any number of parties N, we observe in the N-partite asymptotic scenario that a six-state-type protocol produces higher rates than a BB84 one, extending known results of the bipartite case [3].

Interestingly, the rate of both protocols does not decrease for an increasing number of parties and fixed P_{AB}. However, one should keep in mind that increasing N for fixed P_{AB} may not be physically reasonable. In fact, according to our error model, if P_{AB} is fixed then also the noise parameter ν (quantifying the amount of depolarization on all N qubits) is fixed, and increasing N with a fixed noise parameter may not describe realistic quantum channels. Consider, for instance, the case in which part of the noise generating P_{AB} is due to the failure of imperfect bipartite gates used for the distribution of the GHZ state. Then an increase of N, obtained by adding gates with the same failure probability, would lead to an increase of P_{AB} [5].

Moreover, the adoption of other error models can lead to key rates decreasing in the number of parties, for fixed P_{AB}. For instance if the noise on the ideal distributed state is modeled as the independent action of the depolarizing map

[5] The same error model is used, for instance, in [5].

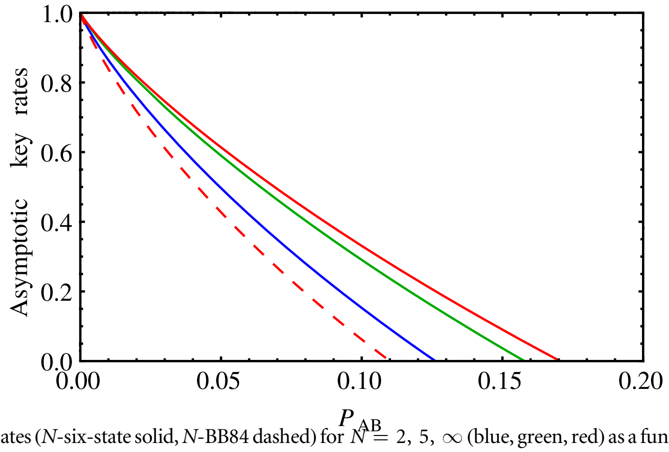

Figure 1. Asymptotic key rates (N-six-state solid, N-BB84 dashed) for $N = 2, 5, \infty$ (blue, green, red) as a function of the probability of discordant Z-outcomes between A and B_i (P_{AB}), in the presence of a global depolarizing channel (3.1). Due to the symmetric action of the white noise on the quantum channel: $P_X = P_{AB}$. The N-BB84 asymptotic key rate presents only one curve since it is independent of N.

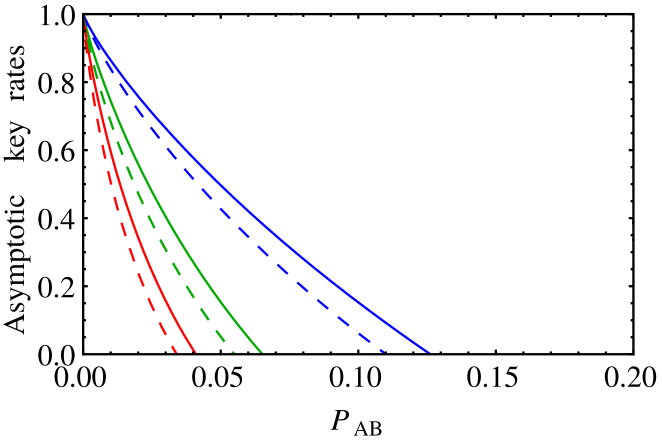

Figure 2. Asymptotic key rates (N-six-state solid, N-BB84 dashed) for $N = 2, 5, 10$ (blue, green, red) as a function of the probability of discordant Z-outcomes between A and B_i (P_{AB}), in the presence of local depolarizing channels (3.8). With this model the rate of both protocols decreases for increasing number of parties and fixed P_{AB}.

$$\mathcal{D}(\rho) = (1 - \nu)\rho + \nu\,\frac{\mathrm{id}_2}{2} \tag{3.7}$$

on each B_i, i.e. the single-round state reads:

$$\rho_{\mathbf{AB}} = \mathcal{D}^{\otimes(N-1)}(|\mathrm{GHZ}\rangle_N\,\langle\mathrm{GHZ}|_N), \tag{3.8}$$

then the probabilities of interest are given by:

$$P_{AB} = \nu/2, \tag{3.9}$$

$$P_X = \frac{1 - (1 - 2P_{AB})^{N-1}}{2}, \tag{3.10}$$

$$P_Z = 1 - (1 - P_{AB})^{N-1}, \tag{3.11}$$

where we dropped the index i in the probabilities P_{AB_i}. The asymptotic key rates of the N-BB84 and N-six-state protocol computed with the new probabilities (3.9)–(3.11) decrease for increasing number of parties, see figure 2.

3.3. Finite resources

In figure 3 we compare the key rates of both NQKD protocols for a finite number of signals L transmitted through the quantum channel, with noise discussed in section 3.1. The rates are numerically maximized over the parameters: p, $\bar{\varepsilon}$, $\varepsilon_{\mathrm{PE}}$, $\varepsilon_{\mathrm{EC}}$, $\varepsilon_{\mathrm{PA}}$, with the constraint given by the fixed value of the total security parameter: $\varepsilon_{\mathrm{tot}} = 5 \times 10^{-9}$. The fact that we are still able to obtain non-zero rates in the finite-key scenario means that the correction term '$-h(p)$' due to the preshared secret key is not prominent, as a matter of fact the optimal values for p are typically well below 0.1.

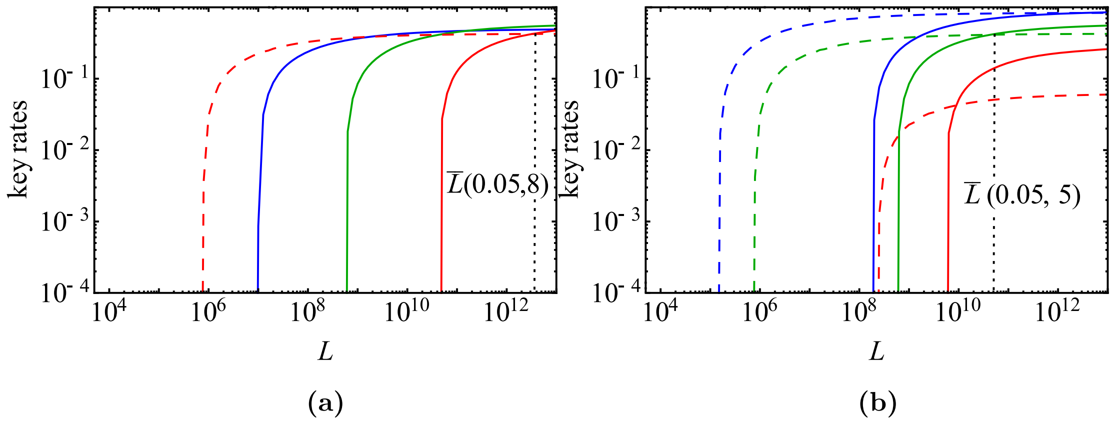

Figure 3. Key rates (N-six-state solid, N-BB84 dashed) as a function of the number of signals L. (a) Key rates as a function of the total number of rounds L for $N = 2, 5, 8$ (blue, green, red; left to right) and fixed $Q_{AB}^{m} = 0.05$. Note that even for finite number of rounds the N-BB84 rate is approximately independent of N. (b) Key rates as a function of the total number of rounds L for $Q_{AB}^{m} = 0.01, 0.05, 0.1$ (blue, green, red; left to right) and fixed $N = 5$.

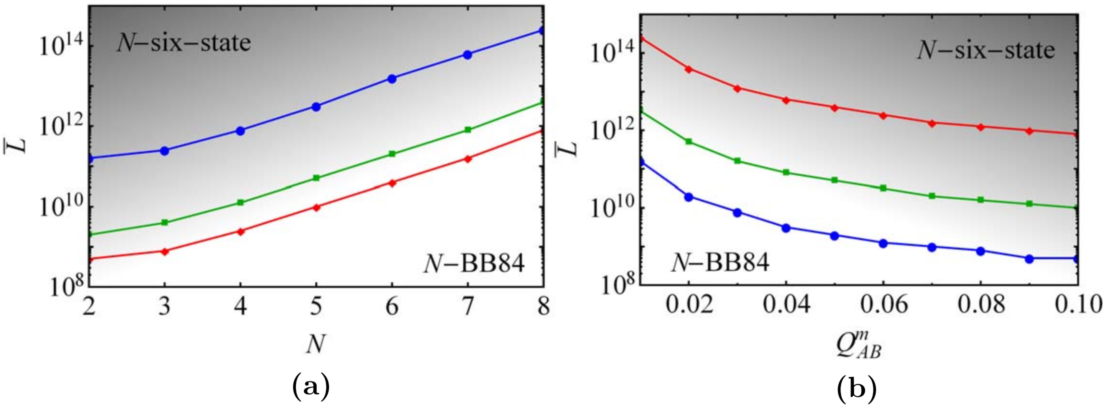

Figure 4. The threshold $\bar{L}$ as a function of one of its variables, while keeping the other one fixed. (a) Threshold function $\bar{L}$ for $Q_{AB}^{m} = 0.01, 0.05, 0.1$ (blue circles, green squares, red diamonds) as a function of the number of parties N. (b) Threshold function $\bar{L}$ for $N = 2, 5, 8$ (blue circles, green squares, red diamonds) as a function of Q_{AB}^{m}, proportional to the channel noise.

We observe that, although for large L the N-six-state still performs better than the N-BB84 protocol, there exists a certain number of rounds—identified by the threshold function $\bar{L}(Q_{AB}^{m}, N)$—below which the N-six-state protocol is outperformed by the N-BB84 protocol. The threshold function $\bar{L}$ is defined as:

$$\bar{L}(Q_{AB}^{m}, N) = \min L \quad \text{s.t.} \quad r_{\text{6-state}}(L, Q_{AB}^{m}, N) \geqslant r_{\text{BB84}}(L, Q_{AB}^{m}, N). \tag{3.12}$$

From figure 3(a) one deduces that the N-six-state protocol is much more sensitive than the N-BB84 if the number of parties is increased, displaying the opposite behavior with respect to the asymptotic case (figure 1). This causes the threshold function to increase with N and fixed Q_{AB}^{m} (figure 4(a)).

On the other hand, the N-six-state protocol is more robust than the N-BB84 protocol when the quantum channels become noisier (figure 3(b)). As a result the threshold function decreases for increasing noise and fixed N (figure 4(b)).

We point out that the function $\bar{L}$ may not be a physical threshold for the number of rounds above which the N-six-state protocol is more efficient than the N-BB84 protocol, as the achievable key rates depend on quantitatively different estimates. As a matter of fact, it is known [11] that the uncertainty relation employed for the N-BB84 protocol yields tighter bounds compared to the PS technique used for the N-six-state protocol, especially for low values of L. Instead, asymptotically the correction terms introduced by the PS technique and the uncertainty relation vanish[6], allowing the N-six-state to outperform the N-BB84 protocol (figure 1). Therefore the crossover between the two key rates at $\bar{L}$ is mainly caused by the different tightness of the min-entropy bounds used in the two protocols.

[6] Recall that the correction terms due to PS allow one to extend the security of the key against collective attacks to coherent attacks, however in the asymptotic limit these attacks are equivalent [13], thus the PS corrections vanish.

Moreover, the PS corrections become more pronounced for increasing number of parties, thus explaining the rise of the threshold function with N. Indeed, the reduction in the key length scales quadratically with the dimension d of the Hilbert space of a single-signal state shared by all N parties. Since we assume that the quantum system held by each party is a qubit, $d = 2^N$, i.e. the reduction in the key length introduced by the PS technique scales exponentially in N.

3.4. Why different strategies?

In section 3.3 we argued that the N-BB84 protocol outperforms the N-six-state protocol, at low values of L, due to the adoption of tighter bounds on the min-entropy. One could wonder what would happen if the same strategy were used in obtaining the computable key length for both protocols. Unfortunately, this is not possible: the two strategies employed (uncertainty relation and PS technique) are suited to the particular protocol to which they are applied and they cannot be used in the other protocol.

In principle the uncertainty relation may also be used to bound the min-entropy of the N-six-state protocol, but then the additional symmetries due to the extended depolarization procedure would be ignored, such that one ends with the same key length as for the N-BB84 protocol.

Conversely, one could employ the PS technique in combination with the AEP to bound the min-entropy of the N-BB84 protocol. The problem in this case would be the lack of information provided by any symmetrization procedure performed on the shared signals. Indeed without any further symmetrization, the degrees of freedom of the shared signals[7], reduced by the PE observations, would still be too many to find a computable bound to the min-entropy (i.e. a bound that only depends on the PE statistics and on the input parameters).

4. Conclusion and outlook

In this paper we presented the first complete finite-key analysis of two NQKD protocols, which can be regarded as the multipartite versions of the BB84 [1] and of the six-state [7] protocol. Although both protocols adopt genuinely multipartite entangled states as resources, these states are only required for a small number of rounds, while in the majority of the cases product states are distributed.

In order to study finite-size effects in NQKD schemes, we extended the information theoretic security analysis [8] of bipartite QKD protocols to the multipartite case, taking into account both one-way and two-way EC protocols. Then we employed the general results on the security of NQKD to investigate the N-six-state protocol [5] and the newly-defined N-BB84 protocol. In particular, we derived analytical formulas for the achievable secret key length of both protocols which only depend on the PE statistics and on the desired level of security. We achieved this by bounding the knowledge of the eavesdropper about the secret key by means of the best-known strategies adopted in bipartite QKD, namely the uncertainty relation for smooth entropies [11] and the postselection technique [12].

We compared the performance of the two NQKD protocols in the case of finite resources and in the asymptotic limit. We observed that, although the N-six-state protocol reaches higher rates asymptotically, there exists a threshold value for the number of signals below which it is outperformed by the N-BB84 protocol. We argued that this crossover between the rates of the two protocols is caused by the different strategies adopted in obtaining the computable key lengths, and we justified the choice of the strategy for each protocol.

In order to carry out a fairer comparison between the N-six-state protocol and the N-BB84 when the number of available resources is low, it would be desirable to implement tighter bounds for the min-entropy of the former protocol. In any case, the framework of NQKD ε-security developed in this paper may be used for the finite-key analysis of other multipartite QKD protocols.

This work is based on the assumptions that the measurement devices are ideal and that the parties have access to true randomness. In order to address more realistic scenarios, one can consider the fact that the measurements in the Z and X bases are not necessarily projective measurements in diagonal bases, but rather generic positive operator-valued measurements. This fact could be easily implemented in our N-BB84 protocol, thanks to the properties of the uncertainty relation [14]. A more drastic approach is represented by device-independent QKD (DIQKD) [15, 16], where no assumption is made on the devices except for spatial separation. In this context it is worth mentioning the recent security proof of a multipartite DIQKD protocol [6]. In that protocol security is guaranteed for every violation of a bipartite Bell inequality (CHSH inequality [17]) between one of the parties and the other $N - 1$. It is not yet known whether security can still be proven for violations of a multipartite Bell inequality (MABK inequality [18–20]) that do not necessarily imply CHSH violations.

[7] Remember that we are considering N-qubit states, thus their degrees of freedom are much more than in the bipartite case.

Acknowledgments

We thank Renato Renner for having generously provided the proof of the result presented in appendix E. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662 and support from the Federal Ministry of Education and Research (BMBF, projects Q.com-Q and HQS).

Appendix A. Notation

- The binary entropy function is defined as: $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$, for $p \in [0, 1]$.
- The norm $\|\cdot\|$ of an operator O is defined as: $\|O\| = \mathrm{Tr}[\sqrt{O^{\dagger}O}]$.
- $\mathcal{P}(\mathcal{H})$ is the set of positive-semidefinite operators on the Hilbert space $\mathcal{H}$.
- The set of possible secret keys shared by the parties is $\mathcal{S}$.
- The set of operators which are ε-close to a given density operator ρ is defined as:

$$\mathcal{B}^{\varepsilon}(\rho) \equiv \left\{\tau \in \mathcal{P}(\mathcal{H}):\ \mathrm{Tr}[\tau] \leqslant 1,\ \frac{1}{2}\|\tau - \rho\| \leqslant \varepsilon\right\} \tag{A.1}$$

  if the distance is computed with respect to the trace distance, or as:

$$\mathcal{B}^{\varepsilon,\mathrm{P}}(\rho) \equiv \{\tau \in \mathcal{P}(\mathcal{H}):\ \mathrm{Tr}[\tau] \leqslant 1,\ P(\tau, \rho) \leqslant \varepsilon\} \tag{A.2}$$

  if the distance is given by the purified distance [21]:

$$P(\tau, \rho) \equiv \sqrt{1 - \bar{F}(\tau, \rho)^2}$$

  where $\bar{F}(\tau, \rho)$ is called generalized fidelity:

$$\bar{F}(\tau, \rho) \equiv \mathrm{Tr}|\sqrt{\tau}\sqrt{\rho}| + \sqrt{(1 - \mathrm{Tr}\,\rho)(1 - \mathrm{Tr}\,\tau)}. \tag{A.3}$$

  Since the purified distance is an upper bound to the trace distance [21], it holds:

$$\mathcal{B}^{\varepsilon,\mathrm{P}}(\rho) \subseteq \mathcal{B}^{\varepsilon}(\rho). \tag{A.4}$$

- We say that ρ_X is the operator representation of the probability distribution P_X on the set $\mathcal{X}$ if:

$$\rho_X \equiv \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \tag{A.5}$$

  for some orthonormal basis $\{|x\rangle\}_x$.
- We define the set of probability distributions which are ε-close to a given probability distribution P_X as those distributions whose operator representation is ε-close to the operator representation of P_X, according to (A.1) and (A.2).
- The Rényi zero-entropy $H_0(P_{XY}|Y)$ of the probability distribution P_{XY} over the set $\mathcal{X} \times \mathcal{Y}$ is given by [8, 22]:

$$H_0(P_{XY}|Y) \equiv \log_2 \max_{y\in\mathcal{Y}} |\mathrm{supp}(P_X^y)|, \tag{A.6}$$

  where P_X^y denotes the function $P_X^y : x \mapsto P_{XY}(x, y)$. This entropy was called 'max-entropy' in [8].
- The ε-smooth Rényi zero-entropy $H_0^{\varepsilon}(P_{XY}|Y)$ is defined as [8, 23]:

$$H_0^{\varepsilon}(P_{XY}|Y) \equiv \min_{Q_{XY}\in\mathcal{B}^{\varepsilon}(P_{XY})} H_0(Q_{XY}|Y). \tag{A.7}$$

  If the minimization is performed on $\mathcal{B}^{\varepsilon,\mathrm{P}}(P_{XY})$ the corresponding Rényi zero-entropy is denoted as: $H_0^{\varepsilon,\mathrm{P}}(P_{XY}|Y)$.
- The Rényi zero-entropy $H_0(\rho)$ of the density operator ρ is defined as [8]:

$$H_0(\rho) \equiv \log_2 \mathrm{rank}(\rho). \tag{A.8}$$

- The min-entropy of the density operator ρ_{AB} relative to σ_B is [8, 22]:

$$H_{\min}(\rho_{AB}|\sigma_B) \equiv -\log_2 \min\{\lambda \in \mathbb{R}:\ \lambda(\mathrm{id}_A \otimes \sigma_B) - \rho_{AB} \geqslant 0\}. \tag{A.9}$$

Note that for $H_{\min}(\rho_{AB}|\sigma_B)$ to exist, a necessary condition is that: $\mathrm{supp}(\rho_B) \subseteq \mathrm{supp}(\sigma_B)$. If $\mathcal{H}_B$ is the trivial space $\mathbb{C}$, then the min-entropy reduces to:

$$H_{\min}(\rho_A) = -\log_2 \lambda_{\max}(\rho_A), \tag{A.10}$$

where $\lambda_{\max}(\rho_A)$ is the maximum eigenvalue of ρ_A.

- The min-entropy of the probability distribution P_{XY} relative to the distribution Q_Y is [8]:

$$H_{\min}(P_{XY}|Q_Y) \equiv H_{\min}(\rho_{XY}|\sigma_Y), \tag{A.11}$$

where ρ_{XY} and σ_Y are the operators representations (A.5) of P_{XY} and Q_Y, respectively.

- The min-entropy of A conditioned on B of the density operator ρ_{AB} is [8, 22, 24]:

$$H_{\min}(\rho_{AB}|B) \equiv -\log_2 \min\{\mathrm{Tr}\,\sigma_B : \sigma_B \in \mathcal{P}(\mathcal{H}_B), (\mathrm{id}_A \otimes \sigma_B) - \rho_{AB} \geqslant 0\}. \tag{A.12}$$

- The ε-smooth min-entropy of A conditioned on B of the state ρ_{AB} is [8, 22]:

$$H^{\varepsilon}_{\min}(\rho_{AB}|B) \equiv \max_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(\tilde{\rho}_{AB}|B). \tag{A.13}$$

If the maximization is performed on $\mathcal{B}^{\varepsilon,\mathrm{P}}(\rho_{AB})$ the corresponding min-entropy is denoted as: $H^{\varepsilon,\mathrm{P}}_{\min}(\rho_{AB}|B)$.

- The max-entropy of A conditioned on B of the density operator ρ_{AB} is [22]:

$$H_{\max}(\rho_{AB}|B) \equiv -H_{\min}(\rho_{AC}|C), \tag{A.14}$$

where the min-entropy of the rhs is evaluated for a purification ρ_{ABC} of ρ_{AB}.

- The ε-smooth max-entropy of A conditioned on B of the density operator ρ_{AB} is [22]:

$$H^{\varepsilon}_{\max}(\rho_{AB}|B) \equiv \min_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\max}(\tilde{\rho}_{AB}|B). \tag{A.15}$$

If the minimization is performed on $\mathcal{B}^{\varepsilon,\mathrm{P}}(\rho_{AB})$ the corresponding max-entropy is denoted as: $H^{\varepsilon,\mathrm{P}}_{\max}(\rho_{AB}|B)$.

Appendix B. Further NQKD definitions and theorems' proofs

In this appendix we prove the two results (theorems 1 and 2) presented in section 1.

First we show that correctness and secrecy of a protocol are a sufficient condition for security (definition 2), analogously to the bipartite case [8, 9]:

Definition 5 [6, 14]. Let $\rho_{\mathbf{AB}E}$ be a density operator. Any NQKD protocol, which is $\varepsilon_{\mathrm{rob}}$-robust on $\mathrm{Tr}_E[\rho_{\mathbf{AB}E}]$, is said to be ε'-correct on $\rho_{\mathbf{AB}E}$ if:

$$(1 - \varepsilon_{\mathrm{rob}})\Pr[\exists\, i \in \{1, \ldots, N-1\} : s_A \neq s_{B_i}] \leqslant \varepsilon', \tag{B.1}$$

where $(s_A, \mathbf{s_B})$ are the secret keys generated by the NQKD protocol and the probability is conditioned on the fact that the protocol did not abort.

Note that the definition of robustness of an NQKD protocol is given in definition 1.

Definition 6 [6, 14]. Let $\rho_{\mathbf{AB}E}$ be a density operator. Any NQKD protocol, which is $\varepsilon_{\mathrm{rob}}$-robust on $\mathrm{Tr}_E[\rho_{\mathbf{AB}E}]$, is said to be ε''-secret on $\rho_{\mathbf{AB}E}$ if:

$$(1 - \varepsilon_{\mathrm{rob}})\frac{1}{2}\|\rho_{S_A E'} - \rho_U \otimes \rho_{E'}\| \leqslant \varepsilon'', \tag{B.2}$$

where ρ_U is the uniform state on A's key space.

The following lemma holds:

Lemma 1. *Given an NQKD protocol which is ε'-correct and ε''-secret, then it is also $(\varepsilon' + \varepsilon'')$-secure.*

Proof. From the correctness hypothesis we have:

$$\begin{aligned}&\Pr[\exists\, i \in \{1, \ldots, N-1\} : s_A \neq s_{B_i}] = 1 - \Pr[\nexists i \in \{1, \ldots, N-1\}: s_A \neq s_{B_i}]\\ &= 1 - \sum_{s\in\mathcal{S}} P_{S_A\mathbf{S_B}}(s, \ldots, s) = 1 - \sum_{s_A,\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\delta_{s_A\mathbf{s_B}},\end{aligned}$$

where $\delta_{s_A\mathbf{s_B}} \equiv \Pi_{i=1}^{N-1}\delta_{s_A s_{B_i}}$. Therefore, ε'-correctness yields:

$$\sum_{s_A,\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})(1 - \delta_{s_A\mathbf{s_B}}) \leqslant \frac{\varepsilon'}{1 - \varepsilon_{\rm rob}}. \tag{B.3}$$

From the secrecy hypothesis we have:

$$\begin{aligned}\frac{1}{2}\|\rho_{S_A E'} - \rho_U \otimes \rho_{E'}\| &= \frac{1}{2}\left\| \sum_{s_A,\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})|s_A\rangle\langle s_A| \otimes \rho_{E'}^{s_A,\mathbf{s_B}} - \sum_{s_A}\frac{1}{|\mathcal{S}|}|s_A\rangle\langle s_A| \otimes \rho_{E'}\right\|\\ &= \frac{1}{2}\left\|\sum_{s_A}|s_A\rangle\langle s_A| \otimes \left(\sum_{\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}} - \frac{1}{|\mathcal{S}|}\rho_{E'}\right)\right\|\\ &= \frac{1}{2}\sum_{s_A}\left\|\sum_{\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}} - \frac{1}{|\mathcal{S}|}\rho_{E'}\right\| \leqslant \frac{\varepsilon''}{1 - \varepsilon_{\rm rob}}.\end{aligned} \tag{B.4}$$

Having obtained inequalities (B.3) and (B.4), we are ready to prove the thesis:

$$\begin{aligned}&\frac{1}{2}\|\rho_{S_A\mathbf{S_B}E'} - \rho_{\mathbf{U}} \otimes \rho_{E'}\|\\ &= \frac{1}{2}\left\| \sum_{s_A,\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})|s_A\rangle\langle s_A| \otimes |\mathbf{s_B}\rangle\langle\mathbf{s_B}| \otimes \rho_{E'}^{s_A,\mathbf{s_B}}\right.\\ &\left.- \sum_{s_A,\mathbf{s_B}}\frac{1}{|\mathcal{S}|}\delta_{s_A\mathbf{s_B}}|s_A\rangle\langle s_A| \otimes |\mathbf{s_B}\rangle\langle\mathbf{s_B}| \otimes \rho_{E'}\right\|\\ &= \frac{1}{2}\sum_{s_A,\mathbf{s_B}}\left\| P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}} - \frac{\delta_{s_A\mathbf{s_B}}}{|\mathcal{S}|}\rho_{E'}\right\|\\ &= \frac{1}{2}\left[\sum_{s_A,\mathbf{s_B}}(1 - \delta_{s_A\mathbf{s_B}})\left\| P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}} - \frac{\delta_{s_A\mathbf{s_B}}}{|\mathcal{S}|}\rho_{E'}\right\|\right.\\ &\left.+ \sum_{s_A,\mathbf{s_B}}\delta_{s_A\mathbf{s_B}}\left\| P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}} - \frac{\delta_{s_A\mathbf{s_B}}}{|\mathcal{S}|}\rho_{E'}\right\|\right]\\ &= \frac{1}{2}\left[\sum_{s_A,\mathbf{s_B}}(1 - \delta_{s_A\mathbf{s_B}})\|P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}}\| + \sum_{s_A}\left\| P_{S_A\mathbf{S_B}}(s_A, \ldots, s_A)\rho_{E'}^{s_A,\ldots,s_A} - \frac{1}{|\mathcal{S}|}\rho_{E'}\right\|\right]\\ &\overset{(1)}{\leqslant} \frac{\varepsilon'}{2(1 - \varepsilon_{\rm rob})} + \frac{1}{2}\sum_{s_A}\left\| P_{S_A\mathbf{S_B}}(s_A, \ldots, s_A)\rho_{E'}^{s_A,\ldots,s_A} - \frac{1}{|\mathcal{S}|}\rho_{E'}\right\|\\ &\overset{(2)}{\leqslant} \frac{\varepsilon'}{2(1 - \varepsilon_{\rm rob})} + \frac{1}{2}\sum_{s_A}\left\| P_{S_A\mathbf{S_B}}(s_A, \ldots, s_A)\rho_{E'}^{s_A,\ldots,s_A} - \sum_{\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}}\right\|\\ &+ \frac{1}{2}\sum_{s_A}\left\|\sum_{\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}} - \frac{1}{|\mathcal{S}|}\rho_{E'}\right\|\\ &\overset{(3)}{\leqslant} \frac{\varepsilon'}{2(1 - \varepsilon_{\rm rob})} + \frac{\varepsilon''}{1 - \varepsilon_{\rm rob}} + \frac{1}{2}\sum_{s_A}\left\|\sum_{\mathbf{s_B}} P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}}(1 - \delta_{s_A\mathbf{s_B}})\right\|\\ &\overset{(4)}{\leqslant} \frac{\varepsilon'}{2(1 - \varepsilon_{\rm rob})} + \frac{\varepsilon''}{1 - \varepsilon_{\rm rob}} + \frac{1}{2}\sum_{s_A,\mathbf{s_B}}\|P_{S_A\mathbf{S_B}}(s_A, \mathbf{s_B})\rho_{E'}^{s_A,\mathbf{s_B}}(1 - \delta_{s_A\mathbf{s_B}})\|\\ &\overset{(5)}{\leqslant} \frac{\varepsilon'}{1 - \varepsilon_{\rm rob}} + \frac{\varepsilon''}{1 - \varepsilon_{\rm rob}}\end{aligned} \tag{B.5}$$

which concludes the proof according to the security definition in definition 2. Note that we made use of the following properties: (1) the fact that the operator $\rho_{E'}^{s_A,\mathbf{s_B}}$ is normalized and (B.3); (2) triangle inequality; (3) (B.4); (4) triangle inequality; (5) $\rho_{E'}^{s_A,\mathbf{s_B}}$ is normalized and (B.3). □

We now prove the result on the achievable key length of a general NQKD protocol:

Proof of theorem 1. In the post-processing protocol $\mathsf{PP}_{\{\mathsf{EC}_i\},\mathcal{F}}$, the sub-protocol which transforms partially correlated key pairs into fully correlated ones is defined by the set $\{\mathsf{EC}_i\}_{i=1}^{N-1}$. Because $\{\mathsf{EC}_i\}_{i=1}^{N-1}$ is ε_{EC}-secure (in the sense of definition 3) on the classical probability distribution defined by $\rho_{X\mathbf{K}}$, according to definition 5 the whole NQKD protocol is ε_{EC}-correct on $\rho_{A\mathbf{B}E}$. Thus by lemma 1 we only need to show that the NQKD protocol is $(2\bar{\varepsilon} + \varepsilon_{\text{PA}})$-secret in order to complete the proof, i.e.:

$$\frac{1}{2}\|\rho_{S_A E'} - \rho_U \otimes \rho_{E'}\| \leqslant \frac{2\bar{\varepsilon} + \varepsilon_{\text{PA}}}{1 - \varepsilon_{\text{rob}}}. \tag{B.6}$$

We stress the fact that in Eve's subsystem E' we included not only Eve's quantum degree of freedom $\mathcal{H}_E$, but also her knowledge about the classical communication $\mathcal{H}_{\mathbf{C}}$ occurring during error correction (defined by $\{\mathsf{EC}_i\}$) and the classical communication taking place in privacy amplification $\mathcal{H}_F$ (defined by the set $\mathcal{F}$).

In order to prove (B.6), we start from the result in [8, corollary 5.6.1] stated in a slightly weaker form:

$$\|\rho_{S_A E'} - \rho_U \otimes \rho_{E'}\| \leqslant \frac{4\bar{\varepsilon}'}{1 - \varepsilon_{\text{rob}}} + 2^{-\frac{1}{2}(H_{\min}^{\bar{\varepsilon}'}(\rho_{X\mathbf{C}E}|\mathbf{C}E) - \ell)} \tag{B.7}$$

valid $\forall\ \bar{\varepsilon}'$, where ℓ is the number of key bits after privacy amplification. The inequality (B.7) leads to a sufficient condition for (B.6) to be true, namely:

$$H_{\min}^{\bar{\varepsilon}'}(\rho_{X\mathbf{C}E}|\mathbf{C}E) - \ell \geqslant 2\log_2 \frac{1 - \varepsilon_{\text{rob}}}{2(2\bar{\varepsilon} + \varepsilon_{\text{PA}} - 2\bar{\varepsilon}')} \tag{B.8}$$

therefore we will now focus on proving (B.8), having fixed: $\bar{\varepsilon}' = \bar{\varepsilon}$.

We first prove the result without assuming that the classical communication $\mathbf{C}$ is one-way, i.e. it may also depend on $\mathbf{B}$'s raw keys. Then we show how to achieve a slightly stronger result by assuming one-way classical communication.

Two-way EC: Since the purified distance is an upper bound to the trace distance, an ε-environment defined with the latter is larger (A.4). Thus:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}^{\bar{\varepsilon},\text{P}}(\rho_{X\mathbf{C}E}|\mathbf{C}E). \tag{B.9}$$

The result stated in appendix E yields:

$$H_{\min}^{\bar{\varepsilon},\text{P}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}^{\bar{\varepsilon},\text{P}}(\rho_{XE}|E) - (H_0(\rho_{\mathbf{C}}) - H_{\min}(\rho_{X\mathbf{KC}}|\rho_{X\mathbf{K}})). \tag{B.10}$$

Now let us concentrate on the last two terms in (B.10):

(i) By definition (A.8): $H_0(\rho_{\mathbf{C}}) = \log_2 \text{rank}(\rho_{\mathbf{C}})$, with:

$$\rho_{\mathbf{C}} = \sum_{c_1,\ldots,c_{N-1}} P_{\mathbf{C}}(c_1, \ldots, c_{N-1}) \bigotimes_{i=1}^{N-1} |c_i\rangle\langle c_i|, \tag{B.11}$$

therefore $\text{rank}(\rho_{\mathbf{C}}) = |\mathcal{C}_{1,\ldots,N-1}|$ according to (1.5).

(ii) By definition (A.9): $H_{\min}(\rho_{X\mathbf{KC}}|\rho_{X\mathbf{K}}) = -\log_2 \min \lambda$, where λ is a real parameter satisfying:

$$\begin{aligned} &\lambda(\rho_{X\mathbf{K}} \otimes \text{id}_{\mathbf{C}}) - \rho_{X\mathbf{KC}} \geqslant 0 \\ \iff\ &\lambda \geqslant P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}}(c_1, \ldots, c_{N-1}|x, \mathbf{k}) \quad \forall\, x, \mathbf{k}, c_1, \ldots, c_{N-1}. \end{aligned}$$

Therefore

$$\min \lambda = \max_{\mathbf{c},\mathbf{k},x} P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}}(c_1, \ldots, c_{N-1}|x, \mathbf{k}), \tag{B.12}$$

which yields:

$$\begin{aligned} H_{\min}(\rho_{X\mathbf{KC}}|\rho_{X\mathbf{K}}) &= \min_{x,\mathbf{k}}\left[-\log_2 \max_{\mathbf{c}} P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}}(c_1, \ldots, c_{N-1}|x, \mathbf{k})\right] \\ &= \min_{x,\mathbf{k}} H_{\min}(P_{\mathbf{C}|X=x,\mathbf{K}=\mathbf{k}}), \end{aligned}$$

where in the last inequality we used the definition of min-entropy for probability distributions (A.11).

Substituting now in (B.10), recalling definition 4 and using (B.9) yields:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}^{\bar{\varepsilon},\text{P}}(\rho_{XE}|E) - \text{leak}_{\{\mathsf{EC}_i\}}^{\text{NQKD}}. \tag{B.13}$$

By using the assumption (1.6) in the last inequality concludes the proof:

$$\begin{aligned} H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) &\geqslant H_{\min}^{\bar{\varepsilon},\mathrm{P}}(\rho_{XE}|E) - \mathrm{leak}_{\{\mathsf{EC}_i\}}^{\mathrm{NQKD}} \\ &\geqslant \ell + 2\log_2\frac{1-\varepsilon_{\mathrm{rob}}}{2\,\varepsilon_{\mathrm{PA}}} \end{aligned} \tag{B.14}$$

since we have just obtained (B.8) with fixed $\bar{\varepsilon}' = \bar{\varepsilon}$.

*One-way EC***:** For the chain rule [8, equation (3.21)] we have:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|E) - H_0(\rho_{\mathbf{C}}), \tag{B.15}$$

where the quantum state is, under the assumption of one-way EC protocols:

$$\hat{\rho}_{X\mathbf{C}E} = \sum_x |x\rangle\langle x| \otimes \hat{\rho}_{\mathbf{C}}^x \otimes \rho_E^x, \tag{B.16}$$

where the hat ˆ indicates normalized density operators and:

$$\rho_E^x \equiv \sum_{\mathbf{k}} P_{X\mathbf{K}}(x,\mathbf{k})\,\hat{\rho}_E^{x,\mathbf{k}}. \tag{B.17}$$

Since in (B.16) the state conditioned on the classical subsystem $\mathcal{H}_X$ is a product state, by [8, equation (3.22)] we conclude that:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|E) \geqslant H_{\min}^{\bar{\varepsilon}}(\rho_{XE}|E) + H_{\min}(\rho_{X\mathbf{C}}|\rho_X). \tag{B.18}$$

Substituting (B.18) in (B.15) yields:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}^{\bar{\varepsilon}}(\rho_{XE}|E) - (H_0(\rho_{\mathbf{C}}) - H_{\min}(\rho_{X\mathbf{C}}|\rho_X)), \tag{B.19}$$

which is equivalent to what was obtained in the two-way scenario (B.10) except for the ε-environment of the min-entropy, here defined via the trace distance. Analogous steps to those employed in the first part lead to the claim valid for one-way EC. □

Finally, we show how to obtain an upper bound on the leakage of an optimal EC protocol.

Proof of theorem 2. Let $\mathcal{X}$ be the set of possible raw keys held by A, while $\mathcal{K}$ is the set of possible raw keys held by $\mathbf{B}$. Let us consider the following N-partite one-way EC protocol $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$ (generalization of the bipartite version in [8, lemma 6.3.3]):

Parameters:

- $\hat{\mathcal{X}}$: family of sets $\hat{\mathcal{X}}_{k_i}^i \subseteq \mathcal{X}$ parametrized by the index i which identifies B_i and by $k_i \in \mathcal{K}$.
- $\mathcal{F}$: family of hash functions from $\mathcal{X}$ to $\mathcal{Z}$.

Protocol:

(i) A receives as input the raw key $x \in \mathcal{X}$, while B_i receives the raw key $k_i \in \mathcal{K}$.

(ii) A chooses uniformly at random $f \in_R \mathcal{F}$ and defines $z \equiv f(x)$. Then, A sends the classical message (f, z) to $\mathbf{B}$.

(iii) B_i selects the set $\hat{\mathcal{X}}_{k_i}^i$ corresponding to the key k_i he is holding, and defines: $\hat{\mathcal{D}}_i \equiv \{\hat{x}_i \in \hat{\mathcal{X}}_{k_i}^i : f(\hat{x}_i) = z\}$.

(iv) If $\hat{\mathcal{D}}_i \neq \varnothing$ then B_i's guess of A's key is $\hat{x}_i \in_R \hat{\mathcal{D}}_i$, otherwise the protocol aborts.

The proof consists of two parts. The first part extends the result stated in [8, lemma 6.3.3] to the multipartite scenario, while the second part generalizes [8, lemma 6.3.4].

Part 1: We first show that the above-defined $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$, for an appropriate choice of the parameters $\hat{\mathcal{X}}$ and $\mathcal{F}$, is 0-robust on $P_{X\mathbf{K}}$, $\varepsilon_{\mathrm{EC}}$-fully secure (see definition 3), and has leakage:

$$\mathrm{leak}_{\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}}^{\mathrm{NQKD}} \leqslant \max_i H_0(P_{XK_i}|K_i) + \log_2(2/\varepsilon_{\mathrm{EC}}) + \log_2(N-1). \tag{B.20}$$

Let $z_{\mathrm{EC}} \equiv \left\lceil \max_i H_0(P_{XK_i}|K_i) + \log_2(N-1) + \log_2(1/\varepsilon_{\mathrm{EC}}) \right\rceil$ and let $\mathcal{F}$ be a two-universal family of hash functions from $\mathcal{X}$ to $\mathcal{Z} = \{0, 1\}^{z_{\mathrm{EC}}}$. Moreover, let $\hat{\mathcal{X}} = \{\hat{\mathcal{X}}_{k_i}^i\}$ be the family of sets defined by $\hat{\mathcal{X}}_{k_i}^i \equiv \mathrm{supp}(P_X^{i,k_i})$, where $\mathrm{supp}(P_X^{i,k_i})$ denotes the support of the function: $P_X^{i,k_i} : x \mapsto P_{XK_i}(x, k_i)$. From the choice of $\mathcal{F}$ we know that: $\Pr_f[f(x') = f(x)]_{x' \neq x} \leqslant 2^{-z_{\mathrm{EC}}}$ for $f \in_R \mathcal{F}$ and fixed elements $x, x' \in \mathcal{X}$. Note that the two parameters $\hat{\mathcal{X}}$, $\mathcal{F}$ defining the EC protocol are completely fixed by the marginals distributions P_{XK_i} of the given probability distribution $P_{X\mathbf{K}}$.

For any given set of raw keys $(x, k_1, \ldots, k_{N-1})$ (not necessarily generated by $P_{X\mathbf{K}}$), one can bound the probability that the protocol $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$ does not abort and outputs a wrong guess for at least one Bob, as:

$$\begin{aligned}\mathrm{Pr}_{f,\hat{\mathbf{x}}}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall i\ \wedge \exists i : \hat{x}_i \neq x] &\leqslant \mathrm{Pr}_{f,\hat{\mathbf{x}}}[\exists i : \hat{x}_i \neq x]\\ &\leqslant \mathrm{Pr}_f[\exists \hat{x} \in \cup_{i=1}^{N-1}\hat{\mathcal{D}}_i : \hat{x} \neq x]\\ &= \mathrm{Pr}_f\Big[\exists \hat{x} \in \cup_{i=1}^{N-1}\hat{\mathcal{X}}^i_{k_i} : \hat{x} \neq x \wedge f(\hat{x}) = f(x)\Big]\\ &\leqslant \sum_{\hat{x} \in \cup_{i=1}^{N-1}\hat{\mathcal{X}}^i_{k_i}, \hat{x} \neq x} \mathrm{Pr}_f[f(\hat{x}) \neq f(x)]\\ &\leqslant \sum_{\hat{x} \in \cup_{i=1}^{N-1}\hat{\mathcal{X}}^i_{k_i}, \hat{x} \neq x} 2^{-z_{\mathrm{EC}}},\end{aligned} \tag{B.21}$$

where the third inequality is due to the union bound and the fourth to the chosen set $\mathcal{F}$. Finally, we can bound (B.21) by:

$$\begin{aligned}\mathrm{Pr}_{f,\hat{\mathbf{x}}}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall i\ \wedge \exists i : \hat{x}_i \neq x] &\leqslant \left|\cup_{i=1}^{N-1}\hat{\mathcal{X}}^i_{k_i}\right| 2^{-z_{\mathrm{EC}}}\\ &\leqslant (N-1)\max_i \max_{k_i}|\mathrm{supp}(P_X^{i,k_i})|\ 2^{-z_{\mathrm{EC}}}\\ &= 2^{\log_2(N-1)}2^{\max_i H_0(P_{XK_i}|K_i)}2^{-z_{\mathrm{EC}}}\\ &\leqslant \varepsilon_{\mathrm{EC}}\end{aligned}$$

which proves that $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$ is $\varepsilon_{\mathrm{EC}}$-fully secure according to definition 3. Note that we used (A.6) for the equality and the definition of z_{EC} in the last inequality.

If the set of keys $(x, k_1, \ldots, k_{N-1})$ is now generated by the distribution $P_{X\mathbf{K}}$, then $x \in \hat{\mathcal{X}}^i_{k_i}\ \forall i$ since $P_{XK_i}(x, k_i) \neq 0\ \forall i$ (otherwise the pair (x, k_i) could not have been generated). Therefore, being $f(x) = z$ true by definition, the sets $\hat{\mathcal{D}}_i$ are never empty, thus the EC protocol never aborts, i.e. it is 0-robust (definition 1) on $P_{X\mathbf{K}}$.

Let us now consider the leakage of the protocol $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$. Since it is a one-way EC protocol where the information sent to one Bob is then copied and then sent to all the other Bobs, the leakage reads (definition 4):

$$\mathrm{leak}^{\mathrm{NQKD}}_{\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}} = \log_2|\mathcal{F} \times \mathcal{Z}| - \min_x H_{\min}(P_{C|X=x}). \tag{B.22}$$

For this EC protocol, after having fixed A's key x, the classical communication (f, z) is simply depending on the random choice of f, therefore: $P_{C|X=x} = 1/|\mathcal{F}|$. Substituting in (B.22) yields:

$$\begin{aligned}\mathrm{leak}^{\mathrm{NQKD}}_{\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}} &= \log_2|\mathcal{F} \times \mathcal{Z}| - \log_2|\mathcal{F}|\\ &\leqslant \log_2|\mathcal{Z}| = z_{\mathrm{EC}}\\ &= \left\lceil \max_i H_0(P_{XK_i}|K_i) + \log_2(N-1) + \log_2(1/\varepsilon)\right\rceil\\ &\leqslant \log_2 2 + \max_i H_0(P_{XK_i}|K_i) + \log_2(N-1) + \log_2(1/\varepsilon)\\ &= \max_i H_0(P_{XK_i}|K_i) + \log_2(2/\varepsilon) + \log_2(N-1),\end{aligned}$$

which concludes the first part of the proof (B.20).

Part 2: Now we employ the result (B.20) for another protocol $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$ where the parameters $\hat{\mathcal{X}}$, $\mathcal{F}$ are defined by a new set of distributions $\{\bar{P}_{XK_i}\}_{i=1}^{N-1}$ linked to the marginals of $P_{X\mathbf{K}}$. Such an EC protocol will be the one that satisfies the claim (1.7). The distributions $\{\bar{P}_{XK_i}\}_{i=1}^{N-1}$ are obtained by the definition of smooth Rényi zero-entropy (A.7):

$$\begin{aligned}&\forall i \in \{1, \ldots, N-1\} \quad \exists \bar{P}_{XK_i} \quad \text{s.t.}\\ &\|\bar{P}_{XK_i} - P_{XK_i}\| \leqslant 2\varepsilon' \quad \wedge \quad H_0(\bar{P}_{XK_i}|K_i) = H_0^{\varepsilon'}(P_{XK_i}|K_i),\end{aligned} \tag{B.23}$$

where the distance between two probability distributions is defined as:

$$\|P - Q\| = \sum_x |P(x) - Q(x)|.$$

We define $\bar{i} \equiv \mathrm{argmax}_i H_0(\bar{P}_{XK_i}|K_i)$, then (B.23) implies:

$$\begin{aligned}\max_i H_0(\bar{P}_{XK_i}|K_i) = H_0(\bar{P}_{XK_{\bar{i}}}|K_{\bar{i}}) &= H_0^{\varepsilon'}(P_{XK_{\bar{i}}}|K_{\bar{i}})\\ &\leqslant \max_i H_0^{\varepsilon'}(P_{XK_i}|K_i).\end{aligned} \tag{B.24}$$

Let us now consider the protocol $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$ where $\hat{\mathcal{X}}$ and $\mathcal{F}$ are fixed by the above-defined set of distributions $\{\bar{P}_{XK_i}\}_{i=1}^{N-1}$. Then, by (B.20) we know that such an EC protocol is $\varepsilon_{\mathrm{EC}}$-fully secure and has leakage:

$$\begin{aligned}\mathrm{leak}^{\mathrm{NQKD}}_{\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}} &\leqslant \max_i H_0(\bar{P}_{XK_i}|K_i) + \log_2(2/\varepsilon_{\mathrm{EC}}) + \log_2(N-1)\\ &\leqslant \max_i H_0^{\varepsilon'}(P_{XK_i}|K_i) + \log_2(2/\varepsilon_{\mathrm{EC}}) + \log_2(N-1),\end{aligned}$$

where we used (B.24) in the second inequality.

The last thing to be shown is that such an EC protocol is also $2(N-1)\varepsilon'$-robust on the distribution $P_{X\mathbf{K}}$:

$$\Pr_{(x,\mathbf{k})}[\mathrm{abort}]_P \leqslant 2(N-1)\varepsilon', \tag{B.25}$$

i.e. the probability that the protocol aborts when initiated with a set of keys $(x, \mathbf{k})$ generated by the distribution $P_{X\mathbf{K}}$ is lower or equal than $2(N-1)\varepsilon'$[8]. Let us compute the probability of $\mathrm{EC}_{\hat{\mathcal{X}},\mathcal{F}}$ to abort:

$$\begin{aligned}\Pr_{(x,\mathbf{k})}[\mathrm{abort}]_P &= \Pr_{(x,\mathbf{k})}[\exists\ i : \hat{\mathcal{D}}_i = \varnothing]_P\\ &= 1 - \Pr_{(x,\mathbf{k})}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall\, i]_P.\end{aligned}$$

One of the possibilities for $\hat{\mathcal{D}}_i$ not to be empty is $x \in \hat{\mathcal{D}}_i \leftrightarrow\ x \in \hat{\mathcal{X}}^i_{k_i} \leftrightarrow \bar{P}_{XK_i}(x, k_i) \neq 0$, which is not obvious since x was generated through the distribution $P_{X\mathbf{K}}$. Therefore:

$$\Pr_{(x,\mathbf{k})}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall\, i]_P \geqslant \Pr_{(x,\mathbf{k})}[\bar{P}_{XK_i}(x, k_i) \neq 0\ \forall\, i]_P. \tag{B.26}$$

By employing the following inequality from probability theory (straightforward proof based on union bound and de-Morgan's law):

$$\Pr\left(\bigcap_{i=1}^{n} A_i\right) \geqslant \sum_{i=1}^{n} \Pr(A_i) - (n-1), \tag{B.27}$$

where $\Pr(A_i)$ is the probability of event A_i, we are able to recast the rhs of (B.26) as:

$$\begin{aligned}\Pr_{(x,\mathbf{k})}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall\, i]_P &\geqslant \Pr_{(x,\mathbf{k})}[\bar{P}_{XK_i}(x, k_i) \neq 0\ \forall\, i]_P\\ &\geqslant \sum_{i\,=\,1}^{N-1} \Pr_{(x,k_i)}[\bar{P}_{XK_i}(x, k_i) \neq 0]_P - [(N-1) - 1].\end{aligned} \tag{B.28}$$

We now concentrate on computing $\Pr_{(x,k_i)}[\bar{P}_{XK_i}(x, k_i) \neq 0]_P$, which is the probability that, having generated the couple (x, k_i) from distribution P_{XK_i}, it holds that $\bar{P}_{XK_i}(x, k_i) \neq 0$. We employ the fact that by assumption (B.23) the distance between the two involved distributions is bounded by $2\varepsilon'$, which implies that, for instance:

$$|P_{XK_i}(x, k_i) - \bar{P}_{XK_i}(x, k_i)| \leqslant 2\varepsilon' \quad \forall (x, k_i). \tag{B.29}$$

Let us focus on the probability of the complementary event: $\Pr_{(x,k_i)}[\bar{P}_{XK_i}(x, k_i) = 0]_P$. Since this event is a sufficient condition for having $P_{XK_i}(x, k_i) \leqslant 2\varepsilon'$ (because of (B.29)), this means that:

$$\Pr_{(x,k_i)}[P_{XK_i}(x, k_i) \leqslant 2\varepsilon']_P \geqslant \Pr_{(x,k_i)}[\bar{P}_{XK_i}(x, k_i) = 0]_P, \tag{B.30}$$

but the lhs of (B.30) can be bounded by:

$$\Pr_{(x,k_i)}[P_{XK_i}(x, k_i) \leqslant 2\varepsilon']_P \leqslant 2\varepsilon', \tag{B.31}$$

therefore we have:

$$\Pr_{(x,k_i)}[\bar{P}_{XK_i}(x, k_i) \neq 0]_P \geqslant 1 - 2\varepsilon'. \tag{B.32}$$

Substituting in (B.28) yields:

$$\Pr_{(x,\mathbf{k})}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall\, i]_P \geqslant (N-1)(1-2\varepsilon') + 1 - (N-1) = 1 - (N-1)2\varepsilon'. \tag{B.33}$$

With this result we can conclude that:

$$\begin{aligned}\Pr_{(x,\mathbf{k})}[\mathrm{abort}]_P &= 1 - \Pr_{(x,\mathbf{k})}[\hat{\mathcal{D}}_i \neq \varnothing\ \forall\, i]_P\\ &\leqslant 2(N-1)\varepsilon'\end{aligned}$$

which concludes the proof. □

Appendix C. Quantifying the channel's noise

As anticipated in section 2, one can bound E's knowledge about the secret key by quantifying the noise she introduced in the quantum channel.

[8] Note that this EC protocol is defined by the distributions $\bar{P}_{XK_i}$ which are one by one $2\varepsilon'$-close to the marginals of the distribution $P_{X\mathbf{K}}$ defining the EC protocol of part 1, which was shown to be 0-robust on $P_{X\mathbf{K}}$. It is not straightforward to infer—unlike the bipartite case—that the new EC protocol is then $(N-1)\cdot 2\varepsilon'$-robust on $P_{X\mathbf{K}}$.

In this section we show how the relevant noise parameters of both protocols can be estimated from the finite statistics collected in PE.

C.1. N-BB84 protocol

In the N-BB84 protocol, the important noise parameters that are subsequently used to characterize E's knowledge are $Q_{AB_i}^n$ and Q_X^n, i.e. the frequency of discordant Z-outcomes between A and B_i and the frequency of the outcome $X^{\otimes N} = -1$, respectively. Both frequencies refer to hypothetical measurements performed on the remaining n signals following PE. The goal is to characterize the noise parameters based on what is observed in PE ($Q_{AB_i}^m$ and Q_X^m). This is easily achieved by means of the following lemma (generalization of a result presented in [14, suppl. note 2]):

Lemma 2. *Let $\varepsilon > 0$. Let $\mathbf{R}$ be a random binary string of $M = n + m$ bits with relative Hamming weight $\Lambda_M = \frac{1}{M}|\mathbf{R}|$. Let $R_1, \ldots, R_m$ be random variables obtained by sampling m random entries of $\mathbf{R}$ without replacement. Then, upon defining:*

$$\Lambda_m = \frac{\sum_{i=1}^m R_i}{m} = \frac{|(\mathbf{R})_m|}{m}, \tag{C.1}$$

$$\Lambda_n = \frac{|(\mathbf{R})_n|}{n} \tag{C.2}$$

as the relative Hamming weights[9] *of the two randomly chosen partitions of $\mathbf{R}$, it holds:*

$$\begin{aligned} \Pr\left[\frac{1}{2}|\Lambda_n - \Lambda_m| > \xi(\varepsilon, n, m)\right] &\leqslant 2\varepsilon \\ \Pr[\Lambda_n > \Lambda_m + 2\xi(\varepsilon, n, m)] &\leqslant \varepsilon \\ \Pr[\Lambda_m > \Lambda_n + 2\xi(\varepsilon, m, n)] &\leqslant \varepsilon, \end{aligned} \tag{C.3}$$

where:

$$\xi(\varepsilon, n, m) \equiv \sqrt{\frac{(n+m)(m+1)}{8nm^2}\ln\left(\frac{1}{\varepsilon}\right)}. \tag{C.4}$$

Proof. Let us first fix the random bit string $\mathbf{R}$ to a given and known string: $\mathbf{R} \equiv \mathbf{r}$; thus also its relative Hamming weight is fixed to some real value: $\Lambda_M \equiv \lambda_M$. Then it holds [25, theorem 1]:

$$\Pr[|\Lambda_n - \lambda_M| > \delta\,|\mathbf{R} = \mathbf{r}, \Lambda_M = \lambda_M] \leqslant 2\,\mathrm{e}^{-2\frac{nM}{m+1}\delta^2}, \tag{C.5}$$

$$\Pr[\Lambda_n > \lambda_M + \delta\,|\mathbf{R} = \mathbf{r}, \Lambda_M = \lambda_M] \leqslant \mathrm{e}^{-2\frac{nM}{m+1}\delta^2}. \tag{C.6}$$

By defining $\nu = \frac{m}{M}$, it is immediate to show the following facts for every $\mu \in \mathbb{R}$:

$$\begin{aligned} &\Lambda_M = \nu\Lambda_m + (1-\nu)\Lambda_n \\ &|\Lambda_n - \Lambda_M| > \nu\mu \iff |\Lambda_n - \Lambda_m| > \mu, \end{aligned} \tag{C.7}$$

$$\Lambda_n > \Lambda_M + \nu\mu \iff \Lambda_n > \Lambda_m + \mu. \tag{C.8}$$

Now one can make use of (C.5) and (C.7) in the following calculation:

$$\begin{aligned} \Pr[|\Lambda_n - \Lambda_m| > \mu] &= \Pr[|\Lambda_n - \Lambda_M| > \nu\mu] \\ &= \sum_{\mathbf{r}} \Pr[\mathbf{R} = \mathbf{r}]\Pr[|\Lambda_n - \lambda_M| > \nu\mu|\mathbf{R} = \mathbf{r}, \Lambda_N = \lambda_M] \\ &\leqslant \sum_{\mathbf{r}} \Pr[\mathbf{R} = \mathbf{r}]2\,\mathrm{e}^{-2\frac{nM}{m+1}\frac{m^2}{M^2}\mu^2} \\ &= 2\,\mathrm{e}^{-2\frac{nm^2}{(m+1)M}\mu^2}. \end{aligned} \tag{C.9}$$

Analogously, by using (C.6) and (C.8) one obtains:

$$\Pr[\Lambda_n > \Lambda_m + \mu] \leqslant \mathrm{e}^{-2\frac{nm^2}{(m+1)M}\mu^2}. \tag{C.10}$$

Finally, by choosing μ such that it holds: $\mathrm{e}^{-2\frac{nm^2}{(m+1)M}\mu^2} = \varepsilon$, i.e. $\mu = 2\xi(\varepsilon, n, m)$ with $\xi(\varepsilon, n, m)$ defined as in (C.4), one obtains from (C.9) and (C.10):

[9] We denote by $(\mathbf{R})_m$ the m-bit string composed by the random variables $R_1, \ldots, R_m$, while $(\mathbf{R})_n$ is the n-bit string composed by the remaining entries of $\mathbf{R}$.

$$\Pr\left[\frac{1}{2}|\Lambda_n - \Lambda_m| > \xi(\varepsilon, n, m)\right] \leqslant 2\varepsilon$$
$$\Pr[\Lambda_n > \Lambda_m + 2\xi(\varepsilon, n, m)] \leqslant \varepsilon$$

which is exactly the claimed result in (C.3). The last expression in (C.3) is simply obtained by exchanging the roles of *n* and *m*. □

In order to make use of lemma 2, we define the following random vectors containing the outcomes of *A* and B_i's *Z*-measurement rounds devoted to PE:

$$(\mathbf{Z}_a)_j \equiv \begin{cases} 1 & z_{a,j} = -1 \\ 0 & z_{a,j} = 1 \end{cases} \quad (\mathbf{Z_i})_j \equiv \begin{cases} 1 & z_{i,j} = -1 \\ 0 & z_{i,j} = 1 \end{cases}. \tag{C.11}$$

Analogously, we define the random vectors containing the outcomes of *A* and **B**'s *X*-measurement rounds:

$$(\mathbf{X_a})_j \equiv \begin{cases} 1 & x_{a,j} = -1 \\ 0 & x_{a,j} = 1 \end{cases} \quad (\mathbf{X_i})_j \equiv \begin{cases} 1 & x_{i,j} = -1 \\ 0 & x_{i,j} = 1 \end{cases}. \tag{C.12}$$

With these definitions, it holds:

$$(\mathbf{X_a} \oplus \mathbf{X_1} \oplus \ldots \oplus \mathbf{X_{N-1}})_j = \begin{cases} 1 & (x_a \prod_{i=1}^{N-1} x_i)_j = -1 \\ 0 & (x_a \prod_{i=1}^{N-1} x_i)_j = 1 \end{cases} \tag{C.13}$$

therefore it is immediate to verify that:

$$Q_{AB_i}^m = \frac{|\mathbf{Z}_a \oplus \mathbf{Z_i}|}{m}$$
$$Q_X^m = \frac{|\mathbf{X_a} \oplus \mathbf{X_1} \oplus \ldots \oplus \mathbf{X_{N-1}}|}{m}. \tag{C.14}$$

Since we were able to write the frequencies $Q_{AB_i}^m$ and Q_X^m as relative Hamming weights of random vectors, we can apply lemma 2 and state that:

$$\Pr[Q_X^n \leqslant Q_X^m + 2\xi(\varepsilon_x, n, m) \wedge Q_{AB_i}^n \leqslant Q_{AB_i}^m + 2\xi(\varepsilon_z, n, m)\,\forall\, i] \geqslant 1 - \varepsilon_{\mathrm{PE}}^2, \tag{C.15}$$

where we used (B.27) and defined:

$$\varepsilon_{\mathrm{PE}} \equiv \sqrt{(N-1)\varepsilon_z + \varepsilon_x}. \tag{C.16}$$

C.2. N-six-state protocol

In this case *E* is supposed to gain information about the key only via collective attacks, i.e. she attacks each of the shared signals independently and identically[10]. Thus, the needed noise parameters are the probabilities P_X, P_{AB_i} and P_Z computed on a single *N*-qubit signal state, which in turn has a very simple expression [5, equation (11)] thanks to the extended depolarization procedure.

The PE frequencies $Q_X^{m'}$, $Q_{AB_i}^m$ and Q_Z^m are thus observed on multiple copies of the same *N*-qubit signal state. Therefore they constitute an estimation of the corresponding probabilities by the law of large numbers [26]:

$$\Pr\left[\frac{1}{2}|Q_{AB_i}^m - P_{AB_i}| \leqslant \eta(\varepsilon_z, 2, m)\forall i \wedge \frac{1}{2}|Q_X^{m'} - P_X| \leqslant \eta(\varepsilon_x, 2, m')\right.$$
$$\left.\wedge \frac{1}{2}|Q_Z^m - P_Z| \leqslant \eta(\varepsilon_z', 2, m)\right] \geqslant 1 - \varepsilon_{\mathrm{PE}}, \tag{C.17}$$

where we used (B.27) and defined:

$$\varepsilon_{\mathrm{PE}} \equiv \varepsilon_z' + (N-1)\varepsilon_z + \varepsilon_x \tag{C.18}$$

$$\eta(\varepsilon, d, m) \equiv \sqrt{\frac{\ln(1/\varepsilon) + d\ln(m+1)}{8m}}. \tag{C.19}$$

Appendix D. Derivation of the computable key lengths

In order to obtain a computable key length for the *N*-BB84 (theorem 3) and the *N*-six-state (theorem 4) protocol starting from the general result (theorem 1), one needs to lower bound the min-entropy (which quantifies *E*'s

[10] Then the result is extended to coherent attacks via the PS technique, see appendix D for the details.

uncertainty about the key) and to upper bound the leakage term with quantities depending on the channel's noise.

In this section we show how to achieve this task for both protocols and how to further characterize the noise via the PE finite statistics, by using the results of appendix C.

Concerning the notation, for the remainder of the section we indicate with an apex the number of signals described by the quantum state, and we also indicate as Z the classical system containing A's raw key bits (since in both protocols the raw keys are generated by Z-basis measurements). Thus the quantum state describing the parties' raw keys and E's degree of freedom is indicated as: $\rho^n_{Z\mathbf{K}E}$.

D.1. N-BB84 protocol

Leakage. The leakage of an optimal one-way EC protocol (1.7) is bounded by the smooth Rényi zero-entropy of the probability distribution of A and B_i's raw keys (A.7). Note that, thanks to (A.4), we can bound such an entropy by:

$$H_0^{\varepsilon_{\rm PE}}(P^n_{ZK_i}|K_i) \leqslant H_0^{\varepsilon_{\rm PE},{\rm P}}(P^n_{ZK_i}|K_i). \tag{D.1}$$

In this way, one can follow the proof of [14, lemma 3] and show that there exists a probability distribution $R^n_{ZK_i} \in \mathcal{B}^{\varepsilon_{\rm PE},{\rm P}}(P^n_{ZK_i})$ such that the frequency of discordant bits $(Q^n_{AB_i})$ is less or equal than $Q^m_{AB_i} + 2\xi(\varepsilon_z, n, m)$, with certainty. Note that this is not true for the distribution $P^n_{ZK_i}$, since it holds condition (C.15).

This upper limit on the number of discordant bits between A and B_i, when the keys are generated by $R^n_{ZK_i}$, allows one to bound the Rényi zero-entropy of such a distribution by $nh(Q^m_{AB_i} + 2\xi(\varepsilon_z, n, m))$.

Finally, since the smooth Rényi entropy of order zero is defined with a *minimization* over its ε-environment (A.7), one obtains:

$$H_0^{\varepsilon_{\rm PE},{\rm P}}(P^n_{ZK_i}|K_i) \leqslant nh(Q^m_{AB_i} + 2\xi(\varepsilon_z, n, m)). \tag{D.2}$$

Combining (D.1) and (D.2) with theorem 2 leads to the desired result. The leakage occurring in the N-BB84 protocol, implemented with the optimal one-way, $\varepsilon_{\rm EC}$-fully secure and $2(N-1)\varepsilon_{\rm PE}$ —robust EC protocol, is:

$$\text{leak}^{\rm NQKD}_{\rm EC} \leqslant n\max_i h(Q^m_{AB_i} + 2\xi(\varepsilon_z, n, m)) + \log_2\frac{2(N-1)}{\varepsilon_{\rm EC}}. \tag{D.3}$$

Min-entropy. Let $\rho^{n+2m}_{A\mathbf{B}E}$ be the pure state describing the whole set of quantum signals and E's quantum system. The state ρ^n_{ZE} is then obtained by performing independent Z-measurements on A's subsystems and taking the partial trace over $\mathbf{B}$'s ones, after the PE procedure took place on $2m$ signals. If we now define $\rho^n_{X\mathbf{B}}$ as the state obtained by performing independent X-measurements on A's subsystems and then taking the partial trace over E, we can employ the uncertainty relation [11]:

$$H^{\bar{\varepsilon},{\rm P}}_{\min}(\rho^n_{ZE}|E) \geqslant q - H^{\bar{\varepsilon},{\rm P}}_{\max}(\rho^n_{X\mathbf{B}}|\mathbf{B}), \tag{D.4}$$

where $q = -\log_2 c$, with:

$$c = \max_{\mathbf{z},\mathbf{x}} \|(P_{z_1} \otimes ... \otimes P_{z_n})(P_{x_1} \otimes ... \otimes P_{x_n})\|^2_\infty \tag{D.5}$$

and $P_{z_1} \otimes ... \otimes P_{z_n}$, $P_{x_1} \otimes ... \otimes P_{x_n}$ are the projectors implementing the Z- and X-measurements on A's subsystems, respectively. In particular, $P_{z_i} \in \{P_{|0\rangle}, P_{|1\rangle}\}$ and $P_{x_i} \in \{P_{|+\rangle}, P_{|-\rangle}\}$. Therefore one can easily compute the quality factor q in this specific case: $q = n$[11].

We can now bound the max-entropy (A.15) of the classical-quantum states $\rho^n_{X\mathbf{B}}$ by performing the same projective measurement on all $\mathbf{B}$'s subsystems and by employing the data processing inequality [24, theorem 6.2]:

$$H^{\bar{\varepsilon},{\rm P}}_{\max}(\rho^n_{X\mathbf{B}}|\mathbf{B}) \leqslant H^{\bar{\varepsilon},{\rm P}}_{\max}(\rho^n_{X\mathbf{X}}|\mathbf{X}) \tag{D.6}$$

which inserted in (D.4) yields:

$$H^{\bar{\varepsilon},{\rm P}}_{\min}(\rho^n_{ZE}|E) \geqslant n - H^{\bar{\varepsilon},{\rm P}}_{\max}(\rho^n_{X\mathbf{X}}|\mathbf{X}). \tag{D.7}$$

Finally one can bound the max-entropy of the classical state $\rho^n_{X\mathbf{X}}$—i.e. of the probability distribution $P^n_{X\mathbf{X}}$—by means of [14, lemma 3]. As a matter of fact, one can consider the whole set of $\mathbf{B}$ as one single Bob with the X-outcomes vector defined as:

$$\mathbf{X}' = \mathbf{X_1} \oplus ... \oplus \mathbf{X_{N-1}}, \tag{D.8}$$

where the random vectors are defined in (C.12). Under this classical operation the data processing inequality holds:

[11] The norm $\|\cdot\|_\infty$ evaluates the largest singular value.

$$H_{\max}^{\bar{\varepsilon},\mathrm{P}}(\rho_{X\mathbf{X}}^{n}|\mathbf{X}) = H_{\max}^{\bar{\varepsilon},\mathrm{P}}(P_{X\mathbf{X}}^{n}|\mathbf{X}) \leqslant H_{\max}^{\bar{\varepsilon},\mathrm{P}}(P_{XX'}^{n}|X'). \tag{D.9}$$

In this fashion, the PE parameter Q_X^m is exactly the frequency of discordant bits between $\mathbf{X_a}$ and $\mathbf{X}'$ (see its definition in (C.14)). Therefore one can apply [14, lemma 3]:

$$H_{\max}^{\varepsilon_{\mathrm{PE}},\mathrm{P}}(P_{XX'}^{n}|X') \leqslant nh(Q_X^m + 2\xi(\varepsilon_x, n, m)) \tag{D.10}$$

which combined with (D.9) yields:

$$H_{\max}^{\varepsilon_{\mathrm{PE}},\mathrm{P}}(\rho_{X\mathbf{X}}^{n}|\mathbf{X}) \leqslant nh(Q_X^m + 2\xi(\varepsilon_x, n, m)). \tag{D.11}$$

Finally inserting (D.11) in (D.7) after having fixed: $\bar{\varepsilon} = \varepsilon_{\mathrm{PE}}$, yields the desired result:

$$H_{\min}^{\varepsilon_{\mathrm{PE}},\mathrm{P}}(\rho_{ZE}^{n}|E) \geqslant n(1 - h(Q_X^m + 2\xi(\varepsilon_x, n, m))). \tag{D.12}$$

*Computable key length.*By employing the bounds on the leakage (D.3) and on the min-entropy (D.12) in theorem 1, one obtains the computable key length presented in theorem 3, which only depends on the PE statistics and on the security parameters.

D.2. N-six-state protocol

As anticipated in section 2.1, the strategy adopted to achieve a computable expression of the N-six-state key length relies on the PS technique [12]. Such a technique allows to prove a given property of a quantum channel, acting on a general multipartite state, by just proving it on inputs consisting of identical and independent copies of a state on a single subsystem. Therefore one can infer the security of a QKD protocol -viewed as a quantum channel- under coherent attacks (arbitrary input) from the security of the same protocol under collective attacks (product state input) [27]. For this reason in the following we restrict E's action to collective attacks, meaning that the quantum state describing the parties' raw keys and E's quantum system is a product state: $\rho_{Z\mathbf{K}E}^{\otimes n}$, and the raw keys' probability distribution is a product distribution: $(P_{Z\mathbf{K}})^n$.

Leakage. We start from the general upper bound stated in (1.7) and employ the finite version of the AEP for probability distributions [28, theorem 1] to further bound the smooth Rényi zero-entropy (A.7):

$$H_0^{\varepsilon_{\mathrm{PE}}}((P_{ZK_i})^n|K_i) \leqslant n\left[H(Z|K_i) + \log_2(5)\sqrt{\frac{2\log_2(1/(2\varepsilon_{\mathrm{PE}}))}{n}}\right], \tag{D.13}$$

where we fixed $\varepsilon' = \varepsilon_{\mathrm{PE}}$ as defined in (C.18) and where $H(Z|K_i)$ is the conditional Shannon entropy of P_{ZK_i}. Thanks to the symmetries introduced by the extended depolarization procedure [5] each raw key bit is uniform: $H(Z) = H(K_i) = 1$. These constraints on the probability distribution P_{ZK_i} imply that its conditional entropy $H(Z|K_i)$ can be expressed as a function of the only parameter P_{AB_i} as follows: $H(Z|K_i) = h(P_{AB_i})$.

Finally, we characterize the probability P_{AB_i} through the observed frequency $Q_{AB_i}^m$ in PE (C.17). In particular, we exploit the composable-security property by adding $\varepsilon_{\mathrm{PE}}$ to the total security parameter and by maximizing (D.13) over the allowed probabilities. Combining this with theorem 2 leads to the desired result. The leakage occurring in the N-six-state protocol, implemented with the optimal one-way, $\varepsilon_{\mathrm{EC}}$-fully secure and $2(N-1)\varepsilon_{\mathrm{PE}}$ —robust EC protocol, is:

$$\begin{aligned}\mathrm{leak}_{\mathrm{EC}}^{\mathrm{NQKD}} \leqslant n&\left[\max_i h(Q_{AB_i}^m + 2\eta(\varepsilon_z, 2, m)) + \log_2(5)\sqrt{\frac{2\log_2(1/(2\varepsilon_{\mathrm{PE}}))}{n}}\right]\\ &+ \log_2\frac{2(N-1)}{\varepsilon_{\mathrm{EC}}}.\end{aligned} \tag{D.14}$$

Min-entropy. We can bound the min-entropy of a product state via the finite version of the AEP for quantum states, reported in [29, equation (B7)]:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{ZE}^{\otimes n}|E) \geqslant n\left(S(\rho_{ZE}) - S(\rho_E) - 5\sqrt{\frac{\log_2(1/\bar{\varepsilon})}{n}}\right), \tag{D.15}$$

where $S(\rho)$ is the Von Neumann entropy. The rhs of (D.15) can be recast in terms of the probabilities P_X and P_Z, by following analogous steps in [5] and by exploiting the symmetries of the single-signal state due to the extended depolarization procedure.

Finally, the probabilities P_X and P_Z are characterized by the PE measurements through (C.17). Thus we can minimize the min-entropy bound over the allowed probabilities while adding the PE failure probability $\varepsilon_{\mathrm{PE}}$ to the total security parameter. These operations yield:

$$H_{\min}^{\bar{\varepsilon}}(\rho_{ZE}^{\otimes n}|E) \geqslant n \inf_{\Gamma_{\mathrm{PE}}}\left[\left(1-\frac{P_Z}{2}-P_X\right)\log_2\left(1-\frac{P_Z}{2}-P_X\right)\right.$$
$$\left.+\left(P_X-\frac{P_Z}{2}\right)\log_2\left(P_X-\frac{P_Z}{2}\right)+(1-P_Z)(1-\log_2(1-P_Z))-5\sqrt{\frac{\log_2(1/\bar{\varepsilon})}{n}}\right], \tag{D.16}$$

where the set Γ_{PE} is defined in (2.6).

Computable key length. By substituting the bounds (D.14) and (D.16) into theorem 1, one obtains the computable key length of the N-six-state protocol when performed under collective attacks.

The PS technique [12] allows to extend the security of a protocol against collective attacks, to any kind of attack, by just shortening the key length and introducing a corrective factor on the total security parameter. Consider an NQKD protocol $\mathcal{E}$ acting on L-partite systems (the L shared signals), where each of the L constituents has dimension d (in our case each signal describes the state of N qubits, thus $d = 2^N$). If $\mathcal{E}$ is $\varepsilon_{\mathrm{tot}}$-secure against collective attacks, then the protocol $\mathcal{E}'$ obtained from $\mathcal{E}$ by shortening the output of the hashing by '$2(d^2-1)\log_2(L+1)$' bits is $(L+1)^{(d^2-1)}\varepsilon_{\mathrm{tot}}$-secure against coherent attacks. By applying the PS corrections to the N-six-state key valid for collective attacks, we extend its validity to coherent attacks, yielding the final result: theorem 4.

Appendix E. Information leaked from the classical channel

The following lemma is the result of a private communication [10] with Renato Renner. It shows that the additional information that E has about A's raw key X due to EC's classical communication can be quantified by the leakage (as defined in definition 4), even for a general two-way EC protocol. The proof relies on the fact that the ε-environment of the entropies is defined via the purified distance. The crucial advantage of this definition of distance is that one can always find extensions and purifications of quantum states without increasing their distance [30].

Lemma 3. *Let $\rho_{X\mathbf{KC}E}$ be a density operator with X, $\mathbf{K}$, $\mathbf{C}$ classical, such that the Markov chain condition $\mathbf{C} \leftrightarrow (X, \mathbf{K}) \leftrightarrow E$ holds. Then, for any $\varepsilon \geqslant 0$,*

$$H_{\min}^{\varepsilon,\mathrm{P}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}^{\varepsilon,\mathrm{P}}(\rho_{XE}|E) - H_0(\rho_{\mathbf{C}}) + H_{\min}(\rho_{X\mathbf{KC}}|\rho_{X\mathbf{K}}). \tag{E.1}$$

Proof. We first prove the statement in the special case where $\varepsilon = 0$. This is achieved by the following chain of inequalities:

$$\begin{aligned} H_{\min}(\rho_{X\mathbf{C}E}|\mathbf{C}E) &\overset{(1)}{\geqslant} H_{\min}(\rho_{X\mathbf{C}E}|E) - H_0(\rho_{\mathbf{C}}) \\ &\overset{(2)}{\geqslant} H_{\min}(\rho_{X\mathbf{C}E}|\rho_{XE}) + H_{\min}(\rho_{XE}|E) - H_0(\rho_{\mathbf{C}}) \\ &\overset{(3)}{\geqslant} H_{\min}(\rho_{X\mathbf{KC}E}|\rho_{X\mathbf{K}E}) + H_{\min}(\rho_{XE}|E) - H_0(\rho_{\mathbf{C}}) \\ &\overset{(4)}{\geqslant} H_{\min}(\rho_{X\mathbf{KC}}|\rho_{X\mathbf{K}}) + H_{\min}(\rho_{XE}|E) - H_0(\rho_{\mathbf{C}}), \end{aligned} \tag{E.2}$$

where we used: (1) chain rule [8, section 3.1.3], (2) proposition 1 at the end of this section, (3) strong subadditivity [8, lemma 3.1.7], and (4) Markov chain condition.

To prove the general statement, for any $\varepsilon \geqslant 0$, let ρ'_{XE} be the state ε-close to ρ_{XE} (with respect to the purified distance) such that:

$$H_{\min}^{\varepsilon,\mathrm{P}}(\rho_{XE}|E) = H_{\min}(\rho'_{XE}|E). \tag{E.3}$$

Thanks to the definition of purified distance we can find an extension of ρ'_{XE}, namely $\rho'_{X\mathbf{K}E}$, such that it is still ε-close to $\rho_{X\mathbf{K}E} = \mathrm{Tr}_{\mathbf{C}}[\rho_{X\mathbf{KC}E}]$ [30], corollary 9]. We can assume, without loss of generality, that $\rho'_{X\mathbf{K}E}$ is classical on X and $\mathbf{K}$ and that $\rho'_{X\mathbf{K}}$ has support contained in the support of $\rho_{X\mathbf{K}}$[12]. Furthermore, let $\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}}$ be the CPTP recovery map that recovers $\mathbf{C}$ from $(X, \mathbf{K})$, i.e.: $\rho_{X\mathbf{KC}} = \mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}}(\rho_{X\mathbf{K}})$. Since X, $\mathbf{K}$ and $\mathbf{C}$ are classical, this map can be chosen to be of the form:

$$\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}}: \ Q_{X\mathbf{K}} \mapsto \sum_{x,\mathbf{k},\mathbf{c}} P_{\mathbf{C}|X\mathbf{K}}(\mathbf{c}|x,\mathbf{k})\langle x|\langle\mathbf{k}|Q_{X\mathbf{K}}|x\rangle|\mathbf{k}\rangle\,|x\rangle\langle x|\otimes|\mathbf{k}\rangle\langle\mathbf{k}|\otimes|\mathbf{c}\rangle\langle\mathbf{c}|, \tag{E.4}$$

where $P_{\mathbf{C}|X\mathbf{K}}$ is the conditional probability distribution defined by the EC protocol which led to the given state $\rho_{X\mathbf{KC}E}$. According to the definition of min-entropy (A.9), for any $Q_{X\mathbf{K}}$ that is classical on X and $\mathbf{K}$ we have that:

[12] It is always possible to turn subsystems into classical ones by applying a CPTP map that projects onto the elements of a fixed 'classical' basis. Note that such a map cannot increase the distance between states.

$$H_{\min}(\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}}(Q_{X\mathbf{K}})|Q_{X\mathbf{K}}) = -\log_2\lambda, \tag{E.5}$$

where λ is the minimum real number that satisfies the inequality:

$$\lambda\ \mathrm{id}_{\mathbf{C}} \otimes Q_{X\mathbf{K}} - \sum_{x,\mathbf{k},\mathbf{c}} P_{\mathbf{C}|X\mathbf{K}}(\mathbf{c}|x,\ \mathbf{k})\langle x|\langle\mathbf{k}|Q_{X\mathbf{K}}|x\rangle|\mathbf{k}\rangle|x\rangle\langle x| \otimes |\mathbf{k}\rangle\langle\mathbf{k}| \otimes |\mathbf{c}\rangle\langle\mathbf{c}| \geqslant 0,$$

or equivalently:

$$\lambda - P_{\mathbf{C}|X\mathbf{K}}(\mathbf{c}|x,\ \mathbf{k}) \geqslant 0 \quad \forall\, x,\ \mathbf{k},\ \mathbf{c}:\ \langle x|\langle\mathbf{k}|Q_{X\mathbf{K}}|x\rangle|\mathbf{k}\rangle > 0. \tag{E.6}$$

The minimum λ satisfying (E.6) is the maximum eigenvalue of the non-normalized state $\sum_{\mathbf{c}} P_{\mathbf{C}|X\mathbf{K}}(\mathbf{c}|x,\ \mathbf{k})|\mathbf{c}\rangle\langle\mathbf{c}|$, further maximized over x and $\mathbf{k}$. Thus from [8, remark 3.1.3] combined with (E.5) we get:

$$H_{\min}(\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}}(Q_{X\mathbf{K}})|Q_{X\mathbf{K}}) = \inf_{x,\mathbf{k}:\ \langle x|\langle\mathbf{k}|Q_{X\mathbf{K}}|x\rangle|\mathbf{k}\rangle>0} H_{\min}\left(\sum_{\mathbf{c}} P_{\mathbf{C}|X\mathbf{K}}(\mathbf{c}|x,\ \mathbf{k})|\mathbf{c}\rangle\langle\mathbf{c}|\right). \tag{E.7}$$

Because $\rho_{X\mathbf{KC}E}$ satisfies the Markov condition $\mathbf{C} \leftrightarrow (X,\ \mathbf{K}) \leftrightarrow E$, we have:

$$\rho_{X\mathbf{KC}E} = (\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}} \otimes \mathrm{id}_E)(\rho_{X\mathbf{K}E}). \tag{E.8}$$

Therefore, defining:

$$\rho'_{X\mathbf{KC}E} = (\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}} \otimes \mathrm{id}_E)(\rho'_{X\mathbf{K}E}) \tag{E.9}$$

and using the fact that CPTP maps cannot increase the distance between states, $\rho'_{X\mathbf{KC}E}$ is ε-close to $\rho_{X\mathbf{KC}E}$, so that:

$$H_{\min}^{\varepsilon,\mathrm{P}}(\rho_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}(\rho'_{X\mathbf{C}E}|\mathbf{C}E). \tag{E.10}$$

Furthermore, since $\mathrm{supp}(\rho'_{X\mathbf{K}}) \subseteq \mathrm{supp}(\rho_{X\mathbf{K}})$, the action of the recovery map is such that $\mathrm{supp}(\rho'_{\mathbf{C}}) \subseteq \mathrm{supp}(\rho_{\mathbf{C}})$, and hence by [8, remark 3.1.3] it holds:

$$H_0(\rho_{\mathbf{C}}) \geqslant H_0(\rho'_{\mathbf{C}}). \tag{E.11}$$

Note also that, because of (E.7), the min-entropy of $\mathbf{C}$ conditioned on X and $\mathbf{K}$ of any classical state $Q_{X\mathbf{K}}$ only depends on the recovery map $\mathcal{R}_{X\mathbf{K}\to X\mathbf{KC}}$ and on the support of $Q_{X\mathbf{K}}$. Since the support of $\rho'_{X\mathbf{K}}$ is contained in the support of $\rho_{X\mathbf{K}}$, we have:

$$H_{\min}(\rho_{X\mathbf{KC}}|\rho_{X\mathbf{K}}) \leqslant H_{\min}(\rho'_{X\mathbf{KC}}|\rho'_{X\mathbf{K}}). \tag{E.12}$$

Since $\rho'_{X\mathbf{KC}E}$ by construction satisfies the Markov chain condition, inequality (E.2) also holds for this operator, i.e.:

$$H_{\min}(\rho'_{X\mathbf{C}E}|\mathbf{C}E) \geqslant H_{\min}(\rho'_{X\mathbf{KC}}|\rho'_{X\mathbf{K}}) + H_{\min}(\rho'_{X E}|E) - H_0(\rho'_{\mathbf{C}}). \tag{E.13}$$

Combining (E.13), (E.3), (E.10), (E.11) and (E.12) yields the claim. □

Proposition 1. *For any density operator* ρ_{ABC}*:*

$$H_{\min}(\rho_{ABC}|C) \geqslant H_{\min}(\rho_{ABC}|\rho_{BC}) + H_{\min}(\rho_{BC}|C). \tag{E.14}$$

Proof. By definition of min-entropy (A.12), there exists a density operator σ_C such that:

$$\rho_{BC} \leqslant 2^{-H_{\min}(\rho_{BC}|C)}\mathrm{id}_B \otimes \sigma_C. \tag{E.15}$$

We thus have:

$$\rho_{ABC} \leqslant 2^{-H_{\min}(\rho_{ABC}|\rho_{BC})}\mathrm{id}_A \otimes \rho_{BC} \leqslant 2^{-H_{\min}(\rho_{ABC}|\rho_{BC})-H_{\min}(\rho_{BC}|C)}\mathrm{id}_{AB} \otimes \sigma_C \tag{E.16}$$

which implies the claim. □

ORCID iDs

Federico Grasselli https://orcid.org/0000-0003-2966-7813
Hermann Kampermann https://orcid.org/0000-0002-0659-6699

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Scarani V, Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[4] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 *npj Quantum Inf.* **2** 16025
[5] Epping M, Kampermann H, Macchiavello C and Bruß D 2017 *New J. Phys.* **19** 093012

[6] Ribeiro J, Murta G and Wehner S 2018 *Phys. Rev.* A **97** 022307

[7] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018

[8] Renner R 2008 *Int. J. Quantum Inf.* **6** 1

[9] Portmann C and Renner R 2014 arXiv:1409.3525

[10] Renner R 2017 private communication

[11] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506

[12] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504

[13] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501

[14] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634

[15] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501

[16] Friedman R A, Dupuis F, Fawzi O, Renner R and Vidick T 2018 *Nat. Commun.* **9** 459

[17] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880

[18] Mermin N D 1990 *Phys. Rev. Lett.* **65** 1838

[19] Ardehali M 1992 *Phys. Rev.* A **46** 5375

[20] Belinskii A V and Klyshko D N 1993 *Phys.—Usp.* **36** 653

[21] Tomamichel M, Schaffner C, Smith A and Renner R 2011 *IEEE Trans. Inf. Theory* **57** 8

[22] Tomamichel M, Colbeck R and Renner R 2009 *IEEE Trans. Inf. Theory* **55** 5840–7

[23] Renner R and Wolf S 2004 *Proc. Int. Symp. on Information Theory*

[24] Tomamichel M 2016 *Quantum Information Processing with Finite Resources* (Berlin: Springer)

[25] Bouman N J and Fehr S 2010 Sampling in a quantum population, and applications *Advances in Cryptology—CRYPTO* ed T Rabin (Berlin: Springer)

[26] Bratzik S, Mertz M, Kampermann H and Bruß D 2011 *Phys. Rev.* A **83** 022330

[27] Sheridan L, Le T P and Scarani V 2010 *New J. Phys.* **12** 123019

[28] Holenstein T and Renner R 2011 *IEEE Trans. Inf. Theory* **57** 4

[29] Mertz M, Kampermann H, Bratzik S and Bruß D 2013 *Phys. Rev.* A **87** 012315

[30] Tomamichel M, Colbeck R and Renner R 2010 *IEEE Trans. Inf. Theory* **56** 9

C Practical decoy-state method for twin-field quantum key distribution

Title:	Practical decoy-state method for twin-field quantum key distribution
Authors:	Federico Grasselli and Marcos Curty
Journal:	New Journal of Physics
Impact factor:	3.783 (2018)
Date of submission:	5 February 2019
Publication status:	Published
Contribution by FG:	First author (input approx. 85%)

This publication corresponds to reference [GC19]. A summary of its content is presented in chapter 7.

I was triggered to work on this project by MC, who clearly stated the project's goals and provided insight on how one could obtain the analytical yields bounds. I independently derived the new analytical yields bounds reported in the paper and re-derived all the other analytical quantities appearing in the protocol's key rate, in order to present them in a coherent and precise fashion. I performed all the numerical simulations in the paper. The Mathematica code used for the simulations was completely wrote by me ex novo. I followed MC's suggestions on what simulations to perform and on how to present them in the plots. I extrapolated the positive results of the simulations and adjusted the way in which they are presented. I wrote the whole paper, which then benefited from the useful comments of MC.

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
5 February 2019

REVISED
3 June 2019

ACCEPTED FOR PUBLICATION
19 June 2019

PUBLISHED
1 July 2019

Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Practical decoy-state method for twin-field quantum key distribution

Federico Grasselli[1] and Marcos Curty[2]

[1] Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany
[2] Escuela de Ingeniería de Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain

E-mail: federico.grasselli@hhu.de

Keywords: twin-field quantum key distribution, decoy-state method, single-photon interference, measurement-device-independent quantum key distribution (MDI-QKD), analytical bounds

Abstract

Twin-field (TF) quantum key distribution (QKD) represents a novel QKD approach whose principal merit is to beat the point-to-point private capacity of a lossy quantum channel, thanks to performing single-photon interference in an untrusted node. Indeed, recent security proofs of various TF-QKD type protocols have confirmed that the secret key rate of these schemes scales essentially as the square root of the transmittance of the channel. Here, we focus on the TF-QKD protocol introduced by Curty *et al*, whose secret key rate is nearly an order of magnitude higher than previous solutions. Its security relies on the estimation of the detection probabilities associated to various photon-number states through the decoy-state method. We derive analytical bounds on these quantities assuming that each party uses either two, three or four decoy intensity settings, and we investigate the protocol's performance in this scenario. Our simulations show that two decoy intensity settings are enough to beat the point-to-point private capacity of the channel, and that the use of four decoys is already basically optimal, in the sense that it almost reproduces the ideal scenario of infinite decoys. We also observe that the protocol seems to be quite robust against intensity fluctuations of the optical pulses prepared by the parties.

The last few decades have witnessed major advancements in the field of quantum communication [1, 2], with quantum key distribution (QKD) [3–13] being its most developed application. Recent experiments over about 400 km of optical fibers [14, 15] and over about 1000 km of satellite-to-ground links [16, 17] demonstrated that QKD over long distances is possible. Despite such remarkable experimental achievements, the private capacity of point-to-point QKD is intrinsically limited by fundamental bounds [18, 19]. These bounds state that in the high-loss regime the key rate scales basically linearly with the transmittance of the channel connecting the end-users Alice and Bob, i.e. it decreases exponentially with the total channel length. This imposes strict practical constraints on the possibility of achieving point-to-point QKD over arbitrary long distances.

A way to overcome this limitation is to employ one or more intermediate nodes in the quantum channel connecting the parties. For instance, the use of quantum repeaters [20] yields a polynomial scaling of the communication efficiency with the distance [21]. Moreover, a quantum repeater scheme can be arbitrarily iterated along the quantum channel, thus increasing in principle the total communication distance between Alice and Bob as much as desired. Unfortunately, however, quantum repeaters are very challenging to build in practice with current technology: they either require quantum memories [20–22] or quantum error correction [23, 24]. Of course, technology is improving, and quantum repeaters may become viable in the future.

Other solutions, which attain a square-root improvement in the scaling of the key rate with respect to the transmittance of the channel, are obtained by placing a single untrusted relay between Alice and Bob. Such protocols include, for instance, measurement-device-independent-QKD [6] (MDI-QKD) with quantum memories [25, 26] and adaptive MDI-QKD featuring quantum non-demolition measurements [27]. The philosophy behind both types of protocols is that the central relay is able to adapt the pairings of photons received from Alice and Bob to the photon losses. In this way, for every signal sent by Alice and Bob to the central relay, just one of the two signals is required to arrive, leading to the mentioned square-root improvement in the key rate scaling. However, both protocols still require two-photon interference in the central node, as in the

© 2019 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft

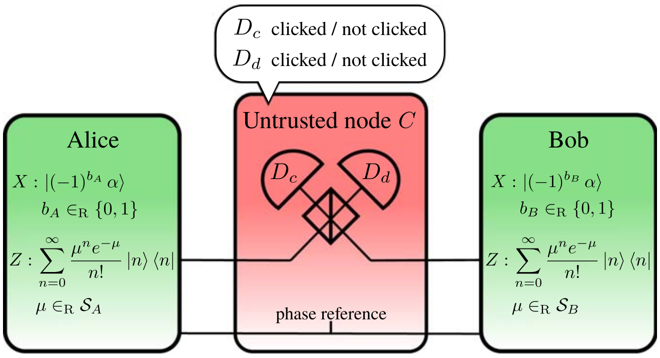
D_c clicked / not clicked
D_d clicked / not clicked
Alice
$X : |(-1)^{b_A}\,\alpha\rangle$
$b_A \in_{\mathrm{R}} \{0,1\}$
$Z : \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} |n\rangle\langle n|$
$\mu \in_{\mathrm{R}} \mathcal{S}_A$
Untrusted node C
D_c
D_d
phase reference
Bob
$X : |(-1)^{b_B}\,\alpha\rangle$
$b_B \in_{\mathrm{R}} \{0,1\}$
$Z : \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} |n\rangle\langle n|$
$\mu \in_{\mathrm{R}} \mathcal{S}_B$

Figure 1. The twin-field QKD protocol introduced in [33].

original MDI-QKD scheme [6]. More recently, [28] proposed the twin-field (TF) QKD protocol, still characterized by an untrusted central node, and conjectured a square-root improvement in the key rate scaling. This scaling has been later on confirmed in [29, 30] for two variants of the original scheme. The advantage of TF-QKD lies in the fact that it is designed to generate key bits from single-photon interference in the central node, thus naturally retaining the scaling with the square-root of the transmittance without the need to adapt to photon losses via sophisticated devices.

Since the original proposal, there has been an intense research activity to develop different versions of TF-QKD protocols equipped with their security proofs [29–33] as well as to investigate their experimental feasibility [34–36]. Among these protocols, the one that seems to deliver the higher secret ket rate [37] is that introduced in [33]. Its security relies on the ability to estimate the detection statistics (usually called yields) of various Fock states sent by Alice and Bob through the decoy-state method [38–40]. The key-rate simulations provided in [33] indeed exhibit an improved scaling with the loss, but the estimation of the yields is only carried out by means of *numerical* tools based on linear programming and considering only the case of three decoy intensity settings.

In this paper, we derive *analytical* bounds on the yields which are required to evaluate the key rate formula of [33], assuming two, three and four decoy intensity settings. In so doing, we are able to show, for instance, that the use of two decoy intensity settings is already enough to beat the point-to-point private capacity bound reported in [19]. Also, we show that the use of four decoys is basically optimal in the sense that the resulting secret key rate is already very close to the ideal scenario which assumes infinite decoy intensity settings. Analytical bounds imply a fully-analytical expression for the protocol's secret key rate, which could be very convenient for performance optimization in scenarios where the number of parameters is high, like for instance in finite-key security analyses. In addition, we study how the performance of TF-QKD is affected under intensity fluctuations, which are inevitable in practice, and we demonstrate that the protocol in [33] seems to be actually quite robust against such fluctuations.

Like in [33], for simplicity, here we focus on the asymptotic-key rate scenario. However, we remark that by using the techniques reported in [41], it is cumbersome but straightforward to adapt our analytical methods also to the finite-key rate scenario, where, as mentioned above, it becomes particularly useful to have analytical bounds for the main quantities that enter the key rate formula.

The article is structured as follows. In section 1 we present the TF protocol from [33] and highlight the main yields that need to be bounded. In section 2 we provide the analytical bounds on the yields for the case of two decoys (the cases of three and four decoys are treated in appendices C and D, respectively). In section 3 we provide simulations of the secret key rate versus the loss for a typical channel model (briefly described in appendix A), and we also evaluate the effect of intensity fluctuations. We conclude the paper in section 4.

1. The TF-QKD protocol

As discussed above, we consider the TF-QKD protocol presented in [33] and sketched in figure 1. Alice and Bob establish a secret shared key by sending optical pulses to a central untrusted node, *C*. It is assumed that the node *C* shares a phase reference with Alice and Bob, which can be achieved by the transmission of strong optical pulses. The protocol is composed of the following five steps.

(i) Alice (Bob) chooses the X-basis with probability p_X and the Z-basis with probability $p_Z = 1 - p_X$. Upon choosing the X-basis, Alice (Bob) prepares an optical pulse in a coherent state $|\alpha\rangle$ or $|-\alpha\rangle$ at random, corresponding to the key bit $b_A = 0$ $(b_B = 0)$ or $b_A = 1$ $(b_B = 1)$, respectively. Upon choosing the Z-basis, she (he) prepares an optical pulse in a phase-randomized coherent state:

$$\hat{\rho}_{\beta_A} = \frac{1}{2\pi}\int_0^{2\pi} \mathrm{d}\theta |\beta_A \mathrm{e}^{\mathrm{i}\theta}\rangle\langle\beta_A \mathrm{e}^{\mathrm{i}\theta}| = \sum_{n=0}^{\infty} \frac{(\beta_A^2)^n \mathrm{e}^{-\beta_A^2}}{n!}|n\rangle\langle n| \tag{1.1}$$

($\hat{\rho}_{\beta_B}$) whose intensity β_A^2 (β_B^2) is drawn randomly from a set $\mathcal{S}_A = \{\beta_i^2\}_i$ ($\mathcal{S}_B = \{\beta_j^2\}_j$) of real non-negative numbers.

(ii) Both parties send their optical pulses to the untrusted node C via optical channels in a synchronized manner.

(iii) The central node C applies a balanced beamsplitter to the incoming pulses and features two threshold detectors at its output ports. The detector placed at the output port associated to constructive (destructive) interference is denoted by D_c (D_d).

(iv) The node C announces the measurement outcome k_c (k_d) of detector D_c (D_d), with $k_c = 0$ and $k_c = 1$ ($k_d = 0$ and $k_d = 1$) corresponding to a no-click and a click event, respectively.

(v) Alice and Bob form their raw keys with the bits b_A and b_B collected when both parties chose the X-basis and node C reported a click in only one detector ($k_c + k_d = 1$). Bob flips his bits b_B for which the click occurred in D_d.

1.1. Secret key rate formula

The security analysis performed in [33] yields the following lower bound on the asymptotic key rate R:

$$R \geqslant \max\{R_{10}, 0\} + \max\{R_{01}, 0\}, \tag{1.2}$$

where the terms $R_{k_ck_d}$, for $(k_c, k_d) \in \{(1, 0), (0, 1)\}$, are defined as:

$$R_{k_ck_d} = p_X^2\, p(k_c, k_d)[1 - f\, h(e_{k_ck_d}) - h(e_{k_ck_d}^{\mathrm{ph}})], \tag{1.3}$$

with $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ being the binary entropy function, f the inefficiency function associated to error correction, and $p(k_c, k_d)$ the conditional probability that node C announces the outcome (k_c, k_d) when both parties selected the X-basis. The probability $p(k_c, k_d)$ can be expressed as:

$$p(k_c, k_d) = \sum_{b_A,b_B=0}^{1} p(b_A, b_B)p(k_c, k_d|b_A, b_B), \tag{1.4}$$

where $p(b_A, b_B)$ is the joint probability of Alice and Bob preparing the coherent states $|(-1)^{b_A}\alpha\rangle$ and $|(-1)^{b_B}\alpha\rangle$, respectively. According to the protocol description above, we have: $p(b_A, b_B) = 1/4\ \forall\, b_A, b_B$. $p(k_c, k_d|b_A, b_B)$ instead denotes the conditional probability that node C announced (k_c, k_d) given that Alice and Bob sent the coherent states $|(-1)^{b_A}\alpha\rangle$ and $|(-1)^{b_B}\alpha\rangle$, respectively. Since we consider the asymptotic key-rate scenario, we assume that $p(k_c, k_d|b_A, b_B)$ coincides with the correspondent distribution observed by the parties.

Finally, the terms $e_{k_ck_d}$ and $e_{k_ck_d}^{\mathrm{ph}}$ in (1.3) represent the bit-error rate in the X-basis and an upper bound on the phase-error rate, respectively. The former is defined as:

$$e_{10} = \frac{\sum_{i,j=0|i\oplus j=1}^{1} p(b_A = i, b_B = j)p(k_c = 1, k_d = 0|b_A = i, b_B = j)}{p(k_c = 1, k_d = 0)}, \tag{1.5}$$

$$e_{01} = \frac{\sum_{i=0}^{1} p(b_A = i, b_B = i)p(k_c = 0, k_d = 1|b_A = i, b_B = i)}{p(k_c = 0, k_d = 1)}, \tag{1.6}$$

and the latter as:

$$e_{k_ck_d}^{\mathrm{ph}} = \frac{1}{p(k_c, k_d)}\left[\left(\sum_{n,m=0}^{\infty} c_{2n}c_{2m}\sqrt{Y_{2n\,2m}^{k_c,k_d}}\right)^2 + \left(\sum_{n,m=0}^{\infty} c_{2n+1}c_{2m+1}\sqrt{Y_{2n+1\,2m+1}^{k_c,k_d}}\right)^2\right], \tag{1.7}$$

where the coefficients c_n are defined as $c_n = \mathrm{e}^{\frac{-\alpha^2}{2}}\alpha^n/\sqrt{n!}$ and the yields $Y_{nm}^{k_c,k_d}$ are the conditional probabilities that node C announces the outcome (k_c, k_d) given that Alice and Bob emitted an n-photon state and an m-photon state, respectively. Note that the only yields contributing to (1.7) are those $Y_{nm}^{k_c,k_d}$ such that $n + m$ is an even number.

The yields $Y_{nm}^{k_c,k_d}$ are quantities that are not directly observed by the parties, however they can be estimated either numerically or analytically with techniques based on the decoy-state method [38–40]. Here we consider the analytical approach. In particular, we assume that Alice and Bob have at their disposal either two, three or four decoy intensity settings when choosing the Z-basis. To each further decoy intensity correspond additional linear constraints on the yields, leading to tighter estimations of $Y_{nm}^{k_c,k_d}$ and thus to a higher key rate. However, a finite number of decoys only allows to derive non-trivial upper bounds[3] on a limited number of yields in (1.7), whereas the other yields are set to 1. Nevertheless, even bounding just four yields in a non-trivial way is enough for the secret key rate to beat the point-to-point private capacity bound (PLOB bound) [19] at high losses (see section 3). Also, as we show below, with four decoy intensity settings one can already obtain a secret key rate very close to that achievable with infinite decoy intensity settings.

We remark that standard decoy-state-based QKD protocols require to *lower* bound the value of a few yields (typically those associated to vacuum and single-photon pulses) [42], while the TF-QKD protocol considered here upper bounds the value of the phase-error rate (1.7) by *upper* bounding several yields. In particular, we upper bound the yields $Y_{nm}^{k_c,k_d}$ for $(n,\ m)\in\mathcal{I}$, where $\mathcal{I}$ is a certain subset of $\{(n,\ m)|\ n,\ m\in\mathbb{N}_0\}$ which depends on the number of decoys. Thanks to the derived upper bounds on the yields (which we shall denote by Y_{nm}^{U,k_c,k_d}) we are able to estimate the phase error rate (1.7) as follows:

$$e_{k_ck_d}^{\mathrm{ph}}\leqslant\frac{1}{p(k_c,\ k_d)}\left[\left(\sum_{(2n,2m)\in\mathcal{I}}c_{2n}c_{2m}\sqrt{Y_{2n\ 2m}^{U,k_c,k_d}}+\sum_{(2n,2m)\notin\mathcal{I}}c_{2n}c_{2m}\right)^2\right.$$
$$\left.+\left(\sum_{(2n+1,2m+1)\in\mathcal{I}}c_{2n+1}c_{2m+1}\sqrt{Y_{2n+1\ 2m+1}^{U,k_c,k_d}}+\sum_{(2n+1,2m+1)\notin\mathcal{I}}c_{2n+1}c_{2m+1}\right)^2\right].\tag{1.8}$$

2. Yields estimation

When both Alice and Bob choose the Z-basis in the first step of the TF-QKD protocol, they prepare phase-randomized coherent states with intensities β_A^2 and β_B^2, respectively, and send them to C. From Eve's viewpoint, she cannot distinguish this scenario from the case in which the parties prepared number states $|n\rangle$ and $|m\rangle$ according to the Poissonian distributions $P_{\beta_A^2}(n)$ and $P_{\beta_B^2}(m)$ (see equation (1.1)), where $P_\mu(n)=\mathrm{e}^{-\mu}\mu^n/n!$. Therefore Eve's attack can only depend on the number states $|n\rangle$ and $|m\rangle$ but not on the signals' intensities β_A^2 and β_B^2. As a consequence, the probability that Eve announces outcomes (k_c, k_d) only depends on the number of photons (n, m) she received from Alice and Bob, i.e. the yields $Y_{nm}^{k_c,k_d}$ are independent of the decoy intensities chosen by the parties.

For this reason, one can derive a set of linear constraints on the yields $Y_{nm}^{k_c,k_d}$ by expressing the experimentally observed gains $Q_{k_c,k_d}^{\beta_A^2,\beta_B^2}$—which are defined as the conditional probabilities that node C announced the outcome (k_c, k_d) given that Alice and Bob sent phase-randomized coherent states of intensities β_A^2 and β_B^2, respectively—in terms of the yields:

$$Q_{k_c,k_d}^{\beta_A^2,\beta_B^2}=\sum_{n,m=0}^{\infty}\mathrm{e}^{-\beta_A^2-\beta_B^2}\frac{(\beta_A^2)^n(\beta_B^2)^m}{n!m!}Y_{nm}^{k_c,k_d}.\tag{2.1}$$

As it is clear from (2.1), to every distinct pair of decoy intensities $(\beta_A^2,\ \beta_B^2)$ corresponds a new constraint on the set of infinite yields $\{Y_{nm}^{k_c,k_d}\}_{n,m}$, which leads to tighter upper bounds and thus to a higher secret key rate. On the other hand, having a large number of decoy intensities is experimentally demanding, hence the need to derive the tightest possible bounds on the yields with a limited number of decoys.

In this section we present a simple analytical method to obtain tight bounds on the yields of largest contribution[4] in (1.7)—i.e. relative to the largest coefficients c_n—when the parties use two intensity settings in the Z-basis. It is basically a Gaussian elimination-type technique but involving infinite-size coefficient matrices. In particular, the guiding principle that we use is to combine the constraints (2.1) so that in the resulting expression the yield to be bounded is the one with the largest coefficient, while the yields which had larger coefficients in the initial constraints have been removed in the combination. However, in some cases it turns out that is not possible to remove all the yields with larger coefficients than the one to be bounded, due to a lack of decoy intensity settings (i.e. constraints). In other cases, we manage to remove from the resulting expression even some yields which had a smaller coefficient than the one to be bounded. Such a procedure can be readily extended to the case of three and four decoy intensity settings. The results for these last two cases are presented in appendices C and D, respectively.

From now on, we assume that both optical channels linking the parties to the central node C have the same transmittance $\sqrt{\eta}$. Therefore the set of optimal decoy intensities β_A^2 and β_B^2 is the same for both parties [43] and we define it as: $\{\mu_0, \mu_1\}$. In order to simplify the notation, we also omit the measurement outcome (k_c, k_d) from

[3] Every yield is a probability, thus it is trivially bounded by 1.

[4] The same method can-in principle-be applied to any yield, however the limited number of decoy settings prevents from obtaining a non-trivial bound on every yield.

the constraints given by (2.1). Hence the yields are subjected to the following four equality constraints:

$$\tilde{Q}^{k,l} \equiv \mathrm{e}^{\mu_k+\mu_l} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} {\mu_k}^n {\mu_l}^m \quad k,\, l \in \{0,\, 1\}, \tag{2.2}$$

and to the inequality constraints:

$$0 \leqslant Y_{nm} \leqslant 1 \quad \forall\, n,\, m. \tag{2.3}$$

Below we derive upper bounds on the yields: Y_{00}, Y_{11}, Y_{02} and Y_{20}.

2.1. Upper bound on Y_{11}

Consider the following combination of gains:

$$G_{11} = \tilde{Q}^{0,0} + \tilde{Q}^{1,1} - (\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m). \tag{2.4}$$

The subscript in G_{11} indicates the yield that is going to be bounded with this combination of gains. In (2.4) the coefficients of the yields Y_{0m} and Y_{n0}, for any n and m, are identically zero. Thus (2.4) can be rewritten as:

$$G_{11} = Y_{11}(\mu_0 - \mu_1)^2 + \sum_{\substack{n,m=1\\ n+m>2}}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m). \tag{2.5}$$

We observe that the coefficients that multiply the yields Y_{nm} are always positive, being the product of two factors of equal sign. A valid upper bound for Y_{11} is obtained considering the worst-case scenario for the other yields, taking into account that (2.3) holds. Since all the yield's coefficients carry the same sign in (2.5)—regardless of the relation between μ_0 and μ_1—, the yield Y_{11} is maximal when all the other yields are minimal. Thus the upper bound on Y_{11} is extracted by setting all the other yields to zero in (2.5):

$$Y_{11}^U = \frac{G_{11}}{(\mu_0 - \mu_1)^2}, \tag{2.6}$$

where G_{11} is defined in (2.4).

We remark that by combining the gains as in (2.4), we manage to obtain a closed expression for Y_{11} in which the contribution of all the yields Y_{0m} and Y_{n0} is removed. Additionally, Y_{11} is now the yield with the 'highest weight' in (2.5) since it has the largest coefficient. All the yield's bounds presented in this work follow the same philosophy.

2.2. Upper bound on Y_{02}

Consider the following combination of gains:

$$G_{02} = \mu_1 \tilde{Q}^{0,0} + \mu_0 \tilde{Q}^{1,1} - \mu_1 \tilde{Q}^{0,1} - \mu_0 \tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} (\mu_1 \mu_0^n - \mu_0 \mu_1^n)(\mu_0^m - \mu_1^m). \tag{2.7}$$

In (2.7) the coefficients of the yields Y_{n0} and Y_{1m} are identically zero. Thus (2.7) can be rewritten as:

$$\begin{aligned} G_{02} = &-Y_{01}(\mu_0 - \mu_1)^2 - \frac{Y_{02}}{2}(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2 - \sum_{m=3}^{\infty} \frac{Y_{0m}}{m!}(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m) \\ &+ \sum_{\substack{n=2\\ m=1}}^{\infty} \frac{Y_{nm}}{n!m!} \mu_0 \mu_1 (\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m - \mu_1^m). \end{aligned} \tag{2.8}$$

Like in the derivation of Y_{11}'s bound given by (2.6), a valid upper bound for Y_{02} is obtained by considering the worst-case scenario for the remaining yields in (2.8). More specifically, Y_{02} is maximal when the yields whose coefficient has the same sign as Y_{02}'s coefficient are minimal, and the yields whose coefficient has opposite sign to Y_{02}'s are maximal. Recalling constraint (2.3), this means setting Y_{01} and Y_{0m} to zero and Y_{nm} with $n \geqslant 2$ and $m \geqslant 1$, to 1 in (2.8). In so doing, after rearranging the terms we obtain:

$$Y_{02}^U = \frac{2}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}\left[-G_{02} + \left(\sum_{m=1}^{\infty} \frac{\mu_0^m}{m!} - \frac{\mu_1^m}{m!}\right)\left(\sum_{n=2}^{\infty} \mu_1 \frac{\mu_0^n}{n!} - \mu_0 \frac{\mu_1^n}{n!}\right)\right], \tag{2.9}$$

which leads to the following upper bound on Y_{02}:

$$Y_{02}^U = \frac{2(\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_1})(\mu_0 - \mu_1 + \mu_1 \mathrm{e}^{\mu_0} - \mu_0 \mathrm{e}^{\mu_1}) - 2G_{02}}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}. \tag{2.10}$$

2.3. Upper bound on Y_{20}

Consider the following combination of gains:

$$G_{20} = \mu_1 \tilde{Q}^{0,0} + \mu_0 \tilde{Q}^{1,1} - \mu_0 \tilde{Q}^{0,1} - \mu_1 \tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_1 \mu_0^m - \mu_0 \mu_1^m). \tag{2.11}$$

In (2.11) the coefficients of the yields Y_{n1} and Y_{0m} are identically zero. Thus (2.11) can be rewritten as:

$$\begin{aligned} G_{20} = & -Y_{10}(\mu_0 - \mu_1)^2 - \frac{Y_{20}}{2}(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2 - \sum_{n=3}^{\infty} \frac{Y_{n0}}{n!}(\mu_0 - \mu_1)(\mu_0^n - \mu_1^n) \\ & + \sum_{\substack{n=1 \\ m=2}}^{\infty} \frac{Y_{nm}}{n!m!} \mu_0 \mu_1 (\mu_0^n - \mu_1^n)(\mu_0^{m-1} - \mu_1^{m-1}). \end{aligned} \tag{2.12}$$

A valid upper bound for Y_{20} is obtained by setting to zero the yields whose coefficient has the same sign as Y_{20}'s coefficient, and by setting to 1 the yields whose coefficient has opposite sign to Y_{20}'s. In the case of (2.12) this means setting Y_{10} and Y_{n0} to zero and Y_{nm} with $n \geqslant 1$ and $m \geqslant 2$, to 1. In this way we obtain:

$$Y_{20}^U = \frac{2}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}\left[-G_{20} + \left(\sum_{n=1}^{\infty} \frac{\mu_0^n}{n!} - \frac{\mu_1^n}{n!}\right)\left(\sum_{m=2}^{\infty} \mu_1 \frac{\mu_0^m}{m!} - \mu_0 \frac{\mu_1^m}{m!}\right)\right], \tag{2.13}$$

which leads to the following upper bound on Y_{20}:

$$Y_{20}^U = \frac{2(\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_1})(\mu_0 - \mu_1 + \mu_1 \mathrm{e}^{\mu_0} - \mu_0 \mathrm{e}^{\mu_1}) - 2G_{20}}{(\mu_0 + \mu_1)(\mu_0 - \mu_1)^2}. \tag{2.14}$$

2.4. Upper bound on Y_{00}

Consider the following combination of gains:

$$G_{00} = \mu_1^2 \tilde{Q}^{0,0} + \mu_0^2 \tilde{Q}^{1,1} - \mu_0 \mu_1 (\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n \mu_1 - \mu_0 \mu_1^n)(\mu_0^m \mu_1 - \mu_0 \mu_1^m). \tag{2.15}$$

In (2.15) the coefficients of the yields Y_{1m} and Y_{n1}, for any n and m, are identically zero. Thus (2.15) can be rewritten as:

$$\begin{aligned} G_{00} = & \, Y_{00}(\mu_0 - \mu_1)^2 - \mu_0 \mu_1 (\mu_0 - \mu_1)\left[\sum_{m=2}^{\infty} \frac{Y_{0m}}{m!}(\mu_0^{m-1} - \mu_1^{m-1}) + \sum_{n=2}^{\infty} \frac{Y_{n0}}{n!}(\mu_0^{n-1} - \mu_1^{n-1})\right] \\ & + \mu_0^2 \mu_1^2 \sum_{n,m=2}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^{m-1} - \mu_1^{m-1}). \end{aligned} \tag{2.16}$$

As usual we extract an upper bound on Y_{00} by setting to their lowest value the yields whose coefficient has the same sign as Y_{00}'s coefficient (which correspond to the Y_{nm} with $n,\ m \geqslant 2$), and by setting to their maximum value the yields whose coefficient has opposite sign to Y_{00}'s coefficient (which correspond to Y_{0m} and Y_{n0}). We know that every yield is trivially bounded by (2.3). However, in order to derive a tighter bound on Y_{00}, we employ non-trivial bounds for all the yields Y_{nm} with $n + m \leqslant 4$ in (2.16). The upper bound on Y_{00} thus satisfies:

$$\begin{aligned} G_{00} = & \, Y_{00}^U (\mu_0 - \mu_1)^2 - \mu_0 \mu_1 (\mu_0 - \mu_1)\left[\frac{(\mu_0 - \mu_1)}{2}(Y_{02}^U + Y_{20}^U) + \frac{(\mu_0^2 - \mu_1^2)}{6}(Y_{03}^U + Y_{30}^U) \right. \\ & \left. + \frac{(\mu_0^3 - \mu_1^3)}{24}(Y_{04}^U + Y_{40}^U) + 2\sum_{n=5}^{\infty} \frac{(\mu_0^{n-1} - \mu_1^{n-1})}{n!}\right] + \frac{\mu_0^2 \mu_1^2 (\mu_0 - \mu_1)^2}{4} Y_{22}^L. \end{aligned} \tag{2.17}$$

In this equation Y_{ij}^U are upper bounds and Y_{ij}^L are lower bounds. From (2.17) we obtain the following upper bound on Y_{00}:

$$\begin{aligned} Y_{00}^U = & \frac{G_{00}}{(\mu_0 - \mu_1)^2} + \frac{\mu_0 \mu_1}{\mu_0 - \mu_1}\left[\frac{(\mu_0 - \mu_1)}{2}(Y_{02}^U + Y_{20}^U) + \frac{(\mu_0^2 - \mu_1^2)}{6}(Y_{03}^U + Y_{30}^U) + \frac{(\mu_0^3 - \mu_1^3)}{24}(Y_{04}^U + Y_{40}^U)\right] \\ & + \frac{2}{\mu_0 - \mu_1}\left[\mu_1\left(\mathrm{e}^{\mu_0} - 1 - \frac{\mu_0^2}{2} - \frac{\mu_0^3}{6} - \frac{\mu_0^4}{24}\right) - \mu_0\left(\mathrm{e}^{\mu_1} - 1 - \frac{\mu_1^2}{2} - \frac{\mu_1^3}{6} - \frac{\mu_1^4}{24}\right)\right] - \frac{\mu_0^2 \mu_1^2}{4} Y_{22}^L, \end{aligned} \tag{2.18}$$

where Y_{02}^U and Y_{20}^U are given in (2.10) and (2.14), respectively. The expressions for Y_{03}^U and Y_{04}^U in (2.18) can be found by starting from the same expression (2.8) that we used to derive Y_{02}^U, i.e.:

$$G_{02} = -\sum_{m=1}^{\infty} \frac{Y_{0m}}{m!}(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m) + \sum_{\substack{n=2\\m=1}}^{\infty} \frac{Y_{nm}}{n!m!}\mu_0\mu_1(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m - \mu_1^m). \tag{2.19}$$

From this expression we can extract an upper bound on any generic Y_{0m} as follows:

$$Y_{0m}^U = \min\left\{\frac{m!}{(\mu_0 - \mu_1)(\mu_0^m - \mu_1^m)}[-G_{02} + (e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1})],\ 1\right\}, \tag{2.20}$$

where we employ the constraint (2.3). Similarly, the expressions for Y_{30}^U and Y_{40}^U are obtained starting from (2.12) and deriving an upper bound on a generic Y_{n0} as follows:

$$Y_{n0}^U = \min\left\{\frac{n!}{(\mu_0 - \mu_1)(\mu_0^n - \mu_1^n)}[-G_{20} + (e^{\mu_0} - e^{\mu_1})(\mu_0 - \mu_1 + \mu_1 e^{\mu_0} - \mu_0 e^{\mu_1})],\ 1\right\}. \tag{2.21}$$

At last, the expression for Y_{22}^L can be derived from the same combination of yields which led to Y_{11}^U. In particular, from (2.5) we have that:

$$G_{11} = \sum_{n,m=1}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m).$$

Then, by setting to 1 all the yields whose coefficient has equal sign to Y_{22}'s we obtain:

$$G_{11} = \sum_{n,m=1}^{\infty} \frac{\mu_0^n - \mu_1^n}{n!}\frac{\mu_0^m - \mu_1^m}{m!} - \frac{(\mu_0^2 - \mu_1^2)^2}{4} + \frac{(\mu_0^2 - \mu_1^2)^2}{4}Y_{22}^L, \tag{2.22}$$

which yields:

$$Y_{22}^L = \max\left\{\frac{4}{(\mu_0 - \mu_1)^2(\mu_0 + \mu_1)^2}[G_{11} - (e^{\mu_0} - e^{\mu_1})^2] + 1,\ 0\right\}. \tag{2.23}$$

Note that the upper bounds derived on Y_{04} and Y_{40} in this section could be used to improve the estimation of the phase error rate given by (1.8). However, the resulting improvement in the secret key rate would be extremely small in this case and we neglect it for simplicity.

3. Simulations

In this section we provide plots of the secret key rate given by (1.2) against the overall loss ($-10\log_{10}\eta$) measured in dB of the two optical channels linking Alice and Bob to node C. The channel model we use to simulate the quantities that would be observed experimentally—i.e. the gains $p(k_c, k_d|b_A, b_B)$ and $Q_{k_c,k_d}^{\beta_A^2,\beta_B^2}$—is given in appendix A [33]. It accounts for: the loss in the optical channels together with the non-unity detection efficiency of D_c and D_d (altogether described by the parameter η), the polarization and phase misalignments introduced by the channel and a dark count probability p_d in each detector. For concreteness, in all the plots below we assume fixed polarization and phase misalignments of 2%, independently of the channel loss. Note that, as pointed out in [33], the TF-QKD protocol analyzed in this work is quite robust against phase mismatch. This is so because phase misalignment only affects the quantum bit error rate but not the phase error rate.

For illustration purposes every plot is obtained for three different values of the dark count rate of the detectors, $p_d \in \{10^{-6}, 10^{-7}, 10^{-8}\}$. The plots are obtained by numerically optimizing[5] the secret key rate—for every value of the loss—over the signal intensity (α^2) and over one decoy intensity, while for simplicity the other decoy intensities are fixed to near-to-optimal values for all values of the overall loss. More specifically, we preliminarily performed an optimization of the key rate over the whole set of intensity settings and noticed that most of the decoy intensities are roughly constant with the loss and tend to be as low as possible. For instance, if we consider the case with two decoy intensity settings (μ_0 and μ_1, with $\mu_0 > \mu_1$), we observe that the optimal value for the weakest decoy μ_1 is basically the lowest possible for any value of the loss. In practice, however, it might be difficult to generate very weak signals due to the finite extinction ratio of a practical intensity modulator [44], so we fix μ_1 to a reasonable small value from an experimental point of view, say $\mu_1 = 10^{-5}$ [34, 36], while keeping the optimization over the remaining intensities. Similarly, if we consider the case with three decoy intensity settings (μ_0, μ_1 and μ_2, with $\mu_0 > \mu_1 > \mu_2$), we find that the optimal values for the weakest decoys μ_1 and μ_2 are also the lowest possible for any value of the loss. Moreover, in this last case, we show in appendix B that the system performance remains basically unchanged if one increases the value of the weakest intensity to say $\mu_2 = 10^{-3}$, which might be even easier to implement experimentally than 10^{-5}. Thus, we fix $\mu_2 = 10^{-3}$ and we differentiate it from μ_1 by, for example, one order of magnitude (i.e. we take $\mu_1 = 10^{-2}$). The same argument

[5] The optimization is carried out by using the built-in function 'NMaximize' of the software Wolfram Mathematica 10.0.

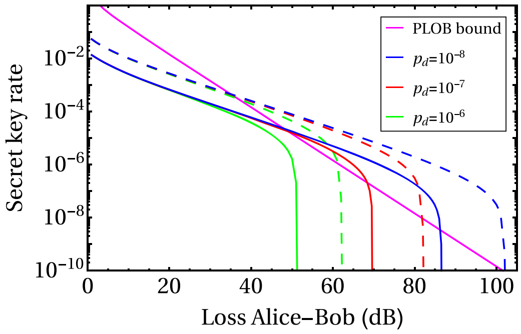

Figure 2. Secret key rate in logarithmic scale as a function of the overall loss in the channels Alice-C and Bob-C for three different dark count rates (10^{-6} green, 10^{-7} red, 10^{-8} blue). The solid lines correspond to the case where the yields Y_{00}, Y_{02}, Y_{20} and Y_{11} are estimated by means of two decoy intensity settings through the bounds presented in section 2 and the key rate is optimized over the signal intensity α^2 (see figure 3(a)) and the decoy intensity μ_0 (see figure 3(b)). The other decoy intensity, μ_1, is fixed to $\mu_1 = 10^{-5}$. The dashed lines assume that all the yields are known from the channel model and the secret key rate is optimized over α^2. That is, these lines show the maximum value of the secret key rate which could be achieved with an infinite number of decoy intensity settings and the security analysis reported in [33]. The solid magenta line illustrates the PLOB bound [19]. The plot shows that in the presence of a dark count rate of at most about $p_d = 10^{-7}$ the protocol can beat the PLOB bound even with just two decoy intensity settings.

holds in the case with four decoy intensity settings (see appendix B), where we fix $\mu_2 = 10^{-3}$, $\mu_1 = 10^{-2}$, and $\mu_0 = 10^{-1}$. We remark, however, that our method is general in the sense that the analytical upper bounds on the yields can be evaluated with any desired combination of intensity settings, while we select these particular decoy intensity values only for illustration purposes. Also, let us emphasize that the optimal decoy intensity values in the finite-key regime might be different from the values mentioned above. The analysis of the finite-key regime is, however, beyond the scope of this paper. Importantly, it turns out that the resulting asymptotic secret key rates in these scenarios are almost indistinguishable from those obtained by optimizing the value of all the intensity settings.

The optimal values of the signal and decoy intensities which are optimized as a function of the loss are also plotted in this section. In this regard, we also study how the key rate is affected when the intensities are subjected to fluctuations around their optimal values in section 3.4.

3.1. Two decoy intensity settings

In figure 2 we plot the secret key rate against the overall loss for the case where Alice and Bob use two decoy intensity settings each. The solid lines are obtained by bounding from above the yields Y_{00}, Y_{02}, Y_{20} and Y_{11} by means of the expressions derived in section 2 and by optimizing the rate over the signal intensity α^2 and the decoy intensity μ_0, while the other decoy intensity is fixed to $\mu_1 = 10^{-5}$ as explained above. The optimal values for α^2 and μ_0 are shown in figures 3(a) and (b), respectively. The dashed lines are instead obtained by employing the exact expression of the yields[6] which is given by (A.6) for the channel model considered. This represents the ideal scenario in which the parties have an infinite number of decoys through which they can estimate all the yields precisely. Note that in order to obtain the dashed lines in figure 2 we use the exact expression of the yields Y_{nm} only for $n,\ m \leqslant 12$ while we set the other yields to 1. This is enough to basically reproduce the behavior of the secret key rate when all the infinite number of yields are computed via the channel model's formula given by (A.6), as argued in [33]. The dashed lines are only optimized over the signal intensity, since the yields are directly given by the channel model. Finally, we also insert in figure 2 the PLOB bound on the secret key capacity [19], which reads as follows in terms of the transmittance η:

$$K(\eta) = -\log_2(1 - \eta). \tag{3.1}$$

In figure 2 we observe that even by means of just two decoy intensity settings the key rate can beat the PLOB bound, provided that the dark count rate is $p_d \lesssim 10^{-7}$. This happens because with two decoys the parties can already non-trivially estimate the yields Y_{nm} with $n + m \leqslant 2$ as we showed in section 2, and these yields are the most relevant terms in the phase-error rate formula given by (1.7) [33]. Note that we did not estimate the yields Y_{01} and Y_{10} since only the yields Y_{nm} with $n + m$ an even number contribute to the phase-error rate (1.7).

However, figure 2 also shows that there is a sensible gap between the rates where the yields are estimated with two decoys (solid lines) and the best possible rates one could achieve (dashed lines) if all the yields were known. This clearly indicates that, although two decoys allow to estimate the yields of largest contribution in the phase-error rate, such estimations are not sufficiently tight and the ability to estimate a larger number of yields would increase the performance of the protocol.

[6] By 'exact expression' we mean that if the experimental apparatus were accurately described by the channel model in appendix A, then the yields associated to that experimental setup would be precisely predicted by (A.6).

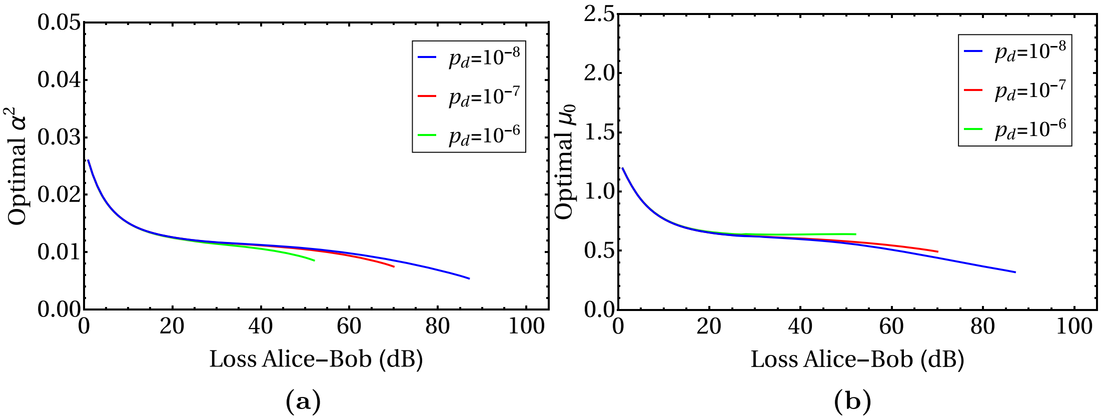

Figure 3. Optimal values of the signal and decoy intensities α^2 and μ_0 for the TF-QKD protocol [33] when the parties have at their disposal two decoy intensity settings to estimate the yields. (a) Optimal values of the signal intensity α^2 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 2. (b) Optimal values of the decoy intensity μ_0 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 2. The other decoy intensity is set to: $\mu_1 = 10^{-5}$.

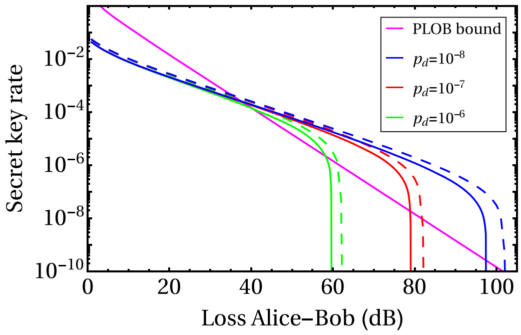

Figure 4. Secret key rate in logarithmic scale as a function of the overall loss in the channels Alice-C and Bob-C for three different dark count rates (10^{-6} green, 10^{-7} red, 10^{-8} blue). The solid lines correspond to the case where the yields Y_{00}, Y_{02}, Y_{20}, Y_{11}, Y_{13}, Y_{31}, Y_{04}, Y_{40} and Y_{22} are estimated by means of three decoy intensity settings through the bounds presented in appendix C and the key rate is optimized over the signal intensity α^2 (see figure 5(a)) and the decoy intensity μ_0 (see figure 5(b)). The other decoy intensities are fixed to $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. The dashed lines assume that all the yields are known from the channel model and the secret key rate is optimized over α^2. That is, these lines show the maximum value of the secret key rate which could be achieved with an infinite number of decoy intensity settings and the security analysis reported in [33]. The solid magenta line illustrates the PLOB bound [19]. The plot shows that already with three decoy intensity settings the key rate (solid lines) is sensibly close to the ideal one in which all the yields are known (dashed lines), meaning that the contribution of the other yields trivially bounded by 1 in the phase error rate is minimal.

By considering figure 3 and the fixed value of the decoy intensity μ_1, one notices that the optimal intensities are rather small and thus, in a real experimental implementation, intensity fluctuations might be an issue. In section 3.4 we address this problem by studying how the key rate is affected under intensity fluctuations and show that for fluctuations up to about 40% the change in the key rate performance is minimal.

Also, we notice that the optimal values of the signal intensity α^2 (see figure 3(a)) and the decoy intensity μ_0 (see figure 3(b)) are almost constant with the loss, for losses $\gtrsim$20 dB. This means that in a scenario where the loss in the quantum channels varies dynamically with time within a reasonable interval, one could still fix the signal intensity and both decoy intensities to constant values which happen to be close to the optimal ones. This argument also holds in the case of three (see section 3.2) and four decoy intensity settings (see section 3.3).

3.2. Three decoy intensity settings

In figure 4 we plot the secret key rate against the overall loss for the case where Alice and Bob use three decoy intensity settings each. The solid lines are obtained by bounding from above the relevant yields Y_{nm} such that $n + m \leqslant 4$ (i.e. we upper bound the yields Y_{00}, Y_{02}, Y_{20}, Y_{11}, Y_{13}, Y_{31}, Y_{04}, Y_{40} and Y_{22}). The exact expressions for the different upper bounds on the yields can be found in appendix C, and we omit them here for simplicity. The solid lines are optimized over the signal intensity α^2 and the decoy intensity μ_0, while the weakest decoy intensities are fixed for simplicity to $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. As explained above, the resulting secret key rate in this scenario is almost

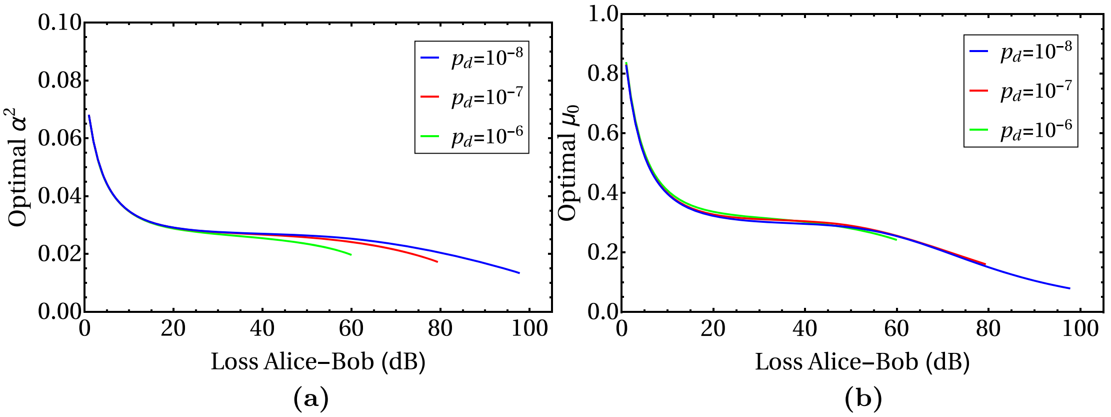

Figure 5. Optimal values of the signal and decoy intensities α^2 and μ_0 for the TF-QKD protocol [33] when the parties have at their disposal three decoy intensity settings to estimate the yields. (a) Optimal values of the signal intensity α^2 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 4. We observe that the optimal signal intensity is roughly doubled with respect to the two-decoys case (figure 3(a)). (b) Optimal values of the decoy intensity μ_0 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 4. The other decoy intensities are set to: $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$.

indistinguishable from that obtained by optimizing over all the intensity settings. The optimal values for α^2 and μ_0 are shown in figures 5(a) and (b), respectively. The dashed lines are again obtained by employing the exact expression of the yields given by the channel model (A.6) and coincide with those plotted in figure 2.

We observe in figure 4 that the use of three decoys yields a significant improvement in the protocol's performance with respect to the two-decoys case (see figure 2). As a matter of fact, in figure 4 the solid lines are almost overlapping the dashed lines for most values of the channel loss. This is due to the fact that with three decoys the parties constrain the yields with nine independent equations (instead of four equations as in the two-decoys case), which enable a tighter estimation of $Y_{00},\ Y_{02},\ Y_{20}$ and Y_{11} and the non-trivial estimation of five additional yields.

Moreover, in the case of three decoys the optimal signal intensity α^2 (see figure 5(a)) is roughly double the value of the correspondent intensity when using two decoys (see figure 3(a)). The reason for this is connected to the role of α^2 in the protocol's key rate. In fact, the prefactor $p(k_c, k_d)$ with $k_c + k_d = 1$ of the key rate formula given by (1.3) increases for increasing α^2: the higher the mean number of photons sent by the parties (within certain limits) the higher the probability of having a click in one of the two detectors. On the other hand, increasing α^2 excessively also affects the phase-error rate. Note that by setting some yields to 1 in the phase error rate formula given by (1.7) we give rise to addends like $c_{2n}\,c_{2m}$ and $c_{2n+1}c_{2m+1}$ which increase for increasing α^2, leading to an overall increase of the phase-error rate and thus decrease of the key rate. The optimal value of α^2 is thus given by the trade-off between the effect of the prefactor $p(k_c, k_d)$ and that of the terms $c_{2n}\,c_{2m}$ and $c_{2n+1}c_{2m+1}$. Now, by noting that the contribution of the therms $c_{2n}\,c_{2m}$ and $c_{2n+1}c_{2m+1}$ decreases for increasing n, m, we understand that their negative effect on the key rate is diminished in the case of three decoys since we non-trivially estimate more yields, i.e. a lower number of yields is set to 1. This allows α^2 to acquire higher values with respect to the two-decoys case, as we observed in figure 5(a).

Finally we point out that such an argument does not apply to the discussion about the optimal value of the decoy intensity μ_0 in the case of two and three decoys. As a matter of fact, the key rate does not depend on the decoy intensities in the same way as on the signal intensity: the decoy intensities only appear in the yield's bounds inserted in the phase-error rate. Additionally, the analytical bounds on the yields when using two or three decoys cannot be compared in a straightforward way. Nonetheless we observe a similar behavior of the optimal μ_0 for two (see figure 3(b)) and three decoys (see figure 5(b)).

3.3. Four decoy intensity settings

In figure 6 we plot the secret key rate against the overall loss for the case where Alice and Bob use four decoy intensity settings each. Like in the three-decoys case, the solid lines are obtained by bounding from above the yields Y_{00}, Y_{02}, Y_{20}, Y_{11}, Y_{13}, Y_{31}, Y_{04}, Y_{40} and Y_{22} by means of four decoys. In particular, for the yields Y_{00}, Y_{02}, Y_{20}, Y_{11} and Y_{22} we use the exact same analytical bounds derived with three decoys since they are tight enough, and the use of a fourth decoy intensity would just make them more cumbersome without providing a significant improvement of the resulting secret key rate. For the remaining four yields we instead derived tighter bounds with the help of the fourth intensity μ_3 (see appendix D). The solid lines are obtained by optimizing the rate over the signal intensity α^2 and the fourth decoy intensity μ_3. It turns out that the optimal values for the other decoy intensities are basically the lowest possible

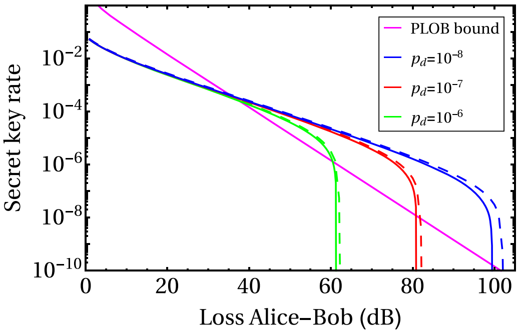

Figure 6. Secret key rate in logarithmic scale as a function of the overall loss in the channels Alice-*C* and Bob-*C* for three different dark count rates (10^{-6} green, 10^{-7} red, 10^{-8} blue). The solid lines correspond to the case where the yields Y_{00}, Y_{02}, Y_{20}, Y_{11} and Y_{22} are estimated by means of three decoys through the bounds presented in appendix C (i.e. for simplicity here we disregard the information provided by the additional fourth decoy intensity setting) and Y_{13}, Y_{31}, Y_{04} and Y_{40} are estimated with four decoys via the bounds in appendix D. The key rate is optimized over the signal intensity α^2 (see figure 7(a)) and the decoy intensity μ_3 (see figure 7(b)), while the other decoy intensities are fixed to $\mu_0 = 10^{-1}$, $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. The dashed lines are optimized over α^2 and assume that all the yields are known from the channel model. They correspond to the maximum value of the secret key rate which could be achieved with an infinite number of decoy intensity settings. The solid magenta line illustrates the PLOB bound [19]. The plot indicates that the tighter estimation of the yields Y_{13}, Y_{31}, Y_{04} and Y_{40} with respect to the case of three decoy intensity settings is enough to basically reproduce the ideal scenario in which all the yields are known (dashed lines).

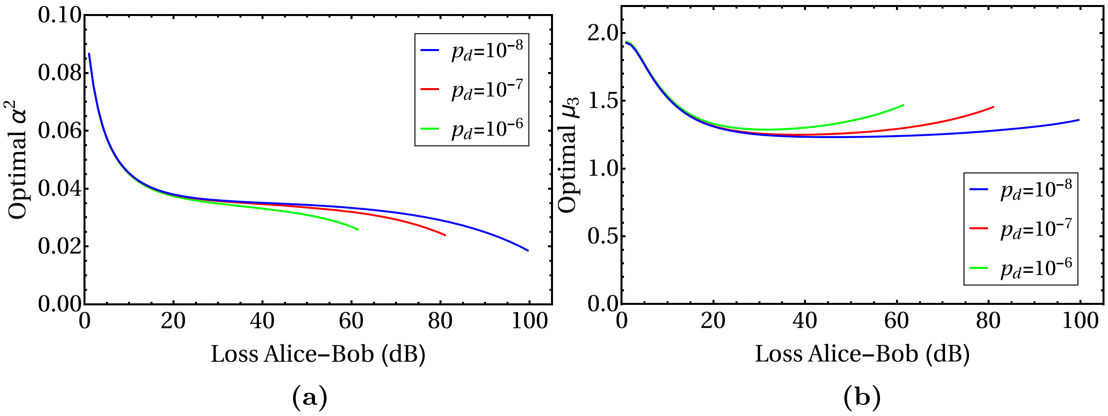

Figure 7. Optimal values of the signal and decoy intensities α^2 and μ_3 for the TF-QKD protocol [33] when the parties have at their disposal four decoy intensity settings to estimate the yields. (a) Optimal values of the signal intensity α^2 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 6. (b) Optimal values of the decoy intensity μ_3 as a function of the loss between Alice and Bob for three different dark count rates. These values are obtained from the optimization of the secret key rate (solid lines) of figure 6. The other decoy intensities are set to: $\mu_0 = 10^{-1}$, $\mu_1 = 10^{-2}$ and $\mu_2 = 10^{-3}$. The difference between this plot and the optimal μ_0 plots (see figures 3(b) and 5(b)) in the case of two and three decoys is due to the fact that, unlike μ_0, the intensity μ_3 does not appear in all the yield's bounds since we used the fourth decoy just for bounding Y_{13}, Y_{31}, Y_{04} and Y_{40}.

for any value of the loss, so, as explained above, for simplicity we fix the smallest one to an experimentally reasonable small value (say $\mu_2 = 10^{-3}$), and then we differentiate it from the other two decoys, μ_1 and μ_0, by one order of magnitude, i.e. we take $\mu_1 = 10^{-2}$ and $\mu_0 = 10^{-1}$. Importantly, this decision has a neglectable effect on the resulting secret key rate, when compared to that obtained by optimizing over all intensity settings. The optimal values for α^2 and μ_3 are shown in figures 7(a) and (b), respectively. The dashed lines are the same as in figures 2 and 4.

With four decoys (see figure 6) the key rates basically reproduces the ideal ones (dashed lines) in which all the yields are known, with the gap being at maximum of 1 dB at the very end of the plot lines (i.e. in the very high loss regime). This demonstrates that there is no need to bound further yields than the nine yields we bounded in the cases of three and four decoys. Of course, the tighter estimation of the yields Y_{13}, Y_{31}, Y_{04} and Y_{40} achieved with four decoys results in an improvement of the key rate with respect to the case of three decoys (see figure 4), especially in the region of high losses.

Concerning the optimal signal intensity (see figure 7(a)), we notice a slight increase with respect to the three-decoys case (see figure 5(a)) due to the tighter estimation of some yields in the phase-error rate formula, which allows their correspondent coefficients to acquire a slightly higher value under an increase of α^2.

Finally, the reason why the optimal μ_3 plot (see figure 7(b)) looks quite different (with values above 1) from the optimal μ_0 plots for the cases of two and three decoys (see figures 3(b) and 5(b)) is the following. In the TF-QKD protocol considered, the most important yields (i.e. those with a bigger impact on the resulting phase error

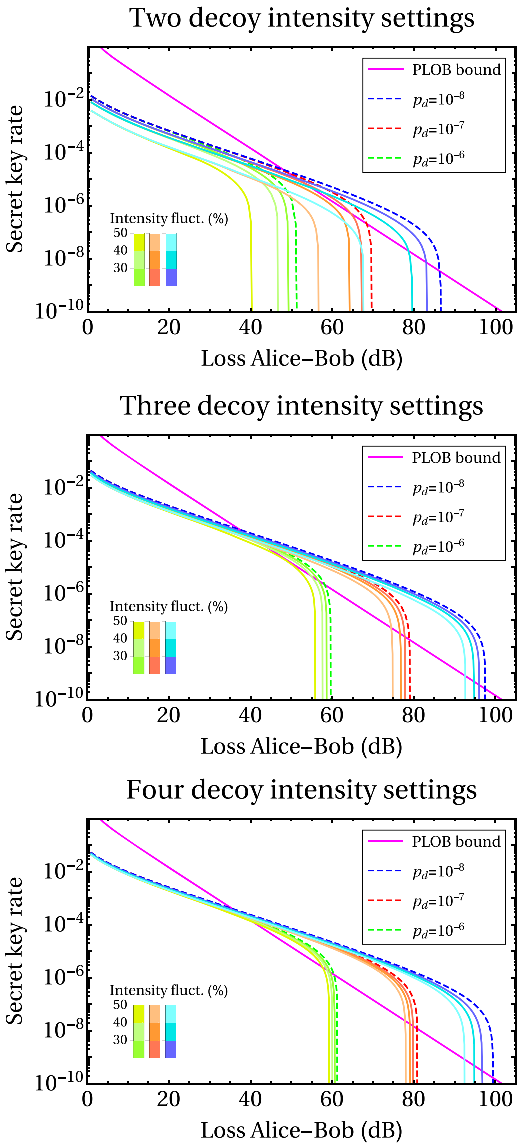

Figure 8. Comparison of the secret key rate with optimal signal and decoys intensities (dashed lines, computed in section 3) with the secret key rates affected by increasing intensity fluctuations (solid lines): 30%, 40% and 50% (brighter colors; right to left). We assume that the fluctuations affect each decoy intensity and the signal intensity as well. The plots show that the TF-QKD protocol is quite robust against intensity fluctuations, and that its robustness increases with the number of decoys.

rate) are those associated to pairs of pulses with zero or with a very low number of photons. It is therefore very important to be able to estimate these yields as tightly as possible. For this, we have that the optimal intensities μ_0 and μ_1 (μ_0, μ_1 and μ_2) for the case with two (three) decoys are well below 1, just like in standard decoy-state QKD protocols [39, 40]. However, as explained above, here we use the intensity μ_3 to improve the upper bounds for the yields Y_{13}, Y_{31}, Y_{04} and Y_{40}. That is, the intensity μ_3 is only used to estimate yields associated to pairs of pulses with a total number of photons equal to four. Thus, it is natural that the optimal value of μ_3 is not too low and greater than 1.

3.4. Intensity fluctuations

Here we investigate the robustness of the TF-QKD protocol against intensity fluctuations that may occur in the preparation of the pulses sent by Alice and Bob. This is motivated by the fact that the optimal signal and decoy intensities that the parties should adopt in order to maximize the key rate for a given loss are quite small, thus the effect of intensity fluctuations might be an issue in practice. On the other hand, we also note that the optimal value of a given decoy or signal intensity is either constant or varies very moderately with the loss.

Here we consider the simple scenario in which the intensity fluctuations are symmetric, i.e. we assume that the intensity of Alice's signal matches perfectly with the intensity of Bob's signal. Or, to put it in other words, we consider that Alice's and Bob's signals suffer from the same intensity fluctuations and thus their intensities are equal. This means that such analysis is only valid to evaluate auto-compensating TF-QKD set-ups like, for instance, the one introduced in [36]. It cannot be used however to analyze set-ups where more than one laser source is used [34, 35]. Although we do not expect a dramatic change of our results when asymmetric intensity fluctuations are considered in the latter case, specially if they are not too large.

Also, we assume that the signal and all the decoy intensities suffer from a fluctuation of magnitude 30%, 40% or 50% around their optimal value. This means for example that, for a fluctuation say of 30%, the signal intensity α^2 and all the decoy intensities μ_k fluctuate in the intervals: $0.7\ \alpha_{\rm opt}^2 \leqslant \alpha^2 \leqslant 1.3\ \alpha_{\rm opt}^2$ and $0.7\ \mu_k^{\rm opt} \leqslant \mu_k \leqslant 1.3\ \mu_k^{\rm opt}$, respectively, where $\alpha_{\rm opt}^2$ and $\mu_k^{\rm opt}$ represent the optimal values. We then account for the worst-case scenario by numerically minimizing the key rate over all the intensities constrained in their respective fluctuation interval. Only in this way we can still guarantee that the resulting key rate is associated to a secure protocol.

The results of this study are given in figure 8. Here we plot the original key rates—i.e. without fluctuations of the signal and decoy intensities—as dashed lines[7] and the key rates affected by intensity fluctuations as solid lines. The plots are given for the same dark count rates and misalignments used in section 3, in the case of two, three and four decoy intensity settings. The color of the solid lines becomes brighter for increasing fluctuation magnitude.

We observe that the performance of the protocol is considerably affected by intensity fluctuations in the case of two decoys, while the effect becomes almost negligible for three and four decoys. The reason for this lies in the fact that the tightness of the yield's bounds has a stronger dependence on the value of the decoy intensities when the number of decoys—and thus constraints on the yields—is low. In other words, if the parties have at their disposal a larger number of decoys, they can properly combine the numerous constraints on the yields and obtain inherently tight bounds, i.e. bounds that are tight regardless of the actual values of the intensities involved. If, instead, the parties have few decoys, say two, then the bounds they derive on the yields can be tight or loose depending on the values assigned to the decoy intensities, since the constraints on the yields are fewer.

In conclusion, in the case of two decoys the parties can tolerate intensity fluctuations up to 40%, which correspond to a decrease in the protocol's key rate especially in the high-loss region, quantified by a reduction of about 5–6 dB of the maximum tolerated loss[8]. Remarkably, with three decoys the decrease of the maximum tolerated loss would be under 5 dB for fluctuations up to 50%. Finally, for four decoys the protocol's performance remains almost the same for fluctuations up to about 50% around the optimal values (except when the dark count probability is the smallest considered: $p_d = 10^{-8}$). We deduce that the TF-QKD protocol introduced in [33] seems to be quite robust against intensity fluctuations.

4. Conclusions

In this paper we have investigated in detail the performance of the TF-QKD protocol presented in [33] in the realistic scenario of a finite number of decoy intensity settings at the parties' disposal. Indeed, the protocol requires that Alice and Bob use the decoy-state method [38–40] to estimate the phase-error rate by upper bounding certain yields. Unlike most QKD protocols which employ such method, in this case the protocol's key rate depends-in principle-on infinitely many yields and it is essential to upper bound (rather than lower bound) their values. Clearly, the more yields the parties tightly upper bound, the better the protocol's performance is. We have introduced an analytical method to perform such estimation when Alice and Bob use two, three or four decoy intensity settings each. The yield's analytical bounds provided in this work imply a fully-analytical expression for the protocol's secret key rate, which is very convenient for performance optimization (e.g. in the finite-key scenario). Also, we remark that the secret key rates obtained with our analytical bounds basically overlap those achievable with numerical tools like linear programming for most values of the overall loss, which confirms that the analytical approach is actually quite tight.

In so doing, we have shown that the TF-QKD protocol can beat the PLOB bound [19] even with just two decoys for reasonable values of the setup parameters, which include: the loss, the dark count rate, the polarization misalignment and the phase mismatch. Furthermore the plots assuming four decoys demonstrate that one can approximately achieve the best possible performance by tightly estimating only nine yields. The optimization of the key rate over the signal and decoy intensities indicates that their optimal values are all either constant or weakly-dependent on the loss of the channel. This means that the protocol is particularly suitable for contexts where the channel loss varies in time, for instance in the scalable MDI-QKD networks conceived in [43]. Finally we have investigated the scenario where the intensities of the optical states prepared by Alice and Bob are affected by fluctuations and observed that the protocol seems to be very robust against such phenomena.

[7] The dashed lines of the key rates without fluctuations correspond to the solid lines in figures 2, 4 and 6.

[8] By 'maximum tolerated loss' we mean the loss threshold above which the protocol's key rate becomes roughly zero.

A natural continuation of this work would take into account the finite-key effects due to the finite number of pulses sent by the parties to the central relay. This could be done by combining the results presented in this paper with the finite-keys estimation techniques used in [41].

Acknowledgments

We thank Dagmar Bruß and Hermann Kampermann for helpful discussions, and an anonymous referee for very useful comments. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675662, and from the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2017-88243-R.

Appendix A. Channel model

The channel model that we employ to simulate the gains that would be observed experimentally in the X-basis (i.e. the probabilities $p(k_c, k_d|b_A, b_B)$) and Z-basis (i.e. the probabilities $Q_{k_c,k_d}^{k,l}$) is taken from [33]. In all the expressions of this section we assume $k_c + k_d = 1$.

In particular, a beam splitter of transmittance $\sqrt{\eta}$ accounts for the loss in the quantum channel linking Alice (Bob) to node C and for the non-unity detection efficiency of detectors D_c and D_d. The polarization misalignment introduced by the channel Alice-C (Bob-C) is modeled with a unitary operation mapping the polarization input modes $a_{\rm in}^\dagger$ ($b_{\rm in}^\dagger$) to the orthogonal polarization output modes $a_{\rm out}^\dagger$ and $a_{{\rm out}\perp}^\dagger$ ($b_{\rm out}^\dagger$ and $b_{{\rm out}\perp}^\dagger$) according to: $a_{\rm in}^\dagger \to \cos\theta_A a_{\rm out}^\dagger - \sin\theta_A a_{{\rm out}\perp}^\dagger$ ($b_{\rm in}^\dagger \to \cos\theta_B b_{\rm out}^\dagger - \sin\theta_B b_{{\rm out}\perp}^\dagger$), for an angle θ_A (θ_B). Moreover, the phase mismatch between Alice and Bob's signals arriving at node C is modeled by shifting the phase of Bob's signals by an angle $\phi = \delta\pi$, for a certain parameter δ. Finally the model considers that both detectors are affected by a dark count probability p_d, which is independent of the signals received and has the same value for both detectors.

With this setup, the gains in the X-basis can be written as:

$$p(k_c, k_d|b_A, b_B) = (1 - p_d)[p_d \mathrm{e}^{-2\gamma} + q(k_c, k_d|b_A, b_B)], \tag{A.1}$$

where $\gamma = \sqrt{\eta}\alpha^2$ (with α being the amplitude of the signal states) and

$$q(k_c, k_d|b_A, b_B) = \begin{cases} \mathrm{e}^{-\gamma(1-\cos\phi\cos\theta)} - \mathrm{e}^{-2\gamma} & \text{if } k_c \oplus b_A \oplus b_B = 1 \\ \mathrm{e}^{-\gamma(1+\cos\phi\cos\theta)} - \mathrm{e}^{-2\gamma} & \text{if } k_c \oplus b_A \oplus b_B = 0 \end{cases} \tag{A.2}$$

with $\theta = \theta_A - \theta_B$. Starting from (A.1), one can readily compute the probability $p(k_c, k_d)$ and the bit-error rate e_{k_c,k_d} by means of equations (1.4) and (1.5), (1.6), respectively:

$$p(k_c, k_d) = \frac{1}{2}(1 - p_d)(\mathrm{e}^{-\gamma\cos\phi\cos\theta} + \mathrm{e}^{\gamma\cos\phi\cos\theta})\mathrm{e}^{-\gamma} - (1 - p_d)^2\mathrm{e}^{-2\gamma}, \tag{A.3}$$

$$e_{k_c,k_d} = \frac{\mathrm{e}^{-\gamma\cos\phi\cos\theta} - (1 - p_d)\mathrm{e}^{-\gamma}}{\mathrm{e}^{-\gamma\cos\phi\cos\theta} + \mathrm{e}^{\gamma\cos\phi\cos\theta} - 2(1 - p_d)\mathrm{e}^{-\gamma}}. \tag{A.4}$$

The gains in the Z-basis instead read:

$$Q_{k_c,k_d}^{k,l} = (1 - p_d)[(p_d - 1)\mathrm{e}^{-\sqrt{\eta}(\mu_k+\mu_l)} + \mathrm{e}^{-\sqrt{\eta}(\mu_k+\mu_l)/2} I_0(\sqrt{\eta\mu_k\mu_l}\cos\theta)], \tag{A.5}$$

where the function $I(z) = \frac{1}{2\pi\mathrm{i}}\oint \mathrm{e}^{(z/2)(t+1/t)}t^{-1}\mathrm{d}t$ is the modified Bessel function of first kind.

In the simulations shown in section 3 we compare the key rate computed with our analytical bounds on the yields with the key rate evaluated with the exact expressions of the yields, i.e. the expressions obtained directly from the channel model. According to the above channel model, the yields read:

$$Y_{nm}^{k_c,k_d} = (1 - p_d)[(p_d - 1)(1 - \sqrt{\eta})^{n+m} + y_{nm}^{k_c,k_d}], \tag{A.6}$$

where

$$y_{nm}^{k_c,k_d} = \sum_{k=0}^{n}\binom{n}{k}\sum_{l=0}^{m}\binom{m}{l}\frac{\sqrt{\eta}^{k+l}(1 - \sqrt{\eta})^{n+m-k-l}}{2^{k+l}k!l!}\sum_{r=0}^{k}\binom{k}{r}\sum_{p=0}^{l}\binom{l}{p}\sum_{q\,=\,\max(0,r+p-l)}^{\min(k,r+p)}\binom{k}{q}$$
$$\binom{l}{r + p - q}(r + p)!(k + l - r - p)!\cos^{r+q}(\theta_A)\cos^{r+2p-q}(\theta_B)\sin^{2k-r-q}(\theta_A)\sin^{2l-r-2p+q}(\theta_B). \tag{A.7}$$

To conclude, we remark that all the quantities entering the key rate formula (1.2)—i.e. (A.3), (A.4) and the gains (A.5) indirectly through the yield's bounds—are symmetric under the swap $k_c \leftrightarrow k_d$ due to the symmetries of the channel model.

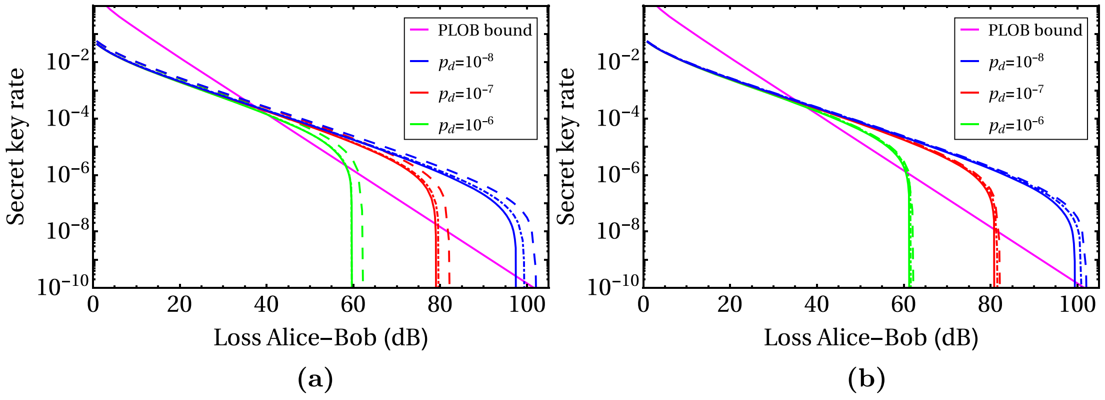

Figure B1. Comparison of the optimal key rates achievable with different fixed values of the weaker decoy intensities. The two cases analyzed (solid and dotted–dashed lines) are almost indistinguishable. (a) Optimal key rate as a function of the overall loss when the parties use three decoy intensity settings, for three different values of the dark count rate (p_d). The solid lines are obtained by fixing the weaker decoy intensities to $\mu_2 = 10^{-3}$ and $\mu_1 = 10^{-2}$, while the dotted–dashed lines are obtained by fixing the same intensities to $\mu_2 = 10^{-5}$ and $\mu_1 = 10^{-4}$. The dashed lines assume that all the yields are known from the channel model and the magenta line is the PLOB bound [19]. Note that the green dotted–dashed lines and green solid lines ($p_d = 10^{-6}$) are almost perfectly overlapping. (b) Optimal key rate as a function of the overall loss when the parties use four decoy intensity settings, for three different values of the dark count rate (p_d). The solid lines are obtained by fixing the weaker decoy intensities to $\mu_2 = 10^{-3}$, $\mu_1 = 10^{-2}$ and $\mu_0 = 10^{-1}$, while the dotted–dashed lines are obtained by fixing the same intensities to $\mu_2 = 10^{-5}$, $\mu_1 = 10^{-4}$ and $\mu_0 = 10^{-3}$. The dashed lines assume that all the yields are known from the channel model and the magenta line is the PLOB bound [19].

In all the simulations shown in section 3 we fix both polarization and phase misalignments to 2%, which means that: $\theta_A = -\theta_B = \arcsin\sqrt{0.02}$ and $\delta = 0.02$.

Appendix B. Stronger and weaker decoy intensities

As explained in section 3, the optimal key rates are basically not affected if their optimization is only performed over the signal intensity (α) and over one decoy intensity, while having the remaining weaker decoy intensities fixed to near-to-optimal values for all losses. In figure B1, we compare the optimal key rate that the parties can achieve when fixing their weaker decoy intensities to substantially different values, in the case of three (left) and four (right) decoy intensity settings. In particular, the solid lines are the same plotted in figures 4 and 6 for the three- and four-decoys case, respectively, i.e. they are obtained by fixing the weaker decoy intensities to $\mu_2 = 10^{-3}$ and $\mu_1 = 10^{-2}$ (three decoy intensity settings) and to $\mu_2 = 10^{-3}$, $\mu_1 = 10^{-2}$ and $\mu_0 = 10^{-1}$ (four decoy intensity settings). The dotted–dashed lines, instead, are obtained by fixing the weaker intensities to values which are two orders of magnitude lower, that is $\mu_2 = 10^{-5}$ and $\mu_1 = 10^{-4}$ in the case of three decoy intensity settings and $\mu_2 = 10^{-5}$, $\mu_1 = 10^{-4}$ and $\mu_0 = 10^{-3}$ in the case of four decoy intensity settings. Clearly, the optimal key rates are basically not affected by employing relatively stronger pulses (those with $\mu_2 = 10^{-3}$ as the weakest intensity) for the weaker decoy intensity settings. Such stronger pulses could be more easily implemented experimentally and, for this, have been chosen in our simulations.

Appendix C. Yield's bounds with three decoys

Here we derive analytical upper bounds on the yields appearing in (1.7), following the same lines of section 2. In this case we assume that Alice and Bob can prepare their phase-randomized coherent pulses with three different intensity settings: $\{\mu_0, \mu_1, \mu_2\}$, which are the same for both parties. This choice is optimal since we assumed that the two optical channels linking the parties to the central node C have equal transmittance $\sqrt{\eta}$ [43].

The whole set of infinite yields is subjected to the following nine equality constraints:

$$\tilde{Q}^{k,l} \equiv \mathrm{e}^{\mu_k+\mu_l} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} {\mu_k}^n {\mu_l}^m \quad k,\, l \in \{0,\, 1,\, 2\}, \tag{C.1}$$

and to the inequality constraints given by (2.3).

We derive bounds on the yields Y_{00}, Y_{11}, Y_{02}, Y_{20}, Y_{22}, Y_{13}, Y_{31}, Y_{04} and Y_{40}.

C.1. Upper bound on Y_{22}

Consider the following combinations of gains in which all the terms Y_{1m} and Y_{n1} are removed (i.e. their coefficients are equal to zero):

$$G_{22}^{0,1} = \mu_1^2 \tilde{Q}^{0,0} + \mu_0^2 \tilde{Q}^{1,1} - \mu_0\mu_1(\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m);$$

$$G_{22}^{0,2} = \mu_2^2 \tilde{Q}^{0,0} + \mu_0^2 \tilde{Q}^{2,2} - \mu_0\mu_2(\tilde{Q}^{0,2} + \tilde{Q}^{2,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m);$$

$$G_{22}^{1,2} = \mu_2^2 \tilde{Q}^{1,1} + \mu_1^2 \tilde{Q}^{2,2} - \mu_1\mu_2(\tilde{Q}^{1,2} + \tilde{Q}^{2,1}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m), \tag{C.2}$$

where the superscripts in $G_{22}^{k,l}$ indicate which intensities are involved, while the subscripts indicate the yield that is going to be bounded.

We now combine $G_{22}^{0,1}$, $G_{22}^{0,2}$ and $G_{22}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{0m} and Y_{n0} removed as well:

$$G_{22}^{0,1} + c_0\, G_{22}^{0,2} + c_1\, G_{22}^{1,2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}[(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m)$$
$$+ c_0(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)]. \tag{C.3}$$

Note that the linear combination above is already the most general for our needs. As a matter of fact, for every linear combination of $G_{22}^{0,1}$, $G_{22}^{0,2}$ and $G_{22}^{1,2}$ one can always factor out the coefficient in front of $G_{22}^{0,1}$, as far as it is not zero. However, if the particular combination of gains which removes the terms Y_{0m} and Y_{n0} has a null coefficient in front of $G_{22}^{0,1}$, for symmetry reasons there would also exist another combination—that also removes the yields Y_{0m} and Y_{n0}—with a null coefficient in front of say $G_{22}^{0,2}$, and this one could be found in our case given by (C.3).

For Y_{0m} and Y_{n0} to be removed in (C.3) it suffices that:

$$(\mu_1 - \mu_0)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + c_0(\mu_2 - \mu_0)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_2 - \mu_1)(\mu_1^m\mu_2 - \mu_1\mu_2^m) = 0 \quad \forall\ m, \tag{C.4}$$

which implies:

$$\mu_0^m[\mu_1(\mu_1 - \mu_0) + c_0\mu_2(\mu_2 - \mu_0)] + \mu_1^m[-\mu_0(\mu_1 - \mu_0) + c_1\mu_2(\mu_2 - \mu_1)]$$
$$+ \mu_2^m[-c_0\mu_0(\mu_2 - \mu_0) - c_1\mu_1(\mu_2 - \mu_1)] = 0 \quad \forall m. \tag{C.5}$$

A sufficient condition for this is that every coefficient of μ_i^m is identically zero, which happens for:

$$c_0 = -\frac{\mu_1(\mu_0 - \mu_1)}{\mu_2(\mu_0 - \mu_2)}, \tag{C.6}$$

$$c_1 = \frac{\mu_0(\mu_0 - \mu_1)}{\mu_2(\mu_1 - \mu_2)}. \tag{C.7}$$

Substituting (C.6) and (C.7) back into (C.3) and multiplying both sides by μ_2, we get an expression where all the terms Y_{0m}, Y_{1m}, Y_{n0} and Y_{n1} are removed and where the term Y_{22} gives the largest contribution:

$$\mu_2 G_{22}^{0,1} - \mu_1\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}\, G_{22}^{0,2} + \mu_0\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}\, G_{22}^{1,2} = \sum_{n,m=2}^{\infty} \frac{Y_{nm}}{n!m!}[\mu_2(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m)$$
$$\left. - \mu_1\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + \mu_0\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)\right]. \tag{C.8}$$

In order to extract a bound for Y_{22} we need to recast the yield's coefficients in such a way that their sign becomes manifest. Each term of the sum in (C.8) may be recast as follows:

$$\frac{Y_{nm}}{n!m!}\mu_0\mu_1\mu_2\left[(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^m\mu_1 - \mu_0\mu_1^m) - \frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^{n-1} - \mu_2^{n-1})(\mu_0^m\mu_2 - \mu_0\mu_2^m)\right.$$
$$\left. + \frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^{n-1} - \mu_2^{n-1})(\mu_1^m\mu_2 - \mu_1\mu_2^m)\right], \tag{C.9}$$

or equivalently as:

$$\frac{Y_{nm}}{n!m!}\frac{\mu_0\mu_1\mu_2}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)} A_{22}(\mu_0, \mu_1, \mu_2, m) \cdot A_{22}(\mu_0, \mu_1, \mu_2, n), \tag{C.10}$$

where

$$A_{22}(\mu_0, \mu_1, \mu_2, m) \equiv \mu_1^m(\mu_0 - \mu_2) + \mu_2^m(\mu_1 - \mu_0) + \mu_0^m(\mu_2 - \mu_1). \tag{C.11}$$

We can now rewrite factor A_{22} as:

$$\begin{aligned}
A_{22}(\mu_0, \mu_1, \mu_2, m) &= \mu_1[\mu_1^{m-1}(\mu_0 - \mu_2) - (\mu_0^m - \mu_2^m)] + \mu_0\mu_2(\mu_0^{m-1} - \mu_2^{m-1})\\
&= \mu_1\left[\mu_1^{m-1}(\mu_0 - \mu_2) - (\mu_0 - \mu_2)\left(\sum_{k=0}^{m-1}\mu_0^{m-1-k}\mu_2^k\right)\right] + \mu_0\mu_2(\mu_0 - \mu_2)\left(\sum_{j=0}^{m-2}\mu_0^{m-2-j}\mu_2^j\right)\\
&= (\mu_0 - \mu_2)\left[\mu_1^m - \mu_1\sum_{k=0}^{m-1}\mu_0^{m-1-k}\mu_2^k + \mu_0\mu_2\sum_{j=0}^{m-2}\mu_0^{m-2-j}\mu_2^j\right]\\
&= (\mu_0 - \mu_2)\left[\mu_1^m + \sum_{k=0}^{m-1}\mu_2^k(-\mu_1\mu_0^{m-1-k} + \mu_0\mu_2\mu_0^{m-2-k}) - \mu_0\mu_2\frac{\mu_2^{m-1}}{\mu_0}\right]\\
&= (\mu_0 - \mu_2)\left[-(\mu_2^m - \mu_1^m) + \sum_{k=0}^{m-1}\mu_2^k\mu_0^{m-1-k}(\mu_2 - \mu_1)\right]\\
&= (\mu_0 - \mu_2)(\mu_2 - \mu_1)\left[\sum_{k=0}^{m-1}\mu_2^k\mu_0^{m-1-k} - \sum_{j=0}^{m-1}\mu_2^j\mu_1^{m-1-j}\right]\\
&= (\mu_0 - \mu_2)(\mu_2 - \mu_1)\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k}).
\end{aligned} \tag{C.12}$$

Of course we can employ this expression also for $A_{22}(\mu_0, \mu_1, \mu_2, n)$, under the substitution $m \to n$. We will apply this consideration from now on to similar scenarios. By substituting (C.12) into (C.10), we get the final expression for each term of the sum in (C.8):

$$\begin{aligned}
&\frac{Y_{nm}}{n!m!}\frac{\mu_0\mu_1\mu_2}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)}(\mu_0 - \mu_2)^2(\mu_2 - \mu_1)^2\\
&\times\left[\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k})\right]\left[\sum_{j=0}^{n-1}\mu_2^j(\mu_0^{n-1-j} - \mu_1^{n-1-j})\right].
\end{aligned} \tag{C.13}$$

That is, the sign of Y_{nm}'s coefficient is independent of n and m and it is the same for all terms in (C.8) (note that the product of the two sums in (C.13) is always positive). Thus a valid upper bound for Y_{22} is obtained by setting all the other yields to zero in (C.8), except for Y_{22}. We obtain:

$$\mu_2 G_{22}^{0,1} - \mu_1\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}G_{22}^{0,2} + \mu_0\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}G_{22}^{1,2} = \frac{Y_{22}^U\mu_0\mu_1\mu_2}{4}(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)^2, \tag{C.14}$$

which implies the following expression for the upper bound on Y_{22}:

$$Y_{22}^U = 4\frac{\frac{G_{22}^{0,1}}{\mu_0\mu_1(\mu_0 - \mu_1)} - \frac{G_{22}^{0,2}}{\mu_0\mu_2(\mu_0 - \mu_2)} + \frac{G_{22}^{1,2}}{\mu_1\mu_2(\mu_1 - \mu_2)}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)}. \tag{C.15}$$

We remark that the bound given by (C.15) is not valid when any of the intensities μ_0, μ_1 or μ_2 is equal to zero. As a matter of fact, in any of these cases the starting expression given by (C.8) becomes trivial. However, in most practical situations, due to the finite extinction ratio of amplitude modulators, none of the decoy intensities is actually equal to zero.

C.2. Upper bound on Y_{11}

Consider the following combinations of gains in which all the terms Y_{0m} and Y_{n0} are removed:

$$\begin{aligned}
G_{11}^{0,1} &= \tilde{Q}^{0,0} + \tilde{Q}^{1,1} - (\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m);\\
G_{11}^{0,2} &= \tilde{Q}^{0,0} + \tilde{Q}^{2,2} - (\tilde{Q}^{0,2} + \tilde{Q}^{2,0}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_2^n)(\mu_0^m - \mu_2^m);\\
G_{11}^{1,2} &= \tilde{Q}^{1,1} + \tilde{Q}^{2,2} - (\tilde{Q}^{1,2} + \tilde{Q}^{2,1}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_1^n - \mu_2^n)(\mu_1^m - \mu_2^m).
\end{aligned} \tag{C.16}$$

We now combine $G_{11}^{0,1}$, $G_{11}^{0,2}$ and $G_{11}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{2m} and Y_{n2} also removed:

$$G_{11}^{0,1} + c_0\, G_{11}^{0,2} + c_1\, G_{11}^{1,2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}[(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m) \\ + c_0(\mu_0^n - \mu_2^n)(\mu_0^m - \mu_2^m) + c_1(\mu_1^n - \mu_2^n)(\mu_1^m - \mu_2^m)]. \tag{C.17}$$

For Y_{2m} and Y_{n2} to be removed it suffices:

$$(\mu_0^n - \mu_1^n)(\mu_0^2 - \mu_1^2) + c_0(\mu_0^n - \mu_2^n)(\mu_0^2 - \mu_2^2) + c_1(\mu_1^n - \mu_2^n)(\mu_1^2 - \mu_2^2) = 0 \quad \forall\, n, \tag{C.18}$$

which is fulfilled by:

$$c_0 = -\frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}, \tag{C.19}$$

$$c_1 = \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}. \tag{C.20}$$

Substituting these terms back into (C.17) yields a combination of gains in which the terms Y_{0m}, Y_{n0}, Y_{2m} and Y_{n2} are removed:

$$\begin{aligned}
G_{11}^{0,1} - \frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}\, G_{11}^{0,2} + \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}\, G_{11}^{1,2} &= Y_{11}(\mu_0 - \mu_1)\left[(\mu_0 - \mu_1) - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0 - \mu_2)\right. \\
&\left. + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1 - \mu_2)\right] \\
&+ \sum_{m=3}^{\infty} \frac{Y_{1m}}{m!}(\mu_0 - \mu_1)\left[(\mu_0^m - \mu_1^m) - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0^m - \mu_2^m) + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1^m - \mu_2^m)\right] \\
&+ \sum_{n=3}^{\infty} \frac{Y_{n1}}{n!}(\mu_0 - \mu_1)\left[(\mu_0^n - \mu_1^n) - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0^n - \mu_2^n) + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1^n - \mu_2^n)\right] \\
&+ \sum_{n,m=3}^{\infty} \frac{Y_{nm}}{n!m!}\left[(\mu_0^n - \mu_1^n)(\mu_0^m - \mu_1^m) - \frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}(\mu_0^n - \mu_2^n)(\mu_0^m - \mu_2^m)\right. \\
&\left. + \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}(\mu_1^n - \mu_2^n)(\mu_1^m - \mu_2^m)\right].
\end{aligned} \tag{C.21}$$

In order to get a valid upper bound for Y_{11} we need to determine the signs of the coefficients of the remaining yields. We start by recasting each term of the sum in (C.21) corresponding to the Y_{nm}, with $n,\ m \geqslant 3$, as follows:

$$\frac{Y_{nm}}{n!m!} \frac{1}{(\mu_0^2 - \mu_2^2)(\mu_1^2 - \mu_2^2)} A_{11}(\mu_0,\, \mu_1,\, \mu_2,\, m) \cdot A_{11}(\mu_0,\, \mu_1,\, \mu_2,\, n), \tag{C.22}$$

where

$$A_{11}(\mu_0,\, \mu_1,\, \mu_2,\, m) \equiv \mu_1^m(\mu_0^2 - \mu_2^2) + \mu_2^m(\mu_1^2 - \mu_0^2) + \mu_0^m(\mu_2^2 - \mu_1^2). \tag{C.23}$$

The factor A_{11} can be rewritten as:

$$\begin{aligned}
A_{11}(\mu_0,\, \mu_1,\, \mu_2,\, m) &= \mu_1^2[\mu_1^{m-2}(\mu_0^2 - \mu_2^2) - (\mu_0^m - \mu_2^m)] + \mu_0^2\mu_2^2(\mu_0^{m-2} - \mu_2^{m-2}) \\
&= (\mu_0 - \mu_2)\left[\mu_1^m(\mu_0 + \mu_2) - \mu_1^2 \sum_{k=0}^{m-1} \mu_0^{m-1-k}\mu_2^k + \mu_0^2\mu_2^2 \sum_{j=0}^{m-3} \mu_0^{m-3-j}\mu_2^j\right] \\
&= (\mu_0 - \mu_2)\left[\mu_1^m(\mu_0 + \mu_2) + \sum_{k=0}^{m-1} \mu_2^k(-\mu_1^2\mu_0^{m-1-k} + \mu_0^2\mu_2^2\mu_0^{m-3-k}) - \mu_0^2\mu_2^2\left(\frac{\mu_2^{m-2}}{\mu_0} + \frac{\mu_2^{m-1}}{\mu_0^2}\right)\right] \\
&= (\mu_0 - \mu_2)\left[(\mu_1^m - \mu_2^m)(\mu_0 + \mu_2) + \sum_{k=0}^{m-1} \mu_2^k\mu_0^{m-1-k}(\mu_2^2 - \mu_1^2)\right] \\
&= (\mu_0 - \mu_2)\left[(\mu_0 + \mu_2)(\mu_1 - \mu_2)\left(\sum_{j=0}^{m-1} \mu_1^{m-1-j}\mu_2^j\right) - (\mu_1 + \mu_2)(\mu_1 - \mu_2) \sum_{k=0}^{m-1} \mu_2^k\mu_0^{m-1-k}\right] \\
&= (\mu_0 - \mu_2)(\mu_1 - \mu_2) \sum_{k=0}^{m-1} \mu_2^k[(\mu_0 + \mu_2)\mu_1^{m-1-k} - (\mu_1 + \mu_2)\mu_0^{m-1-k}] \\
&= (\mu_0 - \mu_2)(\mu_1 - \mu_2)\left\{\sum_{k=0}^{m-3} \mu_2^k[\mu_2(\mu_1^{m-1-k} - \mu_0^{m-1-k}) + \mu_0\mu_1(\mu_1^{m-2-k} - \mu_0^{m-2-k})]\right.
\end{aligned}$$

$$
\begin{aligned}
&+ \mu_2^{m-1}(\mu_0 - \mu_1) + \mu_2^{m-1}(\mu_1 - \mu_0)\}\\
&= (\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_1 - \mu_0)\sum_{k=0}^{m-3}\mu_2^k\left[\mu_2\sum_{j=0}^{m-2-k}\mu_1^{m-2-k-j}\mu_0^j + \mu_0\mu_1\sum_{j=0}^{m-3-k}\mu_1^{m-3-k-j}\mu_0^j\right]\\
&= (\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_1 - \mu_0)\sum_{k=0}^{m-3}\mu_2^k\left[(\mu_2 + \mu_0)\sum_{j=0}^{m-3-k}\mu_1^{m-2-k-j}\mu_0^j + \mu_2\mu_0^{m-2-k}\right]\\
&\equiv (\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_1 - \mu_0)F(m),
\end{aligned} \tag{C.24}
$$

where the factor $F(m) \geqslant 0,\ \forall m \geqslant 3$. Substituting (C.24) back into (C.22), we recast each term of the sum in (C.21) corresponding to the Y_{nm}, with $n,\ m \geqslant 3$, as:

$$
\frac{Y_{nm}}{n!m!}\frac{(\mu_0 - \mu_2)^2(\mu_1 - \mu_2)^2(\mu_1 - \mu_0)^2}{(\mu_0^2 - \mu_2^2)(\mu_1^2 - \mu_2^2)}F(n)F(m), \tag{C.25}
$$

so that its sign is manifestly dependent on the factor $(\mu_0 - \mu_2)(\mu_1 - \mu_2)$.

In a similar fashion, one can rewrite each term of the sum in (C.21) corresponding to the Y_{1m}, with $m \geqslant 3$, as:

$$
-\frac{Y_{1m}}{m!}\frac{(\mu_0 - \mu_1)^2(\mu_1 - \mu_2)(\mu_0 - \mu_2)}{(\mu_0 + \mu_2)(\mu_1 + \mu_2)}F(m), \tag{C.26}
$$

thus deducing that this expression has opposite sign with respect to that given by (C.25). Same holds for Y_{n1}, since it can be shown that its coefficient is exactly (C.26) with thesubstitution $m \to n$.

Finally, by showing that the term corresponding to Y_{11} in (C.21) can be factorized as:

$$
Y_{11}\frac{(\mu_0 - \mu_1)^2(\mu_1 - \mu_2)(\mu_0 - \mu_2)}{(\mu_0 + \mu_2)(\mu_1 + \mu_2)}, \tag{C.27}
$$

one concludes that this expression has the same sign as that given by (C.25).

Putting together these considerations into (C.21), a valid upper bound on Y_{11} is obtained when the yields Y_{nm}, with $n,\ m \geqslant 3$, are set to zero and the yields Y_{1m} and Y_{n1} are set to their maximum allowed value. Since in appendices C.5 and C.6 we derive upper bounds on Y_{13} and Y_{31} (see (C.65)and (C.73)), we can employ them in (C.21) instead of trivially bounding these yields with 1. In this way we obtain:

$$
\begin{aligned}
&G_{11}^{0,1} - \frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}G_{11}^{0,2} + \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}G_{11}^{1,2} = Y_{11}^U\frac{(\mu_0 - \mu_1)^2(\mu_1 - \mu_2)(\mu_0 - \mu_2)}{(\mu_0 + \mu_2)(\mu_1 + \mu_2)}\\
&+ \frac{(\mu_0 - \mu_1)}{6}(Y_{13}^U + Y_{31}^U)\left[\mu_0^3 - \mu_1^3 - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}(\mu_0^3 - \mu_2^3) + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}(\mu_1^3 - \mu_2^3)\right]\\
&+ 2(\mu_0 - \mu_1)\sum_{n=4}^{\infty}\left[\frac{(\mu_0^n - \mu_1^n)}{n!} - \frac{(\mu_0 + \mu_1)}{(\mu_0 + \mu_2)}\frac{(\mu_0^n - \mu_2^n)}{n!} + \frac{(\mu_0 + \mu_1)}{(\mu_1 + \mu_2)}\frac{(\mu_1^n - \mu_2^n)}{n!}\right],
\end{aligned} \tag{C.28}
$$

which leads to the following upper bound on Y_{11}:

$$
\begin{aligned}
Y_{11}^U &= \frac{(\mu_0 + \mu_2)(\mu_1 + \mu_2)}{(\mu_0 - \mu_1)^2(\mu_1 - \mu_2)(\mu_0 - \mu_2)}\left[G_{11}^{0,1} - \frac{(\mu_0^2 - \mu_1^2)}{(\mu_0^2 - \mu_2^2)}G_{11}^{0,2} + \frac{(\mu_0^2 - \mu_1^2)}{(\mu_1^2 - \mu_2^2)}G_{11}^{1,2} - 2(\mu_0 - \mu_1)E_{11}\right]\\
&+ \frac{(\mu_1\mu_2 + \mu_0\mu_1 + \mu_0\mu_2)}{6}(Y_{13}^U + Y_{31}^U),
\end{aligned} \tag{C.29}
$$

where the term E_{11} is defined as:

$$
\begin{aligned}
E_{11} = {}&\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_1} - (\mu_0 - \mu_1)\left(1 + \frac{\mu_0}{2} + \frac{\mu_1}{2} + \frac{\mu_0^2}{6} + \frac{\mu_1^2}{6} + \frac{\mu_0\mu_1}{6}\right)\\
&+ \frac{\mu_0 + \mu_1}{\mu_1 + \mu_2}\left[\mathrm{e}^{\mu_1} - \mathrm{e}^{\mu_2} - (\mu_1 - \mu_2)\left(1 + \frac{\mu_1}{2} + \frac{\mu_2}{2} + \frac{\mu_1^2}{6} + \frac{\mu_2^2}{6} + \frac{\mu_1\mu_2}{6}\right)\right]\\
&- \frac{\mu_0 + \mu_1}{\mu_0 + \mu_2}\left[\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_2} - (\mu_0 - \mu_2)\left(1 + \frac{\mu_0}{2} + \frac{\mu_2}{2} + \frac{\mu_0^2}{6} + \frac{\mu_2^2}{6} + \frac{\mu_0\mu_2}{6}\right)\right].
\end{aligned} \tag{C.30}
$$

C.3. Upper bound on Y_{02} and Y_{04}

Consider the following combinations of gains in which all the terms Y_{1m} and , Y_{n0} are removed:

$$G_{02}^{0,1} = \mu_1\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{1,1} - \mu_1\tilde{Q}^{0,1} - \mu_0\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m - \mu_1^m);$$
$$G_{02}^{0,2} = \mu_2\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{2,2} - \mu_2\tilde{Q}^{0,2} - \mu_0\tilde{Q}^{2,0} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m - \mu_2^m);$$
$$G_{02}^{1,2} = \mu_2\tilde{Q}^{1,1} + \mu_1\tilde{Q}^{2,2} - \mu_2\tilde{Q}^{1,2} - \mu_1\tilde{Q}^{2,1} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m - \mu_2^m). \tag{C.31}$$

We now combine $G_{02}^{0,1}$, $G_{02}^{0,2}$ and $G_{02}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{2m} and Y_{n1} also removed:

$$G_{02}^{0,1} + c_0\,G_{02}^{0,2} + c_1\,G_{02}^{1,2} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}[(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m - \mu_1^m)$$
$$+ c_0(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m - \mu_2^m) + c_1(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m - \mu_2^m)]. \tag{C.32}$$

For Y_{2m} and Y_{n1} to be removed the coefficients c_0 and c_1 must satisfy:

$$\begin{cases}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0 - \mu_1) + c_0(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0 - \mu_2) + c_1(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1 - \mu_2) = 0\,\forall\ n\\ (\mu_0^2\mu_1 - \mu_0\mu_1^2)(\mu_0^m - \mu_1^m) + c_0(\mu_0^2\mu_2 - \mu_0\mu_2^2)(\mu_0^m - \mu_2^m) + c_1(\mu_1^2\mu_2 - \mu_1\mu_2^2)(\mu_1^m - \mu_2^m) = 0\,\forall\,m\end{cases} \tag{C.33}$$

or equivalently:

$$\begin{cases}\mu_0^n[\mu_1(\mu_0 - \mu_1) + c_0\mu_2(\mu_0 - \mu_2)] + \mu_1^n[-\mu_0(\mu_0 - \mu_1) + c_1\mu_2(\mu_1 - \mu_2)]\\ -\mu_2^n[\mu_0c_0(\mu_0 - \mu_2) + \mu_1c_1(\mu_1 - \mu_2)] = 0\,\forall\ n\\ \mu_0^m[\mu_1\mu_0^2 - \mu_0\mu_1^2 + c_0(\mu_2\mu_0^2 - \mu_0\mu_2^2)] + \mu_1^m[-(\mu_1\mu_0^2 - \mu_0\mu_1^2) + c_1(\mu_2\mu_1^2 - \mu_1\mu_2^2)]\\ -\mu_2^m[c_0(\mu_2\mu_0^2 - \mu_0\mu_2^2) + c_1(\mu_2\mu_1^2 - \mu_1\mu_2^2)] = 0\,\forall\,m.\end{cases} \tag{C.34}$$

A sufficient condition for this is that the coefficient of every μ_i^n and every μ_i^m is identically zero. This imposes six conditions on c_0 and c_1, however thanks to the inherent symmetries of the system a solution exists, and reads:

$$c_0 = -\frac{\mu_1(\mu_0 - \mu_1)}{\mu_2(\mu_0 - \mu_2)}, \tag{C.35}$$

$$c_1 = \frac{\mu_0(\mu_0 - \mu_1)}{\mu_2(\mu_1 - \mu_2)}. \tag{C.36}$$

Substituting these expressions back into (C.32) and multiplying both sides by μ_2, yields a combination of gains in which the terms Y_{n0}, Y_{n1}, Y_{1m} and Y_{2m} are removed. In particular, we obtain:

$$\mu_2 G_{02}^{0,1} - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}G_{02}^{0,2} + \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}G_{02}^{1,2}$$
$$= \sum_{m=2}^{\infty}\frac{Y_{0m}}{m!}(\mu_0 - \mu_1)[-\mu_2(\mu_0^m - \mu_1^m) + \mu_1(\mu_0^m - \mu_2^m) - \mu_0(\mu_1^m - \mu_2^m)]$$
$$+ \sum_{\substack{n=3\\m=2}}^{\infty}\frac{Y_{nm}}{n!m!}\left[\mu_2(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\mu_0^m - \mu_1^m) - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^n\mu_2 - \mu_0\mu_2^n)(\mu_0^m - \mu_2^m)\right.$$
$$\left.+ \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^n\mu_2 - \mu_1\mu_2^n)(\mu_1^m - \mu_2^m)\right]. \tag{C.37}$$

In order to get a valid upper bound for Y_{02} and Y_{04} we need to study the sign of the coefficients of the remaining yields. We start by recasting each term of the sum corresponding to the Y_{nm}, with $n \geqslant 3$ and $m \geqslant 2$, in (C.37) as follows:

$$\frac{Y_{nm}}{n!m!}\frac{1}{(\mu_0 - \mu_2)(\mu_2 - \mu_1)}A_{22}(\mu_0, \mu_1, \mu_2, m)\cdot B_{02}(\mu_0, \mu_1, \mu_2, n), \tag{C.38}$$

where

$$B_{02}(\mu_0, \mu_1, \mu_2, n) \equiv \mu_1\mu_2\mu_0^n(\mu_1 - \mu_2) + \mu_0^2(\mu_1\mu_2^n - \mu_2\mu_1^n) + \mu_0(\mu_2^2\mu_1^n - \mu_1^2\mu_2^n) \tag{C.39}$$

and A_{22} is the one found when bounding Y_{22}, thus we know from (C.12) it can be recast as:

$$A_{22}(\mu_0, \mu_1, \mu_2, m) = (\mu_0 - \mu_2)(\mu_2 - \mu_1) \sum_{k=0}^{m-1} \mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k}). \tag{C.40}$$

We can rewrite B_{02} as:

$$\begin{aligned} B_{02}(\mu_0, \mu_1, \mu_2, n) &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)\left[\mu_0^{n-1} - \mu_0 \sum_{k=0}^{n-2} \mu_1^{n-2-k}\mu_2^k + \mu_1\mu_2 \sum_{j=0}^{n-3} \mu_1^{n-3-j}\mu_2^j\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)\left[\mu_0^{n-1} + \sum_{k=0}^{n-2} \mu_1^{n-2-k}\mu_2^k(\mu_2 - \mu_0) - \mu_2^{n-1}\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)\left[\mu_0^{n-1} - \mu_2^{n-1} - \sum_{k=0}^{n-2} \mu_1^{n-2-k}\mu_2^k(\mu_0 - \mu_2)\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\left[\sum_{k=0}^{n-2} \mu_2^k\mu_0^{n-2-k} - \sum_{k=0}^{n-2} \mu_2^k\mu_1^{n-2-k}\right] \\ &= \mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2) \sum_{k=0}^{n-2} \mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k}). \end{aligned} \tag{C.41}$$

Employing (C.40) and (C.41) into (C.38) we get:

$$\frac{Y_{nm}}{n!m!}\mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\left[\sum_{k=0}^{n-2} \mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k})\right]\left[\sum_{k=0}^{m-1} \mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k})\right], \tag{C.42}$$

which means that the sign of this expression is fully determined by the factor $(\mu_1 - \mu_2)(\mu_0 - \mu_2)$ (note that the product of the two sums in (C.42) is always positive).

Concerning the terms that appear in the sum in (C.37) corresponding to the Y_{0m}, with $m \geqslant 2$, we have:

$$\begin{aligned} &\frac{Y_{0m}}{m!}(\mu_1 - \mu_0)[\mu_2(\mu_0^m - \mu_1^m) - \mu_1(\mu_0^m - \mu_2^m) + \mu_0(\mu_1^m - \mu_2^m)] \\ &= \frac{Y_{0m}}{m!}(\mu_1 - \mu_0)A_{22}(\mu_0, \mu_1, \mu_2, m) \\ &= \frac{Y_{0m}}{m!}(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1) \sum_{k=0}^{m-1} \mu_2^k(\mu_0^{m-1-k} - \mu_1^{m-1-k}), \end{aligned} \tag{C.43}$$

where we used (C.11) in the first equality and (C.40) in the second equality. Expression (C.43) implies that its sign is always equal to the sign of the terms given by (C.42), since it is determined by the same factor $(\mu_1 - \mu_2)(\mu_0 - \mu_2)$ (note that the product of the last two factors in (C.43) is always positive).

A valid upper bound on Y_{02} is thus obtained by setting all the other yields to zero in (C.37). By doing so, we obtain:

$$Y_{02}^U = 2\frac{\frac{\mu_2 G_{02}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{02}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{02}^{1,2}}{\mu_1 - \mu_2}}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)}. \tag{C.44}$$

One can do the same when bounding Y_{04}, i.e. setting all the other yields to zero except for Y_{04}, in (C.37). We find that:

$$Y_{04}^U = 4!\frac{\frac{\mu_2 G_{02}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{02}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{02}^{1,2}}{\mu_1 - \mu_2}}{\mu_1(\mu_0^4 - \mu_2^4) - \mu_0(\mu_1^4 - \mu_2^4) - \mu_2(\mu_0^4 - \mu_1^4)}. \tag{C.45}$$

C.4. Upper bound on Y_{20} and Y_{40}

Consider the following combinations of gains in which all the terms Y_{0m} and Y_{n1} are removed:

$$\begin{aligned} G_{20}^{0,1} &= \mu_1\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{1,1} - \mu_0\tilde{Q}^{0,1} - \mu_1\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m); \\ G_{20}^{0,2} &= \mu_2\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{2,2} - \mu_0\tilde{Q}^{0,2} - \mu_2\tilde{Q}^{2,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m); \\ G_{20}^{1,2} &= \mu_2\tilde{Q}^{1,1} + \mu_1\tilde{Q}^{2,2} - \mu_1\tilde{Q}^{1,2} - \mu_2\tilde{Q}^{2,1} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_1^n - \mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m). \end{aligned} \tag{C.46}$$

We now combine $G_{20}^{0,1}$, $G_{20}^{0,2}$ and $G_{20}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the resulting expression has the yields Y_{1m} and Y_{n2} also removed:

$$\begin{aligned} G_{20}^{0,1} + c_0\, G_{20}^{0,2} + c_1\, G_{20}^{1,2} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}[(\mu_0^n - \mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m) \\ + c_0(\mu_0^n - \mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m) + c_1(\mu_1^n - \mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)]. \end{aligned} \tag{C.47}$$

For Y_{1m} and Y_{n2} to be removed the coefficients c_0 and c_1 must satisfy:

$$\begin{cases} (\mu_0^m\mu_1 - \mu_0\mu_1^m)(\mu_0 - \mu_1) + c_0(\mu_0^m\mu_2 - \mu_0\mu_2^m)(\mu_0 - \mu_2) + c_1(\mu_1^m\mu_2 - \mu_1\mu_2^m)(\mu_1 - \mu_2) = 0\,\forall\ m \\ (\mu_0^2\mu_1 - \mu_0\mu_1^2)(\mu_0^n - \mu_1^n) + c_0(\mu_0^2\mu_2 - \mu_0\mu_2^2)(\mu_0^n - \mu_2^n) + c_1(\mu_1^2\mu_2 - \mu_1\mu_2^2)(\mu_1^n - \mu_2^n) = 0\,\forall\, n. \end{cases} \tag{C.48}$$

This system of linear equations coincides with the one given by (C.33) that we found when bounding Y_{02}, thus the solution is given by (C.35) for c_0 and by (C.36) for c_1. Substituting these expressions back into (C.47) and multiplying both sides by μ_2, yields a combination of gains in which the terms Y_{n1}, Y_{n2}, Y_{0m} and Y_{1m} are removed:

$$\begin{aligned} &\mu_2 G_{20}^{0,1} - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}\, G_{20}^{0,2} + \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}\, G_{20}^{1,2} \\ &= \sum_{n=2}^{\infty} \frac{Y_{n0}}{n!}(\mu_0 - \mu_1)[-\mu_2(\mu_0^n - \mu_1^n) + \mu_1(\mu_0^n - \mu_2^n) - \mu_0(\mu_1^n - \mu_2^n)] \\ &\quad + \sum_{\substack{n=2\\ m=3}}^{\infty} \frac{Y_{nm}}{n!m!}\left[\mu_2(\mu_0^n - \mu_1^n)(\mu_0^m\mu_1 - \mu_0\mu_1^m) - \frac{\mu_1(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^n - \mu_2^n)(\mu_0^m\mu_2 - \mu_0\mu_2^m)\right. \\ &\quad \left. + \frac{\mu_0(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^n - \mu_2^n)(\mu_1^m\mu_2 - \mu_1\mu_2^m)\right]. \end{aligned} \tag{C.49}$$

Since the coefficients of Y_{n0} and Y_{nm} coincide with those found when bounding Y_{02} if one exchanges $m \longleftrightarrow n$, we can directly use the results obtained in appendix C.3 to recast the terms that contain the Y_{nm} with $n \geqslant 2$ and $m \geqslant 3$. In particular, according to (C.42), we obtain:

$$\frac{Y_{nm}}{n!m!}\mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\left[\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k} - \mu_1^{m-2-k})\right]\left[\sum_{k=0}^{n-1}\mu_2^k(\mu_0^{n-1-k} - \mu_1^{n-1-k})\right], \tag{C.50}$$

and according to (C.43) the terms that contain the yields Y_{n0} can be written as:

$$\frac{Y_{n0}}{n!}(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)\sum_{k=0}^{n-1}\mu_2^k(\mu_0^{n-1-k} - \mu_1^{n-1-k}). \tag{C.51}$$

Like in the case of Y_{02} (see appendix C.3), a valid upper bound on Y_{20} is thus obtained setting all the other yields to zero in (C.49). We obtain:

$$Y_{20}^U = 2\frac{\frac{\mu_2 G_{20}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{20}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{20}^{1,2}}{\mu_1 - \mu_2}}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_1)}. \tag{C.52}$$

One can do the same to bound Y_{40}, i.e. to set all the other yields to zero, except for Y_{40}. In this case we obtain:

$$Y_{04}^U = 4!\frac{\frac{\mu_2 G_{20}^{0,1}}{\mu_0 - \mu_1} - \frac{\mu_1 G_{20}^{0,2}}{\mu_0 - \mu_2} + \frac{\mu_0 G_{20}^{1,2}}{\mu_1 - \mu_2}}{\mu_1(\mu_0^4 - \mu_2^4) - \mu_0(\mu_1^4 - \mu_2^4) - \mu_2(\mu_0^4 - \mu_1^4)}. \tag{C.53}$$

C.5. Upper bound on Y_{13}

We look for that combination of gains in which all the terms proportional to Y_{n0}, Y_{n1}, Y_{0m} and Y_{2m} are removed. In order to find it, we consider the most general combination of all gains:

$$G_{13} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n\mu_j^m\right], \tag{C.54}$$

and impose proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\text{ removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right) = 0\,\forall\, n \quad \Leftarrow \quad c_{i,0} + c_{i,1} + c_{i,2} = 0 \quad \text{for } i = 0,\ 1,\ 2, \tag{C.55}$$

$$Y_{n1}\text{ removed: }\sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\mu_j c_{i,j}\right)=0\,\forall\,n\quad\Leftarrow\quad \mu_0 c_{i,0}+\mu_1 c_{i,1}+\mu_2 c_{i,2}=0\quad\text{for } i=0,\,1,\,2, \tag{C.56}$$

$$Y_{0m}\text{ removed: }\sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right)=0\,\forall\,m\quad\Leftarrow\quad c_{0,j}+c_{1,j}+c_{2,j}=0\quad\text{for } j=0,\,1,\,2, \tag{C.57}$$

$$Y_{2m}\text{ removed: }\sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}\mu_i^2 c_{i,j}\right)=0\,\forall\,m\quad\Leftarrow\quad \mu_0^2 c_{0,j}+\mu_1^2 c_{1,j}+\mu_2^2 c_{2,j}=0\quad\text{for } j=0,\,1,\,2. \tag{C.58}$$

The conditions given by equations (C.55)–(C.58) form an overdetermined system of equations for the nine variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0}=1$):

$$\begin{aligned}
c_{0,0}&=1,\\
c_{0,1}&=-\frac{(\mu_0-\mu_2)}{\mu_1-\mu_2},\\
c_{0,2}&=-1-c_{0,1}=\frac{\mu_0-\mu_1}{\mu_1-\mu_2},\\
c_{1,0}&=-\frac{(\mu_0^2-\mu_2^2)}{\mu_1^2-\mu_2^2},\\
c_{1,1}&=c_{1,0}c_{0,1}=\frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{1,2}&=-c_{1,0}-c_{1,1}=c_{1,0}c_{0,2}=-\frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{2,0}&=-1-c_{1,0}=\frac{\mu_0^2-\mu_1^2}{\mu_1^2-\mu_2^2},\\
c_{2,1}&=-c_{0,1}-c_{1,1}=c_{0,1}c_{2,0}=\frac{(\mu_1^2-\mu_0^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{2,2}&=-c_{2,0}-c_{2,1}=(1+c_{1,0})(1+c_{0,1})=\frac{(\mu_0^2-\mu_1^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)}.
\end{aligned} \tag{C.59}$$

By substituting (C.59) back into (C.54) we get an expression in which the terms Y_{n0}, Y_{n1}, Y_{0m} and Y_{2m} are removed:

$$\begin{aligned}
G_{13}=&\sum_{m=2}^{\infty}\frac{Y_{1m}}{m!}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_2)(\mu_1+\mu_2)}\cdot A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,m)\\
&+\sum_{\substack{m=2\\n=3}}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,m)\cdot A_{11}(\mu_0,\,\mu_1,\,\mu_2,\,n)}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)},
\end{aligned} \tag{C.60}$$

where A_{22} is the factor given by (C.11) also present in the bounds for Y_{02} and Y_{22}, whereas A_{11} is the factor given by (C.23) which appears in the bound on Y_{11}. Note that this is somehow expected: when bounding Y_{02} and Y_{22} we removed the terms Y_{n0} and Y_{n1} as we just did for Y_{13}, and in bounding Y_{11} we removed the terms Y_{0m} and Y_{2m} as we did here. Therefore, by exploiting the result given by (C.12) we can recast each term of the sum corresponding to the Y_{1m}, with $m\geqslant 2$, in (C.60) as:

$$-\frac{Y_{1m}}{m!}\frac{(\mu_0-\mu_2)^2}{(\mu_1+\mu_2)}(\mu_0-\mu_1)\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k}-\mu_1^{m-1-k}), \tag{C.61}$$

and realize that it is always negative, regardless of the value of the intensities.

By employing the results (C.12), (C.24) we can recast each term of the sum corresponding to the Y_{nm} with $n\geqslant 3$ and $m\geqslant 2$, in (C.60) as:

$$\frac{Y_{nm}}{n!m!}\frac{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)}(\mu_0-\mu_1)\sum_{k=0}^{m-1}\mu_2^k(\mu_0^{m-1-k}-\mu_1^{m-1-k})F(n), \tag{C.62}$$

and realize that it is always positive[9], regardless of the intensities.

[9] $F(n)$ is defined in (C.24).

A valid upper bound on Y_{13} is then obtained by setting $Y_{1m} \to 0$ (except for Y_{13}) and $Y_{nm} \to 1$ for all $n \geqslant 3$ and $m \geqslant 2$ in (C.60). As a result we obtain:

$$\begin{aligned} G_{13} &= -\frac{Y_{13}^U}{3!}\frac{(\mu_0-\mu_2)^2}{(\mu_1+\mu_2)}(\mu_0-\mu_1)[\mu_0^2-\mu_1^2+\mu_2(\mu_0-\mu_1)] \\ &+ \sum_{\substack{m=2\\n=3}}^{\infty}\frac{[\mu_1^m(\mu_0-\mu_2)+\mu_2^m(\mu_1-\mu_0)+\mu_0^m(\mu_2-\mu_1)]\cdot[\mu_1^n(\mu_0^2-\mu_2^2)+\mu_2^n(\mu_1^2-\mu_0^2)+\mu_0^n(\mu_2^2-\mu_1^2)]}{n!m!(\mu_1-\mu_2)^2(\mu_1+\mu_2)}, \end{aligned} \tag{C.63}$$

which implies:

$$\begin{aligned} \frac{Y_{13}^U}{6}\frac{(\mu_0-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}{\mu_1+\mu_2} &= -G_{13} \\ &+ \frac{(\mathrm{e}^{\mu_1}-\mu_1-1)(\mu_0-\mu_2)+(\mathrm{e}^{\mu_2}-\mu_2-1)(\mu_1-\mu_0)+(\mathrm{e}^{\mu_0}-\mu_0-1)(\mu_2-\mu_1)}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)} \\ &\times\left[\left(\mathrm{e}^{\mu_1}-\frac{\mu_1^2}{2}-\mu_1-1\right)(\mu_0^2-\mu_2^2)+\left(\mathrm{e}^{\mu_2}-\frac{\mu_2^2}{2}-\mu_2-1\right)(\mu_1^2-\mu_0^2)\right. \\ &+\left.\left(\mathrm{e}^{\mu_0}-\frac{\mu_0^2}{2}-\mu_0-1\right)(\mu_2^2-\mu_1^2)\right]. \end{aligned} \tag{C.64}$$

We thus obtain the following upper bound on Y_{13}:

$$\begin{aligned} Y_{13}^U \;=\; & -\frac{6(\mu_1+\mu_2)G_{13}}{(\mu_0-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}+\frac{6}{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)} \\ & \times[\mathrm{e}^{\mu_2}(\mu_1-\mu_0)+\mathrm{e}^{\mu_1}(\mu_0-\mu_2)+\mathrm{e}^{\mu_0}(\mu_2-\mu_1)] \\ & \times[\mathrm{e}^{\mu_2}(\mu_1^2-\mu_0^2)+\mathrm{e}^{\mu_1}(\mu_0^2-\mu_2^2)+\mathrm{e}^{\mu_0}(\mu_2^2-\mu_1^2)-(\mu_0-\mu_1)(\mu_1-\mu_2)(\mu_0-\mu_2)], \end{aligned} \tag{C.65}$$

where G_{13} is defined in (C.54) and the coefficients of the combination of gains in (C.59).

C.6. Upper bound on Y_{31}

We look for that combination of gains in which all the terms proportional to Y_{n0}, Y_{n2}, Y_{0m} and Y_{1m} are removed. In order to find it, we proceed like in the previous case. That is, we consider the most general combination of all gains:

$$G_{31} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n\mu_j^m\right], \tag{C.66}$$

and impose proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\,\text{removed:}\ \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right)=0\,\forall\, n \quad \Leftarrow \quad c_{i,0}+c_{i,1}+c_{i,2}=0 \ \text{ for } i=0,\,1,\,2, \tag{C.67}$$

$$Y_{n2}\,\text{removed:}\ \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\mu_j^2 c_{i,j}\right)=0\,\forall\, n \quad \Leftarrow \quad \mu_0^2c_{i,0}+\mu_1^2c_{i,1}+\mu_2^2c_{i,2}=0 \ \text{ for } i=0,\,1,\,2, \tag{C.68}$$

$$Y_{0m}\,\text{removed:}\ \sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right)=0\,\forall\, m \quad \Leftarrow \quad c_{0,j}+c_{1,j}+c_{2,j}=0 \ \text{ for } j=0,\,1,\,2, \tag{C.69}$$

$$Y_{1m}\,\text{removed:}\ \sum_{j=0}^{2}\mu_j^m\left(\sum_{i=0}^{2}\mu_i c_{i,j}\right)=0\,\forall\, m \quad \Leftarrow \quad \mu_0c_{0,j}+\mu_1c_{1,j}+\mu_2c_{2,j}=0 \ \text{ for } j=0,\,1,\,2. \tag{C.70}$$

The conditions (C.67)–(C.70) form an overdetermined system of equations for the nine variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0}=1$):

$$
\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= -\frac{(\mu_0^2-\mu_2^2)}{\mu_1^2-\mu_2^2},\\
c_{0,2} &= -1-c_{0,1} = \frac{\mu_0^2-\mu_1^2}{\mu_1^2-\mu_2^2},\\
c_{1,0} &= -\frac{(\mu_0-\mu_2)}{\mu_1-\mu_2},\\
c_{1,1} &= c_{1,0}c_{0,1} = \frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{1,2} &= -c_{1,0}-c_{1,1} = c_{1,0}c_{0,2} = \frac{(\mu_1^2-\mu_0^2)(\mu_0-\mu_2)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{2,0} &= -1-c_{1,0} = \frac{\mu_0-\mu_1}{\mu_1-\mu_2},\\
c_{2,1} &= -c_{0,1}-c_{1,1} = c_{0,1}c_{2,0} = -\frac{(\mu_0^2-\mu_2^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)},\\
c_{2,2} &= -c_{2,0}-c_{2,1} = (1+c_{1,0})(1+c_{0,1}) = \frac{(\mu_0^2-\mu_1^2)(\mu_0-\mu_1)}{(\mu_1^2-\mu_2^2)(\mu_1-\mu_2)}.
\end{aligned}
\tag{C.71}
$$

By substituting (C.71) back into (C.66) we get an expression in which the terms Y_{n0}, Y_{n2}, Y_{0m} and Y_{1m} are removed:

$$
\begin{aligned}
G_{31} = &\sum_{n=2}^{\infty}\frac{Y_{n1}}{n!}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_2)(\mu_1+\mu_2)}\cdot A_{22}(\mu_0,\mu_1,\mu_2,n)\\
&+\sum_{\substack{n=2\\m=3}}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{22}(\mu_0,\mu_1,\mu_2,n)\cdot A_{11}(\mu_0,\mu_1,\mu_2,m)}{(\mu_1-\mu_2)^2(\mu_1+\mu_2)},
\end{aligned}
\tag{C.72}
$$

where A_{22} and A_{11} are again the factors from Y_{22} and Y_{11} bounds given by equations (C.11), (C.23), similarly to what happens when bounding Y_{13} (see appendix C.5). Therefore the analysis of the coefficient's sign is the same as in appendix C.5. Hence a valid upper bound on Y_{31} is obtained by setting $Y_{n1}\to 0$ (except for Y_{31}) and $Y_{nm}\to 1$ in (C.72) for all $n\geqslant 2$ and $m\geqslant 3$ in (C.72). Analogous steps to those in appendix C.5 lead to the following upper bound:

$$
\begin{aligned}
Y_{31}^U = &-\frac{6(\mu_1+\mu_2)G_{31}}{(\mu_0-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}+\frac{6}{(\mu_0-\mu_2)^2(\mu_1-\mu_2)^2(\mu_0-\mu_1)^2(\mu_0+\mu_1+\mu_2)}\\
&\times[\mathrm{e}^{\mu_2}(\mu_1-\mu_0)+\mathrm{e}^{\mu_1}(\mu_0-\mu_2)+\mathrm{e}^{\mu_0}(\mu_2-\mu_1)]\\
&\times[\mathrm{e}^{\mu_2}(\mu_1^2-\mu_0^2)+\mathrm{e}^{\mu_1}(\mu_0^2-\mu_2^2)+\mathrm{e}^{\mu_0}(\mu_2^2-\mu_1^2)-(\mu_0-\mu_1)(\mu_1-\mu_2)(\mu_0-\mu_2)],
\end{aligned}
\tag{C.73}
$$

where G_{31} is defined in (C.66) and the coefficients of the combination of gains in (C.71).

C.7. Upper bound on Y_{00}

Consider the following combinations of gains in which all the terms Y_{1m} and Y_{n1} are removed:

$$
\begin{aligned}
G_{00}^{0,1} &= \mu_1^2\tilde{Q}^{0,0}+\mu_0^2\tilde{Q}^{1,1}-\mu_0\mu_1(\tilde{Q}^{0,1}+\tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1-\mu_0\mu_1^n)(\mu_0^m\mu_1-\mu_0\mu_1^m);\\
G_{00}^{0,2} &= \mu_2^2\tilde{Q}^{0,0}+\mu_0^2\tilde{Q}^{2,2}-\mu_0\mu_2(\tilde{Q}^{0,2}+\tilde{Q}^{2,0}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_2-\mu_0\mu_2^n)(\mu_0^m\mu_2-\mu_0\mu_2^m);\\
G_{00}^{1,2} &= \mu_2^2\tilde{Q}^{1,1}+\mu_1^2\tilde{Q}^{2,2}-\mu_1\mu_2(\tilde{Q}^{1,2}+\tilde{Q}^{2,1}) = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_1^n\mu_2-\mu_1\mu_2^n)(\mu_1^m\mu_2-\mu_1\mu_2^m).
\end{aligned}
\tag{C.74}
$$

We now combine $G_{00}^{0,1}$, $G_{00}^{0,2}$ and $G_{00}^{1,2}$ with arbitrary real coefficients c_0 and c_1 and impose that the terms Y_{2m} and Y_{n2} are also removed in the resulting expression:

$$
\begin{aligned}
G_{00}^{0,1}+c_0\,G_{00}^{0,2}+c_1\,G_{00}^{1,2} = &\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}[(\mu_0^n\mu_1-\mu_0\mu_1^n)(\mu_0^m\mu_1-\mu_0\mu_1^m)\\
&+c_0(\mu_0^n\mu_2-\mu_0\mu_2^n)(\mu_0^m\mu_2-\mu_0\mu_2^m)+c_1(\mu_1^n\mu_2-\mu_1\mu_2^n)(\mu_1^m\mu_2-\mu_1\mu_2^m)].
\end{aligned}
\tag{C.75}
$$

For Y_{2m} and Y_{n2} to be removed it suffices that for every m it holds:

$$(\mu_0^2\mu_1 - \mu_0\mu_1^2)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + c_0(\mu_0^2\mu_2 - \mu_0\mu_2^2)(\mu_0^m\mu_2 - \mu_0\mu_2^m) \\ + c_1(\mu_1^2\mu_2 - \mu_1\mu_2^2)(\mu_1^m\mu_2 - \mu_1\mu_2^m) = 0, \tag{C.76}$$

which is fulfilled by:

$$c_0 = -\frac{\mu_1^2(\mu_0 - \mu_1)}{\mu_2^2(\mu_0 - \mu_2)}, \tag{C.77}$$

$$c_1 = \frac{\mu_0^2(\mu_0 - \mu_1)}{\mu_2^2(\mu_1 - \mu_2)}. \tag{C.78}$$

Substituting (C.77) and (C.78) back into (C.75) and multiplying both sides by μ_2^2, we get an expression where all the terms Y_{0m}, Y_{2m}, Y_{n0} and Y_{n2} are removed and where the term Y_{00} gives the largest contribution. More precisely, we find that:

$$\begin{aligned} &\mu_2^2 G_{00}^{0,1} - \mu_1^2\frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}\, G_{00}^{0,2} + \mu_0^2\frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}\, G_{00}^{1,2} \\ &= Y_{00}[\mu_2^2(\mu_0 - \mu_1)^2 - \mu_1^2(\mu_0 - \mu_1)(\mu_0 - \mu_2) + \mu_0^2(\mu_0 - \mu_1)(\mu_1 - \mu_2)] \\ &\quad + \sum_{m=3}^{\infty}\frac{Y_{0m}}{m!}[\mu_2^2(\mu_1 - \mu_0)(\mu_0^m\mu_1 - \mu_0\mu_1^m) + \mu_1^2(\mu_0 - \mu_1)(\mu_0^m\mu_2 - \mu_0\mu_2^m) - \mu_0^2(\mu_0 - \mu_1)(\mu_1^m\mu_2 - \mu_1\mu_2^m)] \\ &\quad + \sum_{n=3}^{\infty}\frac{Y_{n0}}{n!}[\mu_2^2(\mu_1 - \mu_0)(\mu_0^n\mu_1 - \mu_0\mu_1^n) + \mu_1^2(\mu_0 - \mu_1)(\mu_0^n\mu_2 - \mu_0\mu_2^n) - \mu_0^2(\mu_0 - \mu_1)(\mu_1^n\mu_2 - \mu_1\mu_2^n)] \\ &\quad + \sum_{n,m=3}^{\infty}\frac{Y_{nm}}{n!m!}\mu_0^2\mu_1^2\mu_2^2[(\mu_0^{n-1} - \mu_1^{n-1})(\mu_0^{m-1} - \mu_1^{m-1}) \\ &\quad - \frac{(\mu_0 - \mu_1)}{(\mu_0 - \mu_2)}(\mu_0^{n-1} - \mu_2^{n-1})(\mu_0^{m-1} - \mu_2^{m-1}) + \frac{(\mu_0 - \mu_1)}{(\mu_1 - \mu_2)}(\mu_1^{n-1} - \mu_2^{n-1})(\mu_1^{m-1} - \mu_2^{m-1})\Big]. \end{aligned} \tag{C.79}$$

In order to extract an upper bound on Y_{00} we need to study the sign of the yield's coefficients. We start by recasting the term corresponding to Y_{00} as:

$$\begin{aligned} &Y_{00}(\mu_0 - \mu_1)[\mu_2^2(\mu_0 - \mu_1) - \mu_1^2(\mu_0 - \mu_2) + \mu_0^2(\mu_1 - \mu_2)] \\ &\quad = Y_{00}(\mu_0 - \mu_1)^2(\mu_1 - \mu_2)(\mu_0 - \mu_2). \end{aligned} \tag{C.80}$$

We observe that the sign of this expression is determined by the factors $(\mu_1 - \mu_2)(\mu_0 - \mu_2)$.

We then proceed by recasting each term of the sum corresponding to the Y_{nm}, with $n,\ m \geqslant 3$ in (C.79) as:

$$\frac{Y_{nm}}{n!m!}\frac{A_{00}(\mu_0,\ \mu_1,\ \mu_2,\ m)\cdot A_{00}(\mu_0,\ \mu_1,\ \mu_2,\ n)}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)}, \tag{C.81}$$

where

$$A_{00}(\mu_0,\ \mu_1,\ \mu_2,\ m) \equiv \mu_1^m(\mu_2^2\mu_0 - \mu_2\mu_0^2) + \mu_2^m(\mu_0^2\mu_1 - \mu_0\mu_1^2) + \mu_0^m(\mu_1^2\mu_2 - \mu_1\mu_2^2). \tag{C.82}$$

This factor can be rewritten as:

$$\begin{aligned} &A_{00}(\mu_0,\ \mu_1,\ \mu_2,\ m) = \mu_0\mu_1\mu_2[\mu_1^{m-1}(\mu_2 - \mu_0) + \mu_2^{m-1}(\mu_0 - \mu_1) + \mu_0^{m-1}(\mu_1 - \mu_2)] \\ &\quad = -\mu_0\mu_1\mu_2\, A_{22}(\mu_0,\ \mu_1,\ \mu_2,\ m - 1), \end{aligned} \tag{C.83}$$

where A_{22} is defined as (C.11) in appendix C.1. Thus we can use the result (C.12) obtained in appendix C.1 to directly recast A_{00} as:

$$A_{00}(\mu_0,\ \mu_1,\ \mu_2,\ m) = \mu_0\mu_1\mu_2(\mu_0 - \mu_2)(\mu_1 - \mu_2)\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k} - \mu_1^{m-2-k}). \tag{C.84}$$

By substituting (C.84) back into (C.81), we get the final expression for each term of the sum corresponding to the Y_{nm}, with $n,\ m \geqslant 3$ in (C.79):

$$\frac{Y_{nm}}{n!m!}\mu_0^2\mu_1^2\mu_2^2(\mu_0 - \mu_2)(\mu_1 - \mu_2)\left[\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k} - \mu_1^{m-2-k})\right]\left[\sum_{k=0}^{n-2}\mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k})\right], \tag{C.85}$$

which has manifestly the same sign as the expression given by (C.80), for any value of the intensities (the product of the last two factors is always positive).

Finally, we recast the Y_{0m}'s terms (Y_{n0}'s terms are identical under the replacement $m \to n$) as:

$$\begin{aligned} &\frac{Y_{0m}}{m!}\mu_0\mu_1\mu_2(\mu_0-\mu_1)[\mu_2(\mu_1^{m-1}-\mu_0^{m-1})+\mu_1(\mu_0^{m-1}-\mu_2^{m-1})-\mu_0(\mu_1^{m-1}-\mu_2^{m-1})] \\ &=\frac{Y_{0m}}{m!}(\mu_0-\mu_1)A_{00}(\mu_0,\,\mu_1,\,\mu_2,\,m) \\ &=\frac{Y_{0m}}{m!}\mu_0\mu_1\mu_2(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)\sum_{k=0}^{m-2}\mu_2^k(\mu_0^{m-2-k}-\mu_1^{m-2-k}), \end{aligned} \tag{C.86}$$

where we employed (C.83) in the first equality and (C.84) in the second one. We observe that the sign of the Y_{0m}'s terms is again determined by the factors $(\mu_0-\mu_2)(\mu_1-\mu_2)$.

We conclude that the coefficients of Y_{0m}, Y_{n0} and Y_{nm}, with $n,\ m \geqslant 3$, carry the same sign as Y_{00}'s, which implies that a valid upper bound on Y_{00} is obtained by setting all the other yields to zero in (C.79). In so doing, we find that:

$$Y_{00}^U=\frac{\frac{\mu_2^2G_{00}^{0,1}}{\mu_0-\mu_1}-\frac{\mu_1^2G_{00}^{0,2}}{\mu_0-\mu_2}+\frac{\mu_0^2G_{00}^{1,2}}{\mu_1-\mu_2}}{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)}. \tag{C.87}$$

Appendix D. Yield's bounds with four decoys

Here we derive analytical upper bounds on the yields appearing in (1.7), following the same lines of section 2. In this case we assume that Alice and Bob can prepare their phase-randomized coherent pulses with four different intensity settings: $\{\mu_0, \mu_1, \mu_2, \mu_3\}$, which are the same for both parties. This choice is optimal since we assumed that the two optical channels linking the parties to the central node C have equal transmittance $\sqrt{\eta}$ [43].

The whole set of infinite yields is subjected to the following sixteen equality constraints:

$$\tilde{Q}^{k,l}\equiv \mathrm{e}^{\mu_k+\mu_l}Q^{k,l}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}{\mu_k}^n{\mu_l}^m \quad k,\,l\in\{0,\,1,\,2,\,3\}, \tag{D.1}$$

and to the same inequality constraints given by (2.3).

In this appendix we only obtain bounds on the yields Y_{13}, Y_{31}, Y_{04} and Y_{40} since the bounds derived on the yields Y_{00}, Y_{11}, Y_{02}, Y_{20} and Y_{22} in appendix C are already good enough, i.e bounding them with one additional decoy intensity would not result in a significant improvement of the performance of the protocol.

D.1. Upper bound on Y_{04}

Consider the following combinations of gains in which all the terms Y_{1m} and Y_{n0} are removed:

$$G_{04}^{i,j}=\mu_j\tilde{Q}^{i,i}+\mu_i\tilde{Q}^{j,j}-\mu_j\tilde{Q}^{i,j}-\mu_i\tilde{Q}^{j,i}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i^m-\mu_j^m), \tag{D.2}$$

where $i,\,j\in\{0,\,1,\,2,\,3\}$. Since $G_{04}^{i,i}=0$ and $G_{04}^{i,j}=G_{04}^{j,i}$, we only have six distinct combinations that read (for $j>i$): $G_{04}^{0,1}$, $G_{04}^{0,2}$, $G_{04}^{0,3}$, $G_{04}^{1,2}$, $G_{04}^{1,3}$, $G_{04}^{2,3}$.

We now take the linear combination of the $G_{04}^{i,j}$ such that even the yields Y_{2m}, Y_{3m}, Y_{n1} and Y_{n2} are removed:

$$\sum_{j>i}c_{i,j}G_{04}^{i,j}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\sum_{j>i}c_{i,j}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i^m-\mu_j^m), \tag{D.3}$$

where we implicitly assume that both indexes i, j run over the set $\{0, 1, 2, 3\}$. For Y_{2m}, Y_{3m}, Y_{n1} and Y_{n2} to be removed, the real coefficients $c_{i,j}$ must satisfy:

$$\begin{cases} \sum_{j>i}c_{i,j}(\mu_j\mu_i^2-\mu_i\mu_j^2)(\mu_i^m-\mu_j^m)=0\ \forall\, m \\ \sum_{j>i}c_{i,j}(\mu_j\mu_i^3-\mu_i\mu_j^3)(\mu_i^m-\mu_j^m)=0\ \forall\, m \\ \sum_{j>i}c_{i,j}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i-\mu_j)=0\ \forall\, n \\ \sum_{j>i}c_{i,j}(\mu_j\mu_i^n-\mu_i\mu_j^n)(\mu_i^2-\mu_j^2)=0\ \forall\, n \end{cases}. \tag{D.4}$$

In order to solve system (D.4), we look for those coefficients $c_{i,j}$ such that the multiplicative factors of μ_i^m and μ_i^n (for $i=0,1,2,3$) are all set to zero. This corresponds to imposing sixteen conditions on the six coefficients $c_{i,j}$. These conditions are not all independent, and a solution can be found even when we require (for simplicity) that $c_{0,1}=1$:

$$
\begin{aligned}
c_{0,1} &= 1,\\
c_{0,2} &= -\frac{(\mu_0-\mu_1)\mu_1(\mu_1-\mu_3)}{(\mu_0-\mu_2)\mu_2(\mu_2-\mu_3)},\\
c_{0,3} &= \frac{(\mu_0-\mu_1)\mu_1(\mu_1-\mu_2)}{(\mu_0-\mu_3)\mu_3(\mu_2-\mu_3)},\\
c_{1,2} &= \frac{(\mu_0-\mu_1)\mu_0(\mu_0-\mu_3)}{(\mu_1-\mu_2)\mu_2(\mu_2-\mu_3)},\\
c_{1,3} &= -\frac{(\mu_0-\mu_1)\mu_0(\mu_0-\mu_2)}{(\mu_1-\mu_3)\mu_3(\mu_2-\mu_3)},\\
c_{2,3} &= \frac{\mu_0\mu_1(\mu_0-\mu_1)^2}{\mu_2\mu_3(\mu_2-\mu_3)^2}.
\end{aligned}
\tag{D.5}
$$

By substituting the solution for the coefficients given by (D.5) back into (D.3), one gets:

$$
\sum_{j>i} c_{i,j}G_{04}^{i,j} = \sum_{m=3}^{\infty}\frac{Y_{0m}}{m!}A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m) + \sum_{\substack{n=4\\ m=3}}^{\infty}\frac{Y_{nm}}{n!m!}B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n,\,m),
\tag{D.6}
$$

where:

$$
\begin{aligned}
A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m) &= -\frac{(\mu_0-\mu_1)}{\mu_2\mu_3(\mu_2-\mu_3)}[\mu_0^m(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\\
&\quad -\mu_1^m(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3)+\mu_2^m(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)\\
&\quad -\mu_3^m(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)]\\
&= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_0-\mu_3)(\mu_1-\mu_3)}{\mu_2\mu_3}\left(\sum_{i_1\leqslant i_2\leqslant\,\dots\,\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\,\dots\cdot\mu_{i_{m-3}}\right),
\end{aligned}
\tag{D.7}
$$

and

$$
\begin{aligned}
&B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n,\,m)\\
&= \frac{-\mu_0\mu_1}{(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_0-\mu_3)(\mu_2-\mu_3)^2}[\mu_0^m(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\\
&\quad -\mu_1^m(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3)+\mu_2^m(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)\\
&\quad -\mu_3^m(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)]\times[-\mu_0^{n-1}(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\\
&\quad +\mu_1^{n-1}(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3)-\mu_2^{n-1}(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)\\
&\quad +\mu_3^{n-1}(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)]\\
&= -\mu_0\mu_1\mu_2\mu_3\,A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m)\cdot\left(\sum_{i_1\leqslant i_2\leqslant\,\dots\,\leqslant i_{n-4}}\mu_{i_1}\mu_{i_2}\cdot\,\dots\cdot\mu_{i_{n-4}}\right).
\end{aligned}
\tag{D.8}
$$

In (D.7), (D.8) we again assume that the indexes in the sums run over the set $\{0, 1, 2, 3\}$ and we define $\sum_{i_1\leqslant i_2\leqslant\,\dots\,\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\,\dots\cdot\mu_{i_{m-3}}|_{m=3} = 1$. From (D.7) we deduce that the sign of Y_{0m}'s coefficient is independent of m, while from (D.8) we deduce that Y_{nm}'s coefficient has always opposite sign to that of Y_{0m}. Therefore a valid upper bound on Y_{04} is obtained by setting to zero all the other yields Y_{0m} and to 1 the yields Y_{nm} with $n \geqslant 4$ and $m \geqslant 3$ in (D.6). We thus obtain:

$$
\sum_{j>i} c_{i,j}G_{04}^{i,j} = \frac{Y_{04}^U}{4!}A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4) + \sum_{\substack{n=4\\ m=3}}^{\infty}\frac{B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n,\,m)}{n!m!},
\tag{D.9}
$$

which implies the following upper bound on Y_{04}:

$$
Y_{04}^U = \frac{4!}{A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4)}\left[\sum_{j>i} c_{i,j}G_{04}^{i,j} - \sum_{\substack{n=4\\ m=3}}^{\infty}\frac{B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n,\,m)}{n!m!}\right],
\tag{D.10}
$$

where $c_{i,j}$ are given in (D.5), $G_{04}^{i,j}$ is defined in (D.2), the coefficient A_{04} reads:

$$
A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4) = -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_0-\mu_3)(\mu_1-\mu_3)(\mu_0+\mu_1+\mu_2+\mu_3)}{\mu_2\mu_3},
\tag{D.11}
$$

and the sum over the coefficient B_{04} reads:

$$\sum_{\substack{n=4\\m=3}}^{\infty}\frac{B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n,\,m)}{n!m!}=\frac{\mu_0\mu_1}{(\mu_0-\mu_2)(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_0-\mu_3)(\mu_2-\mu_3)^2}$$
$$\times\left[\left(\mathrm{e}^{\mu_0}-1-\mu_0-\frac{\mu_0^2}{2}\right)(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)\right.$$
$$-\left(\mathrm{e}^{\mu_1}-1-\mu_1-\frac{\mu_1^2}{2}\right)(\mu_0-\mu_2)(\mu_0-\mu_3)(\mu_2-\mu_3)$$
$$+\left(\mathrm{e}^{\mu_2}-1-\mu_2-\frac{\mu_2^2}{2}\right)(\mu_0-\mu_1)(\mu_0-\mu_3)(\mu_1-\mu_3)$$
$$\left.-\left(\mathrm{e}^{\mu_3}-1-\mu_3-\frac{\mu_3^2}{2}\right)(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)\right]^2. \tag{D.12}$$

D.2. Upper bound on Y_{40}

Consider the following combinations of gains in which all the terms Y_{0m} and Y_{n1} are removed:

$$G_{40}^{i,j}=\mu_j\tilde{Q}^{i,i}+\mu_i\tilde{Q}^{j,j}-\mu_i\tilde{Q}^{i,j}-\mu_j\tilde{Q}^{j,i}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^m-\mu_i\mu_j^m), \tag{D.13}$$

where $i, j\in\{0,\,1,\,2,\,3\}$. Since $G_{40}^{i,i}=0$ and $G_{40}^{i,j}=G_{40}^{j,i}$, we only have six distinct combinations that read (for $j>i$): $G_{40}^{0,1}$, $G_{40}^{0,2}$, $G_{40}^{0,3}$, $G_{40}^{1,2}$, $G_{40}^{1,3}$, $G_{40}^{2,3}$.

We now take the linear combination of the $G_{40}^{i,j}$ such that even the yields Y_{1m}, Y_{2m}, Y_{n2} and Y_{n3} are removed:

$$\sum_{j>i}c_{i,j}G_{40}^{i,j}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\sum_{j>i}c_{i,j}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^m-\mu_i\mu_j^m), \tag{D.14}$$

where we implicitly assume that both indexes i, j run over the set $\{0, 1, 2, 3\}$. For Y_{1m}, Y_{2m}, Y_{n2} and Y_{n3} to be removed, the real coefficients $c_{i,j}$ must satisfy:

$$\begin{cases}\sum_{j>i}c_{i,j}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^2-\mu_i\mu_j^2)=0\ \forall\, n\\ \sum_{j>i}c_{i,j}(\mu_i^n-\mu_j^n)(\mu_j\mu_i^3-\mu_i\mu_j^3)=0\ \forall\, n\\ \sum_{j>i}c_{i,j}(\mu_i-\mu_j)(\mu_j\mu_i^m-\mu_i\mu_j^m)=0\ \forall\, m\\ \sum_{j>i}c_{i,j}(\mu_i^2-\mu_j^2)(\mu_j\mu_i^m-\mu_i\mu_j^m)=0\ \forall\, m.\end{cases} \tag{D.15}$$

We now notice that the system (D.15) is exactly the same system solved in appendix D.2 while bounding Y_{04}, thus the solution for the coefficients $c_{i,j}$ is given in (D.5). By substituting the solution (D.5) back into (D.14), one gets:

$$\sum_{j>i}c_{i,j}G_{40}^{i,j}=\sum_{n=3}^{\infty}\frac{Y_{n0}}{n!}A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n)+\sum_{\substack{n=3\\m=4}}^{\infty}\frac{Y_{nm}}{n!m!}B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m,\,n), \tag{D.16}$$

where A_{04} and B_{04} are the coefficients defined in (D.7), (D.8) while bounding Y_{04}. Hence we can adopt the observations made on the sign of A_{04} and B_{04} from appendix D.1 and conclude that a valid upper bound on Y_{40} is obtained by setting to zero all the other yields Y_{n0} and to 1 the yields Y_{nm} with $n\geqslant 3$ and $m\geqslant 4$ in (D.16). The upper bound on Y_{40} then reads:

$$Y_{40}^U=\frac{4!}{A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4)}\left[\sum_{j>i}c_{i,j}G_{40}^{i,j}-\sum_{\substack{n=3\\m=4}}^{\infty}\frac{B_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m,\,n)}{n!m!}\right], \tag{D.17}$$

where $c_{i,j}$, $G_{40}^{i,j}$, $A_{04}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,4)$ and the sum over B_{04} are given in (D.5), (D.13), (D.11) and (D.12), respectively.

D.3. Upper bound on Y_{13}

We consider the most general combination of all sixteen gains:

$$\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{3} c_{i,j}\mu_i^n\mu_j^m\right], \tag{D.18}$$

and require that the terms Y_{n0}, Y_{n1}, Y_{n2}, Y_{0m}, Y_{2m} and Y_{3m} are removed, by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i^n = 0\ \forall n \quad\Leftarrow\quad \sum_{j=0}^{3} c_{i,j} = 0 \text{ for } i = 0, 1, 2, 3, \tag{D.19}$$

$$Y_{n1}\text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i^n\mu_j = 0\ \forall n \quad\Leftarrow\quad \sum_{j=0}^{3} c_{i,j}\mu_j = 0 \text{ for } i = 0, 1, 2, 3, \tag{D.20}$$

$$Y_{n2}\text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i^n\mu_j^2 = 0\ \forall n \quad\Leftarrow\quad \sum_{j=0}^{3} c_{i,j}\mu_j^2 = 0 \text{ for } i = 0, 1, 2, 3, \tag{D.21}$$

$$Y_{0m}\text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_j^m = 0\ \forall m \quad\Leftarrow\quad \sum_{i=0}^{3} c_{i,j} = 0 \text{ for } j = 0, 1, 2, 3, \tag{D.22}$$

$$Y_{2m}\text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i^2\mu_j^m = 0\ \forall m \quad\Leftarrow\quad \sum_{i=0}^{3} c_{i,j}\mu_i^2 = 0 \text{ for } j = 0, 1, 2, 3, \tag{D.23}$$

$$Y_{3m}\text{ removed: } \sum_{i,j=0}^{3} c_{i,j}\mu_i^3\mu_j^m = 0\ \forall m \quad\Leftarrow\quad \sum_{i=0}^{3} c_{i,j}\mu_i^3 = 0 \text{ for } j = 0, 1, 2, 3. \tag{D.24}$$

The twenty-four conditions given by (D.19)–(D.24) form an over-determined system of equations for the sixteen variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0} = 1$):

$$\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= \frac{(\mu_0-\mu_2)(\mu_0-\mu_3)}{(\mu_2-\mu_1)(\mu_1-\mu_3)},\\
c_{0,2} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)}{(\mu_1-\mu_2)(\mu_2-\mu_3)},\\
c_{0,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_3)(\mu_3-\mu_2)},\\
c_{1,0} &= -\frac{(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,1} &= \frac{(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,2} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,1} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},
\end{aligned}$$

$$
\begin{aligned}
c_{2,2} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,3} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)(\mu_3-\mu_2)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,1} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,2} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,3} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}.
\end{aligned}
\tag{D.25}
$$

By substituting these expressions back into (D.18) and by making some simplifications, one gets:

$$
\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j} = \sum_{m=3}^{\infty}\frac{Y_{1m}}{m!}A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m) + \sum_{\substack{n=4\\ m=3}}^{\infty}\frac{Y_{nm}}{n!m!}A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m)\cdot C_n,
\tag{D.26}
$$

where:

$$
A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,m) = \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2}{\mu_2\mu_3+\mu_1\mu_2+\mu_1\mu_3}\left(\sum_{i_1\leqslant i_2\leqslant\,\ldots\,\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{m-3}}\right),
\tag{D.27}
$$

and C_n $(n \geqslant 5)$ is defined recursively as:

$$
\begin{cases}
C_n &= \left[\sum_{j=1}^{n-4}(\mu_0^j+\mu_1^j+\mu_2^j+\mu_3^j)C_{n-j} - \mu_0\mu_1\mu_2\mu_3\left(\sum_{i_1\leqslant i_2\leqslant\,\ldots\,\leqslant i_{n-5}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{n-5}}\right)\right]/(n-4)\\
C_4 &= \mu_0\mu_1\mu_2+\mu_0\mu_1\mu_3+\mu_0\mu_2\mu_3+\mu_1\mu_2\mu_3.
\end{cases}
\tag{D.28}
$$

In (D.27), (D.28) we assume that the indexes i_j in the sums run over the set $\{0, 1, 2, 3\}$ and we define $\sum_{i_1\leqslant i_2\leqslant\,\ldots\,\leqslant i_{m-3}}\mu_{i_1}\mu_{i_2}\cdot\ldots\cdot\mu_{i_{m-3}}|_{m=3} = 1$. From (D.27) we deduce that the sign of Y_{1m}'s coefficient is always positive, while from (D.28) we deduce that Y_{nm}'s coefficient has always equal sign to that of Y_{1m}, since C_n is always a positive quantity. Therefore a valid upper bound on Y_{13} is obtained by setting to zero all the other yields in (D.26). The upper bound on Y_{13} then reads:

$$
Y_{13}^{U} = \frac{6}{A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,3)}\left(\sum_{i,j=0}^{3}c_{i,j}\tilde{Q}^{i,j}\right),
\tag{D.29}
$$

where $c_{i,j}$ are defined in (D.25) and $A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,3)$ reads:

$$
A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,3) = \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2}{\mu_2\mu_3+\mu_1\mu_2+\mu_1\mu_3}.
\tag{D.30}
$$

D.4. Upper bound on Y_{31}

We consider the most general combination of all sixteen gains:

$$
\sum_{i,j=0}^{3}c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{3}c_{i,j}\mu_i^n\mu_j^m\right],
\tag{D.31}
$$

and require that the terms Y_{n0}, Y_{n2}, Y_{n3}, Y_{0m}, Y_{1m} and Y_{2m} are removed, by imposing proper conditions on the real coefficients $c_{i,j}$:

$$
Y_{n0}\text{ removed:}\quad \sum_{i,j=0}^{3}c_{i,j}\mu_i^n = 0\ \forall n \quad\Leftarrow\quad \sum_{j=0}^{3}c_{i,j} = 0 \quad\text{for}\quad i = 0,\,1,\,2,\,3,
\tag{D.32}
$$

$$
Y_{n2}\text{ removed:}\quad \sum_{i,j=0}^{3}c_{i,j}\mu_i^n\mu_j^2 = 0\ \forall n \quad\Leftarrow\quad \sum_{j=0}^{3}c_{i,j}\mu_j^2 = 0 \quad\text{for}\quad i = 0,\,1,\,2,\,3,
\tag{D.33}
$$

$$
Y_{n3}\text{ removed:}\quad \sum_{i,j=0}^{3}c_{i,j}\mu_i^n\mu_j^3 = 0\ \forall n \quad\Leftarrow\quad \sum_{j=0}^{3}c_{i,j}\mu_j^3 = 0 \quad\text{for}\quad i = 0,\,1,\,2,\,3,
\tag{D.34}
$$

$$Y_{0m}\text{ removed:}\quad \sum_{i,j=0}^{3} c_{i,j}\mu_j^m = 0\ \forall\, m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j} = 0 \quad \text{for} \quad j = 0,\, 1,\, 2,\, 3, \tag{D.35}$$

$$Y_{1m}\text{ removed:}\quad \sum_{i,j=0}^{3} c_{i,j}\mu_i\mu_j^m = 0\ \forall\, m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j}\mu_i = 0 \quad \text{for} \quad j = 0,\, 1,\, 2,\, 3, \tag{D.36}$$

$$Y_{2m}\text{ removed:}\quad \sum_{i,j=0}^{3} c_{i,j}\mu_i^2\mu_j^m = 0\,\forall\, m \quad \Leftarrow \quad \sum_{i=0}^{3} c_{i,j}\mu_i^2 = 0 \quad \text{for} \quad j = 0,\, 1,\, 2,\, 3. \tag{D.37}$$

The twenty-four conditions (D.32)–(D.37) form an over-determined system of equations for the sixteen variables $c_{i,j}$. However, thanks to the symmetries of the problem, a unique solution for $c_{i,j}$ exists and reads (we rescale every coefficient by requiring $c_{0,0} = 1$):

$$\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= -\frac{(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{0,2} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{0,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)(\mu_3-\mu_2)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,0} &= \frac{(\mu_0-\mu_2)(\mu_0-\mu_3)}{(\mu_2-\mu_1)(\mu_1-\mu_3)},\\
c_{1,1} &= \frac{(\mu_0-\mu_2)^2(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,2} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{1,3} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_3)}{(\mu_1-\mu_2)(\mu_2-\mu_3)},\\
c_{2,1} &= -\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_0-\mu_3)^2[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)^2(\mu_1-\mu_3)(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,2} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_3)^2[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{2,3} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,0} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)}{(\mu_1-\mu_3)(\mu_3-\mu_2)},\\
c_{3,1} &= \frac{(\mu_0-\mu_1)(\mu_0-\mu_2)^2(\mu_0-\mu_3)[\mu_0(\mu_2+\mu_3)+\mu_2\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)^2(\mu_2-\mu_3)[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,2} &= -\frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)(\mu_0-\mu_3)[\mu_0(\mu_1+\mu_3)+\mu_1\mu_3]}{(\mu_1-\mu_2)(\mu_1-\mu_3)(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]},\\
c_{3,3} &= \frac{(\mu_0-\mu_1)^2(\mu_0-\mu_2)^2[\mu_0(\mu_1+\mu_2)+\mu_1\mu_2]}{(\mu_1-\mu_3)^2(\mu_2-\mu_3)^2[\mu_1(\mu_2+\mu_3)+\mu_2\mu_3]}.
\end{aligned} \tag{D.38}$$

By substituting these expressions back into (D.31) and by making some simplifications, one gets:

$$\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j} = \sum_{n=3}^{\infty} \frac{Y_{n1}}{n!} A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n) + \sum_{\substack{n=3\\ m=4}}^{\infty} \frac{Y_{nm}}{n!m!} A_{13}(\mu_0,\,\mu_1,\,\mu_2,\,\mu_3,\,n)\cdot C_m, \tag{D.39}$$

where A_{13} and C_m also appear in appendix D.3 when bounding Y_{13} and are defined as (D.27) and (D.28), respectively. Thus, following the same lines of appendix D.3, we conclude that all yields in (D.39) are multiplied by a positive factor. A valid upper bound on Y_{31} is then obtained by setting to zero all the other yields in (D.39). We obtain:

$$Y_{31}^{U} = \frac{6}{A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, 3)}\left(\sum_{i,j=0}^{3} c_{i,j}\tilde{Q}^{i,j}\right), \tag{D.40}$$

where $c_{i,j}$ and $A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, 3)$ are defined in (D.38) and (D.30), respectively.

ORCID iDs

Federico Grasselli https://orcid.org/0000-0003-2966-7813

References

[1] Gisin N and Thew R 2007 *Nat. Photon.* **1** 165–71
[2] Kimble H J 2008 *Nature* **453** 1023
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Scarani V, Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[6] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[7] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[8] Lo H-K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595–604
[9] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 *NPJ Quantum Inf.* **2** 16025
[10] Epping M, Kampermann H, Macchiavello C and Bruß D 2017 *New J. Phys.* **19** 093012
[11] Friedman R A, Dupuis F, Fawzi O, Renner R and Vidick T 2018 *Nat. Commun.* **9** 459
[12] Ribeiro J, Murta G and Wehner S 2018 *Phys. Rev.* A **97** 022307
[13] Grasselli F, Kampermann H and Bruß D 2018 *New J. Phys.* **20** 113014
[14] Yin H-L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[15] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502
[16] Liao S-K *et al* 2017 *Nature* **549** 43
[17] Takenaka H *et al* 2017 *Nat. Photon.* **11** 502
[18] Takeoka M, Guha S and Wilde M M 2014 *Nat. Commun.* **5** 5235
[19] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[20] Sangouard N, Simon C, de Riedmatten N and Gisin N 2011 *Rev. Mod. Phys.* **83** 33–80
[21] Duan L-M, Lukin M D, Cirac J I and Zoller P 2001 *Nature* **414** 413–8
[22] Grudka A *et al* 2014 *Phys. Rev.* A **90** 062311
[23] Munro W J, Stephens A M, Devitt S J, Harrison K A and Nemoto K 2012 *Nat. Photon.* **6** 777–81
[24] Azuma K, Tamaki K and Lo H-K 2015 *Nat. Commun.* **6** 6787
[25] Abruzzo S, Kampermann H and Bruß D 2014 *Phys. Rev.* A **89** 012301
[26] Panayi C, Razavi M, Ma X and Lütkenhaus N 2014 *New J. Phys.* **16** 043005
[27] Azuma K, Tamaki K and Munro W J 2015 *Nat. Commun.* **6** 10171
[28] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[29] Tamaki K, Lo H-K, Wang W and Lucamarini M 2018 arXiv:1805.05511
[30] Ma X, Zeng P and Zhou H 2018 *Phys. Rev.* X **8** 031043
[31] Cui C *et al* 2019 *Phys. Rev. Appl.* **11** 034053
[32] Lin J and Lütkenhaus N 2018 *Phys. Rev.* A **98** 042332
[33] Curty M, Azuma K and Lo H-K 2018 arXiv:1807.07667
[34] Minder M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2019 *Nat. Photon.* **13** 334–8
[35] Liu Y *et al* 2019 arXiv:1902.06268
[36] Zhong X, Hu J, Curty M, Qian L and Lo H-K 2019 arXiv:1902.10209
[37] Lucamarini M 2018 *8th Int. Conf. on Quantum Cryptography (QCrypt'2018) (Shanghai, China)* http://2018.qcrypt.net
[38] Hwang W-Y 2003 *Phys. Rev. Lett.* **91** 057901
[39] Lo H-K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[40] Wang X-B 2005 *Phys. Rev. Lett.* **94** 230503
[41] Curty M, Xu F, Cui W, Lim C, Tamaki K and Lo H-K 2014 *Nat. Commun.* **5** 3732
[42] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[43] Wang W, Xu F and Lo H-K 2018 arXiv:1807.03466
[44] Rosenberg D *et al* 2009 *New J. Phys.* **11** 045009

D Asymmetric twin-field quantum key distribution

Title:	Asymmetric twin-field quantum key distribution
Authors:	Federico Grasselli, Álvaro Navarrete and Marcos Curty
Journal:	New Journal of Physics
Impact factor:	3.783 (2018)
Date of submission:	30 July 2019
Publication status:	Published
Contribution by FG:	First author (input approx. 80%)

This publication corresponds to reference [GNC19]. A summary of its content is presented in chapter 7.

This research project represents a natural continuation of the work in [GC19] and was triggered by MC. I derived the new analytical yields bounds contained in the paper and all the other analytical formulas reported therein. I also performed all the numerical simulations with new Mathematica code written by me. I obtained all the plots in the paper except for figure C1, which was obtained by AN together with the associated discussion in appendix C. AN provided help in polishing the presentation of the contour plots and also provided useful comments on the plots' presentation. I had regular discussions with AN on the development of the project. MC provided suggestions on the presentation of the results and guided the general direction of the project. The final results were discussed by all authors. I wrote the majority of the manuscript and AN complemented some parts of it. MC proofread the paper and improved it with his comments.

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
30 July 2019

REVISED
7 October 2019

ACCEPTED FOR PUBLICATION
28 October 2019

PUBLISHED
14 November 2019

Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Asymmetric twin-field quantum key distribution

Federico Grasselli[1,3], Álvaro Navarrete[2] and Marcos Curty[2]

[1] Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225, Düsseldorf, Germany
[2] EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo, E-36310, Spain
[3] Author to whom any correspondence should be addressed.

E-mail: federico.grasselli@hhu.de and anavarrete@com.uvigo.es

Keywords: asymmetric loss, twin-field quantum key distribution (QKD), analytical yields bounds, single-photon interference, decoy state, asymmetric QKD, intensity fluctuations

Abstract

Twin-Field (TF) quantum key distribution (QKD) is a major candidate to be the new benchmark for far-distance QKD implementations, since its secret key rate can overcome the repeaterless bound by means of a simple interferometric measurement. Many variants of the original protocol have been recently proven to be secure. Here, we focus on the TF-QKD type protocol proposed by Curty *et al* (2019 *NPJ Quantum Inf.* **5** 64), which can provide a high secret key rate and whose practical feasibility has been demonstrated in various recent experiments. The security of this protocol relies on the estimation of certain detection probabilities (yields) through the decoy-state technique. Analytical bounds on the relevant yields have been recently derived assuming that both parties use the same set of decoy intensities, thus providing sub-optimal key rates in asymmetric-loss scenarios. Here we derive new analytical bounds when the parties use either two, three or four independent decoy intensity settings each. With the new bounds we optimize the protocol's performance in asymmetric-loss scenarios and show that the protocol is robust against uncorrelated intensity fluctuations affecting the parties' lasers.

1. Introduction

Quantum Key Distribution (QKD) [1–5] allows two separated parties (typically called Alice and Bob) to generate identical bit strings with information-theoretic security. Due to the loss in the quantum channel connecting the parties, the performance of point-to-point QKD generally decreases with the distance, being unpractical for far-distance applications. Nonetheless, there have been remarkable efforts towards improving its range of applicability, such as the recent QKD experiments performed over 421 km of optical fiber [6] and over 1000 km of free space in satellite-to-ground links [7, 8]. However, even for the most outstanding far-distance experiments, the secret key rate turns out to be probably too low for commercial purposes. In fact, it has been proven that there exist fundamental limits on the secret key rate that can be extracted from such point-to-point configurations. These limits say that the secret key rate scales linearly with the transmittance of the quantum channel linking the parties, or in other words, that it decreases exponentially with the channel length [9, 10].

Quantum repeaters [11–13] and measurement-device-independent QKD (MDI-QKD) protocols with either quantum memories [14, 15] or with quantum non-demolition measurements [16] are possible theoretical solutions to overcome these limits. Unfortunately, in practice they require a technology that seems to be far from available in the near future. A more realistic solution was proposed recently by Lucamarini *et al* [17]. They devised an MDI-QKD type protocol—called twin-field QKD (TF-QKD)—in which the untrusted central node performs a single-photon interference measurement on the two incoming pulses, causing the key rate to scale with the square-root of the channel transmittance by using simple optical devices. Since the original proposal, several variants of the TF-QKD protocol were proven to be secure [18–23] and some of them were experimentally implemented [24–27].

Here we focus on the TF-QKD scheme proposed in [19]. In this protocol, Alice and Bob use the decoy-state technique to upper bound the detection probabilities associated to various photon-number states (called yields),

© 2019 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft

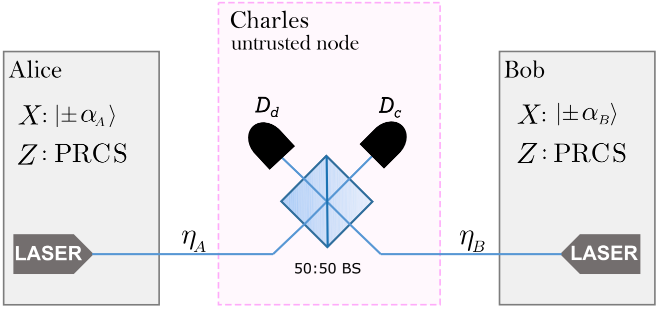

Figure 1. Scheme of the TF-QKD protocol proposed in [19]. After selecting the *X* or *Z* basis randomly, Alice and Bob send optical pulses through a quantum channel to an intermediate node controlled by the untrusted party Charles. In an honest implementation, Charles makes the incoming pulses interfere in a 50:50 beam splitter (BS) and publicly announces which of the two threshold detectors placed at the beam splitter output ports clicks. For the *X* basis, Alice and Bob send coherent states $|\pm\alpha_A\rangle$ and $|\pm\alpha_B\rangle$, respectively. For the *Z* basis, they send PRCS whose intensities are chosen at random from predefined sets.

which are subsequently used to obtain a bound on the phase error rate. Importantly, and in contrast to other solutions [18, 20, 22] which use a post-selection step based on the matching of a global phase, the scheme in [19] pre-selects the value of the global phase and thus it can provide a higher secret key rate. Moreover, the practical feasibility of this scheme has been recently demonstrated in [24, 25, 27]. A complete analysis of the symmetric scenario where both users use the *same* signal intensities and analytically estimate the yields using the *same* decoy intensity settings was performed recently in [28]. However, using the same set of intensities is an optimal strategy only when the quantum channels connecting the users to the central node have approximately the same transmittance. Thus, the bounds derived in [28] are not suitable for several real-world situations in optical networks where the distances between the users and the central node can be notoriously different. Furthermore, assuming that the parties employ exactly the same intensities is problematic even when the losses are symmetric. This is due to the fact that, typically, neither Alice nor Bob can ensure that their lasers emit pulses with a perfectly locked intensity. Instead, their intensities are typically fluctuating randomly and independently from the other party. For these reasons, the use of independent signal intensities and the derivation of yields bounds based on *asymmetric* decoy intensities is crucial for the protocol's security in the presence of intensity fluctuations and for addressing asymmetric-loss scenarios. This idea has already been used to optimize the early MDI-QKD protocols based on two-photon interference in asymmetric-loss scenarios [29] and has recently been applied to another type of TF-QKD protocol in [30]. Moreover, decoy-state based protocols affected by intensity fluctuations have already been studied in [31–34].

In this paper, we address the above-mentioned problems by analyzing the performance of the TF-QKD scheme proposed in [19] in the presence of asymmetric losses and independent laser intensity fluctuations. For this, we derive new analytical bounds on the yields when Alice and Bob use asymmetric intensity settings. In particular, we consider the practical cases where each of Alice and Bob uses two, three and four decoy intensity settings, which are the most efficient solutions for covering long distances. In doing so, we show that the protocol can tolerate highly-asymmetric loss scenarios and is quite robust against intensity fluctuations, thus demonstrating its practicality for realistic network configurations.

The paper is organized as follows. In section 2 we summarize the TF-QKD protocol introduced in [19]. Then, in section 3 we analyze the performance of the aforementioned protocol under the assumption that Alice and Bob use the same signal and decoy intensities. In section 4 we present analytical bounds on the yields when the parties are allowed to use three independent decoy intensity settings. With the derived bounds, we investigate the protocol's performance in section 5 when using independent signal and decoy intensities and in the presence of uncorrelated intensity fluctuations affecting the users' lasers. Finally, in section 6 we present our conclusions. The paper includes also a few Appendixes with additional calculations, including the analytical bounds on the yields when each of Alice and Bob uses either two or four independent decoy intensity settings.

2. TF-QKD

2.1. Protocol description

In this section we briefly summarize the considered TF-QKD protocol [19]. As shown in figure 1, it consists in both Alice and Bob sending optical pulses through a quantum channel to an untrusted third party, Charles, who is in charge of performing joint measurements on the incoming pulses and announcing the results. The protocol is composed of the following seven steps.

(i) Alice (Bob) chooses the X basis with probability p_x^A (p_x^B) and the Z basis with probability $p_z^A = 1 - p_x^A$ ($p_z^B = 1 - p_x^B$). For the X basis, Alice (Bob) prepares an optical pulse in a coherent state $|(-1)^{b_A}\alpha_A\rangle$ ($|(-1)^{b_B}\alpha_B\rangle$), with b_A (b_B) being a randomly chosen bit and $\alpha_A, \alpha_B \in \mathbb{R}$, for simplicity. For the Z basis, Alice (Bob) prepares an optical pulse in a phase-randomized coherent state (PRCS) ρ_{μ_k} (ρ_{ν_l}) whose intensity μ_k (ν_l) is chosen from a set $\mathcal{S}_A = \{\mu_k\}_k$ ($\mathcal{S}_B = \{\nu_l\}_l$) with probability p_k (p_l).

(ii) Both Alice and Bob send their pulses to an intermediate untrusted node, Charles, through optical channels with transmittances η_A and η_B, respectively, in a synchronized manner.

(iii) Charles interferes the incoming pulses in a 50:50 beam splitter, followed by two threshold detectors associated with the constructive (detector D_c) and destructive (detector D_d) interference, respectively.

(iv) Charles announces the measurement outcomes k_c and k_d of the detectors D_c and D_d, respectively, with $k_c = 1$ ($k_d = 1$) corresponding to a click event and $k_c = 0$ ($k_d = 0$) corresponding to a no-click event.

(v) Alice and Bob reveal a small fraction of the bits b_A (b_B) collected from those events when both parties chose the X basis and Charles reported a click only in one detector ($k_c + k_d = 1$) to estimate the bit error rate. Their raw keys consist on the remaining undisclosed bits. Also, Bob flips all the bits b_B collected when the click occurred in D_d.

(vi) Alice and Bob publicly announce the intensities used in all the events when both chose the Z basis, and they use that information to estimate the phase error rate.

(vii) Alice and Bob apply error correction and privacy amplification techniques to their raw keys to distill two identical secret keys.

2.2. Secret key rate

The asymptotic secret key rate of the protocol described above is lower bounded by [19]

$$R \geqslant \max\{R_X^{\Omega_c}, 0\} + \max\{R_X^{\Omega_d}, 0\}, \tag{1}$$

where R_X^{Ω} is a lower bound on the secret key rate that Alice and Bob can obtain from the event $\Omega \in \{\Omega_c, \Omega_d\}$, being $\Omega_c \equiv (k_c = 1 \wedge k_d = 0)$ and $\Omega_d \equiv (k_c = 0 \wedge k_d = 1)$. This lower bound is given by

$$R_X^{\Omega} = p_x^A p_x^B p_X(\Omega)[1 - h_2(e_{Z,\Omega}^{\mathrm{upp}}) - fh_2(e_{X,\Omega})], \tag{2}$$

where $p_X(\Omega) = \frac{1}{4}\sum_{b_A b_B} p_X(\Omega|b_A, b_B)$ is the conditional probability that the event Ω occurs given that Alice and Bob select the X basis, $e_{Z,\Omega}^{\mathrm{upp}}$ is an upper bound on the phase error rate, $e_{X,\Omega}$ is the bit error rate, f is the reconciliation efficiency of the error correction process and $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. Note that in the asymptotic scenario, which is the scenario we consider in this work, we assume for simplicity that $p_x^A = p_x^B \approx 1$. The upper bound on the phase error rate, $e_{Z,\Omega}^{\mathrm{upp}}$, is given by [19]:

$$e_{Z,\Omega}^{\mathrm{upp}} \times p_X(\Omega) = \left(\sum_{n,m\in 2\mathbb{N}^0}^{\infty} c_{n,m}\sqrt{Y_{nm}^{\Omega}}\right)^2 + \left(\sum_{n,m\in 2\mathbb{N}^0+1}^{\infty} c_{n,m}\sqrt{Y_{nm}^{\Omega}}\right)^2, \tag{3}$$

where $Y_{nm}^{\Omega} \equiv p_{ZZ}(\Omega|n, m)$ is the conditional probability of the event Ω given that Alice and Bob sent n and m photons, respectively, $c_{n,m} = \mathrm{e}^{-\frac{\alpha_A^2+\alpha_B^2}{2}}\frac{\alpha_A^n\alpha_B^m}{\sqrt{n!m!}}$ and $\mathbb{N}^0$ denotes the set of non-negative integers. The yields Y_{nm}^{Ω} are not experimentally observed but can be estimated through the decoy-state method [35–37] (see section 4). The bit error rate is given by

$$e_{X,\Omega_c} = p_X(b_A \neq b_B|\Omega_c) = \frac{1}{4}\sum_{b_A\neq b_B}\frac{p_X(\Omega_c|b_A, b_B)}{p_X(\Omega_c)}, \tag{4}$$

$$e_{X,\Omega_d} = p_X(b_A = b_B|\Omega_d) = \frac{1}{4}\sum_{b_A=b_B}\frac{p_X(\Omega_d|b_A, b_B)}{p_X(\Omega_d)}. \tag{5}$$

The values of the bit error rate $e_{X,\Omega}$ and of the probability $p_X(\Omega)$ for a typical channel model are given in appendix A. These are the values we use in our simulations.

3. Symmetric intensities

When analyzing QKD protocols based on a central-node architecture, it is common to consider the symmetric scenario where the transmittances of the channels Alice-Charles and Bob-Charles are equal. This is, however, an

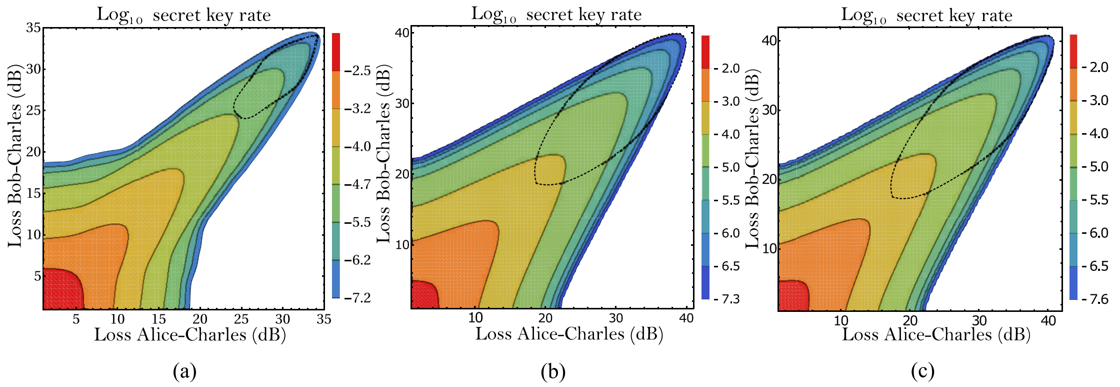

Figure 2. Contour lines for the secret key rate of the TF-QKD protocol introduced in [19] as a function of the channel loss in Alice's and Bob's sides, assuming that both Alice and Bob use the same signal and decoy intensities. Specifically, in (a)–(c) they use two, three and four decoy intensities each, respectively. The black dashed line encloses the loss region where the key rate overcomes the repeaterless bound [10]. We note that for several combinations of losses, it might be beneficial for the parties to increase the loss in one of the channels in order to make them more symmetric, thus maximizing the key rate. The experimental parameters used in the simulations are given in table 1.

Table 1. Experimental parameters used in the simulations. See appendix A for the definitions.

Dark count probability	p_d	10^{-7}
Total polarization misalignment	θ	2%
Phase mismatch	ϕ	2%

unrealistic assumption. In a practical scenario, the loss introduced by the quantum channel Alice-Charles could significantly differ from the loss in the channel Bob-Charles. In this case, the yields bounds obtained by using the decoy-state technique with the same intensity settings for Alice and Bob are not optimal anymore, i.e. they are looser than those obtained when the channel losses are instead symmetric.

Indeed, as already shown in MDI-QKD [29, 38–40], if Alice and Bob use the same intensity settings, they might be in a situation where it is convenient for them to symmetrize the channels losses by increasing the loss in one of the channels, in order to enhance the key rate. In doing so, the intensities of the pulses arriving at the central node are now of similar magnitude, which results in an improvement of the key rate. However, if they use different intensity settings, that is no longer the case [29, 38–40]. The same happens in the TF-QKD scheme introduced in [19]. This is clear from figure 2, where we plot the secret key rate assuming that Alice and Bob use the same set of two, three and four decoy intensities. The plots are obtained by using the analytical yields bounds for the symmetric-intensities scenario derived in [28]. The experimental parameters used for the simulations are given in table 1 and the corresponding channel model is given in appendix A.

In figure 2, the key rate is optimized over the signal intensity $\alpha_A^2 = \alpha_B^2$ and over the strongest decoy intensity (assumed to be equal for the two parties), while the other decoy intensities are fixed to the same values for both parties. As a matter of fact, after having observed that in the asymptotic scenario the optimal values of the weaker decoy intensities tend to be as small as possible regardless of the losses in the two channels, we fixed them to reasonably low values in the key rate optimization. More precisely: the weakest decoy intensities of Alice and Bob in the two-, three- and four-decoy case are fixed to 10^{-5}; the second-to-the-weakest decoy intensities in the three- and four-decoy case are both fixed to 10^{-4}; and the third-to-the-weakest decoy intensities in the four-decoy case are fixed to 10^{-3}. The resulting key rate in both the three- and four-decoy case basically reproduces the rate one would obtain when optimizing even on the weaker decoy intensities [28]. In the two-decoy case, however, the key rate can be enhanced further by decreasing the value of the weakest decoy intensity, as explained in appendix E. The disadvantage of using symmetric signal and decoy intensity settings is clear in all the two-, three- and four-decoy cases, since increasing the loss in one of the channels can lead to an increase of the key rate in asymmetric-loss scenarios.

Furthermore, as already mentioned in the introduction, assuming that Alice and Bob are using exactly the same intensities is not realistic in most experimental implementations [25–27] due to the intensity fluctuations on the transmitters' lasers. The effect of intensity fluctuations was already considered in [28] under the assumption that the fluctuations are correlated among the two parties, which is satisfied in the experiment reported in [24], but does not hold in general.

4. Asymmetric intensities

In order to enhance the protocol's performance in the presence of asymmetric losses and to investigate uncorrelated intensity fluctuations, in this work we derive analytical upper bounds on the yields for the two-, three- and four-decoy scenarios with *independent* intensity settings for Alice and Bob. We note that the use of three or four decoy intensity settings is already enough to obtain a secret key rate close to the one that could be achieved with infinite decoy intensity settings [19, 28]. The derivation of the yields bounds for different decoy intensity settings is presented in appendix F (two-decoy scenario), appendix G (three-decoy scenario) and appendix H (four-decoy scenario). However, for illustration purposes, we present in this section the resulting upper bounds for the three-decoy case.

According to the TF-QKD protocol [19] summarized in section 2—when both parties choose the Z basis—Alice prepares a PRCS whose intensity belongs to the set $\{\mu_0, \mu_1, \mu_2\}$, with $\mu_0 > \mu_1 > \mu_2$. Analogously, Bob prepares a state whose intensity is instead drawn from the set $\{\nu_0, \nu_1, \nu_2\}$, with $\nu_0 > \nu_1 > \nu_2$. The key assumption of the decoy-state method is that the yields are independent of the chosen intensities and are thus subjected to the following four equality constraints:

$$\tilde{Q}^{k,l} \equiv \mathrm{e}^{\mu_k+\nu_l} Q^{k,l} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!} {\mu_k}^n {\nu_l}^m \quad k, l \in \{0, 1, 2\}, \tag{6}$$

where $Q^{k,l}$ is the gain in the Z basis given that Alice and Bob choose intensities μ_k and ν_l, respectively. Note that we omit here and in what follows, for readability, the dependency of the variables with Ω. Being probabilities, the yields are additionally subjected to the inequality constraints:

$$0 \leqslant Y_{nm} \leqslant 1 \quad \forall\, n, m. \tag{7}$$

By properly combining the constraints (6) with a procedure similar to Gaussian elimination, we can obtain analytical upper bounds on the yields Y_{00}, Y_{11}, Y_{22}, Y_{02}, Y_{04}, Y_{20}, Y_{40}, Y_{13} and Y_{31}. The other yields are trivially upper bounded by one. The upper bounds are then inserted in the expression for the phase error rate (3), which can be rewritten as

$$\begin{aligned} e_{Z,\Omega}^{\mathrm{upp}} \times p_X(\Omega) = &(c_{0,0}\sqrt{Y_{00}^{\Omega}} + c_{0,2}\sqrt{Y_{02}^{\Omega}} + c_{2,0}\sqrt{Y_{20}^{\Omega}} + c_{2,2}\sqrt{Y_{22}^{\Omega}} + c_{0,4}\sqrt{Y_{04}^{\Omega}} + c_{4,0}\sqrt{Y_{40}^{\Omega}} + \Delta_{\mathrm{even}})^2 \\ &+ (c_{1,1}\sqrt{Y_{11}^{\Omega}} + c_{1,3}\sqrt{Y_{13}^{\Omega}} + c_{3,1}\sqrt{Y_{31}^{\Omega}} + \Delta_{\mathrm{odd}})^2, \end{aligned} \tag{8}$$

where $\Delta_{\mathrm{even}} = \sum_{(n,m)\in S_0}^{\infty} c_{n,m}$ ($\Delta_{\mathrm{odd}} = \sum_{(n,m)\in S_1}^{\infty} c_{n,m}$), being S_0 (S_1) the subset of $2\mathbb{N}^0$ ($2\mathbb{N}^0 + 1$) which only includes the (n, m) pairs of those yields that are being trivially upper bounded by one. In doing so, we can obtain a fully analytical expression of the asymptotic secret key rate (1). In what follows, we present the resulting upper bounds on the aforementioned yields (we refer the reader to appendix G for their derivation). For this, let's consider the most general combination of the nine constraints (6):

$$G_{uv} = \sum_{i,j=0}^{2} c_{i,j} \tilde{Q}^{i,j}. \tag{9}$$

For simplicity, in (9) and also below, we omit the explicit dependence of the coefficients $c_{i,j}$ with the value of u and v. Then, we can obtain an upper bound on the yield Y_{uv} by appropriately choosing the coefficients $c_{i,j}$ that appear in (9).

4.1. Upper bound on Y_{00}

An upper bound on the yield Y_{00} is given by

$$Y_{00}^{U} = \frac{\mu_1\mu_2\nu_1\nu_2 G_{00}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}, \tag{10}$$

where G_{00} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.54).

4.2. Upper bound on Y_{11}

An upper bound on the yield Y_{11} is given by

$$Y_{11}^U = \frac{G_{11}(\mu_1 + \mu_2)(\nu_1 + \nu_2)}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)} + \frac{Y_{13}^U}{6}(\nu_1\nu_2 + \nu_0\nu_1 + \nu_2\nu_0) + \frac{Y_{31}^U}{6}(\mu_1\mu_2 + \mu_0\mu_1 + \mu_2\mu_0)$$
$$- \frac{\left(e^{\nu_1} - \nu_1 - \frac{\nu_1^2}{2} - \frac{\nu_1^3}{6}\right)(\nu_0^2 - \nu_2^2) + \left(e^{\nu_2} - \nu_2 - \frac{\nu_2^2}{2} - \frac{\nu_2^3}{6}\right)(\nu_1^2 - \nu_0^2) + (e^{\nu_0} - \nu_0 - \frac{\nu_0^2}{2} - \frac{\nu_0^3}{6})(\nu_2^2 - \nu_1^2)}{(\nu_1 - \nu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}$$
$$- \frac{\left(e^{\mu_1} - \mu_1 - \frac{\mu_1^2}{2} - \frac{\mu_1^3}{6}\right)(\mu_0^2 - \mu_2^2) + \left(e^{\mu_2} - \mu_2 - \frac{\mu_2^2}{2} - \frac{\mu_2^3}{6}\right)(\mu_1^2 - \mu_0^2) + \left(e^{\mu_0} - \mu_0 - \frac{\mu_0^2}{2} - \frac{\mu_0^3}{6}\right)(\mu_2^2 - \mu_1^2)}{(\mu_1 - \mu_2)(\mu_0 - \mu_1)(\mu_0 - \mu_2)}, \tag{11}$$

where G_{11} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.16), and where the upper bounds Y_{13}^U and Y_{13}^U are provided below.

4.3. Upper bound on Y_{22}

An upper bound on the yield Y_{22} is given by

$$Y_{22}^U = \frac{4G_{22}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}, \tag{12}$$

where G_{22} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.6).

4.4. Upper bounds on Y_{02} and Y_{04}

The upper bounds on the yields Y_{02} and Y_{04} are given by, respectively,

$$Y_{02}^U = \frac{2G_{02}\mu_1\mu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}, \tag{13}$$

and

$$Y_{04}^U = \frac{24G_{02}\mu_1\mu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_2^2 + \nu_1^2 + \nu_0^2 + \nu_0\nu_1 + \nu_0\nu_2 + \nu_1\nu_2)}, \tag{14}$$

where G_{02} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.28).

4.5. Upper bounds on Y_{20} and Y_{40}

The upper bounds on the yields Y_{20} and Y_{40} are given by, respectively,

$$Y_{20}^U = \frac{2G_{20}\nu_1\nu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}, \tag{15}$$

and

$$Y_{40}^U = \frac{24G_{20}\nu_1\nu_2}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\mu_2^2 + \mu_1^2 + \mu_0^2 + \mu_0\mu_1 + \mu_0\mu_2 + \mu_1\mu_2)}, \tag{16}$$

where G_{20} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.36).

4.6. Upper bound on Y_{13}

An upper bound on the yield Y_{13} is given by

$$\begin{aligned} Y_{13}^U = & \frac{-6(\mu_1 + \mu_2)G_{13}}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_0 + \nu_1 + \nu_2)} \\ & + \frac{6[e^{\nu_2}(\nu_1 - \nu_0) + e^{\nu_1}(\nu_0 - \nu_2) + e^{\nu_0}(\nu_2 - \nu_1)]}{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_1 - \nu_2)(\nu_0 + \nu_1 + \nu_2)} \\ & \times [e^{\mu_2}(\mu_1^2 - \mu_0^2) + e^{\mu_1}(\mu_0^2 - \mu_2^2) + e^{\mu_0}(\mu_2^2 - \mu_1^2) - (\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)], \end{aligned} \tag{17}$$

where G_{13} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.43).

4.7. Upper bound on Y_{31}

An upper bound on the yield Y_{31} is given by

$$\begin{aligned} Y_{31}^{U} = & \frac{-6(\nu_1+\nu_2)G_{31}}{(\mu_0-\mu_1)(\mu_0-\mu_2)(\nu_0-\nu_1)(\nu_0-\nu_2)(\mu_0+\mu_1+\mu_2)} \\ & + \frac{6[\mathrm{e}^{\mu_2}(\mu_1-\mu_0)+\mathrm{e}^{\mu_1}(\mu_0-\mu_2)+\mathrm{e}^{\mu_0}(\mu_2-\mu_1)]}{(\mu_0-\mu_1)(\mu_0-\mu_2)(\mu_1-\mu_2)(\nu_0-\nu_1)(\nu_0-\nu_2)(\nu_1-\nu_2)(\mu_0+\mu_1+\mu_2)} \\ & \times [\mathrm{e}^{\nu_2}(\nu_1^2-\nu_0^2)+\mathrm{e}^{\nu_1}(\nu_0^2-\nu_2^2)+\mathrm{e}^{\nu_0}(\nu_2^2-\nu_1^2)-(\nu_0-\nu_1)(\nu_0-\nu_2)(\nu_1-\nu_2)], \end{aligned} \tag{18}$$

where G_{31} is given by (9) by fixing the $c_{i,j}$ coefficients to those given in (G.47).

5. Simulations

In order to obtain the optimal secret key rate in the asymptotic-key regime, one needs to optimize it over the X basis intensities α_A^2 and α_B^2, and over four, six or eight decoy intensities, depending on the number of decoys used by Alice and Bob. The key rate depends on the decoy intensities through the yields bounds derived in appendices F–H. For instance, for the three-decoy case analyzed in the previous section, we have that the vector of parameters to be optimized is $\vec{p} = (\alpha_A, \alpha_B, \mu_0, \mu_1, \mu_2, \nu_0, \nu_1, \nu_2)$. In order to fairly compare the simulation results with those of the symmetric scenario (figure 2), we use the same experimental parameters given by table 1 and we again fix the weaker decoy intensities to the same symmetric values for Alice and Bob, namely: $\mu_1 = \nu_1 = 10^{-5}$ for the two-decoy case, $\mu_1 = \nu_1 = 10^{-4}$ and $\mu_2 = \nu_2 = 10^{-5}$ for the three-decoy case, $\mu_0 = \nu_0 = 10^{-3}$, $\mu_1 = \nu_1 = 10^{-4}$ and $\mu_2 = \nu_2 = 10^{-5}$ for the four-decoy case. Thus the key rate is actually optimized over $\vec{p} = (\alpha_A, \alpha_B, \mu_0, \nu_0)$ in the two and three-decoy case, and over $\vec{p} = (\alpha_A, \alpha_B, \mu_3, \nu_3)$ in the four-decoy case. As explained in appendix H, note that in the four-decoy case, for convenience of our notation, μ_3 and ν_3 denote the strongest decoy intensities, i.e. we use the ordering $\mu_3 > \mu_0 > \mu_1 > \mu_2$ and $\nu_3 > \nu_0 > \nu_1 > \nu_2$. Although having fixed the weaker decoy intensities to the same values for both parties might seem restrictive in the asymmetric-loss scenario considered here, indeed it is not. As a matter of fact, we observed that the optimal values of the weaker decoy intensities (i.e. μ_1 and ν_1 in the two-decoy case, μ_1, μ_2 and ν_1, ν_2 in the three-decoy case, μ_0, μ_1, μ_2 and ν_0, ν_1, ν_2 in the four-decoy case) tend to be as low as possible, independently of the losses in Alice and Bob's channels. We thus fixed them to symmetric low values that are reasonable from an experimental point of view [24, 25]. We additionally required every non-fixed decoy intensity to be at least one order of magnitude greater than any other fixed decoy intensity of the same scenario, due to practicality reasons in an experiment.

Fixing the decoy intensities reduces the computation complexity of the simulations, which is important since, in contrast to the MDI-QKD scenario [41], the key rate is not, in general, a convex function of $\vec{p}$ (see appendix C). This means that it is not possible to safely use time-efficient optimization methods, such as, for instance, the coordinate descent algorithm [42]. Our optimization is thus carried out by using the built-in global optimization algorithms of Wolfram Mathematica 11.0 [43].

In figure 3 we plot the asymptotic secret key rate as a function of the loss when the parties employ independent signal and decoy intensities, and each party uses either two (figure 3(a)), three (figure 3(b)) or four (figure 3(c)) decoy intensities. In all plots we observe that the improvement given by the use of independent intensities in the asymmetric-loss regions is significant. That is, introducing extra losses in one of the channels does not enhance the key rate any longer, in contrast to figures 2(a)–(c), where the intensities are instead symmetric for the two parties. Interestingly, this substantial improvement is mainly due to the independence of Alice's and Bob's signal intensities, while the independence of the decoy intensities plays a secondary role. In fact, the weaker dependence of the secret key rate on the asymmetry of Alice's and Bob's decoy intensities was recently investigated for specific scenarios and under some approximations in [44]. Nevertheless, allowing Alice and Bob to independently optimize both their signal and decoy intensities can almost double the secret key rate in extremely asymmetric-loss scenarios with respect to the case where only the signal intensities are independently optimized. This is particularly important when the estimation of the phase error rate is poor, like in the two-decoy case. It is also important to mention that, similarly to what happened in section 3, in the two-decoy scenario shown in figure 3(a) the secret key rate can be significantly enhanced by allowing the weakest decoy intensities of Alice and Bob to take lower values (see appendix E for further information). Additionally, by doing so, the trilobal pattern that can be observed in figure 3(a) almost disappears (see figure E1(a)), and the resulting figure looks similar to the three- and four-decoy cases.

The simulations suggest that in order to get a high key rate, it is important that the intensities of the pulses arriving at the central node are of similar magnitude (but not exactly the same), so that a *cleaner* interference occurs. This is clear from figure 4, where we plot the optimal signal and decoy intensities in the three-decoy scenario, as a function of the loss in the channel Alice-Charles and for fixed losses in the channel Bob-Charles.

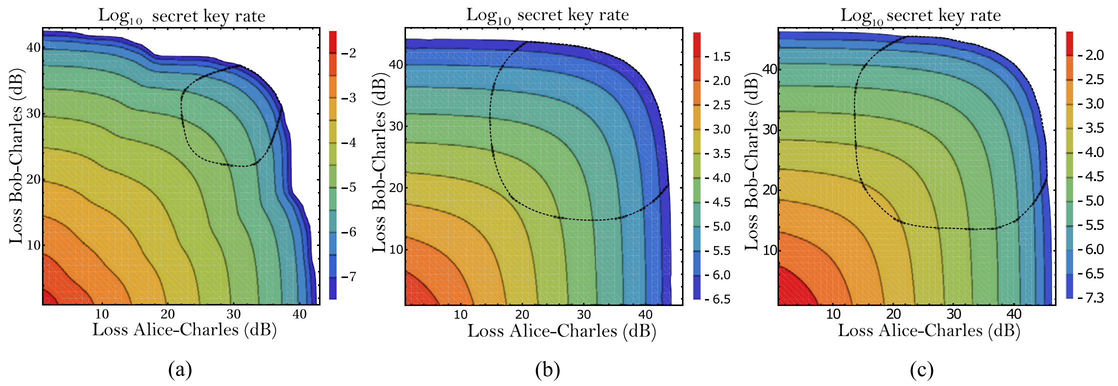

Figure 3. Contour lines for the secret key rate of the TF-QKD protocol introduced in [19] as a function of the channel loss in Alice's and Bob's sides assuming that both Alice and Bob use independent signal and decoy intensities. In (a)–(c), the parties use two, three and four decoy intensities each, respectively. The key rate is never enhanced by increasing the loss in one of the two quantum channels, in contrast to the previous scenario with symmetric intensities (figures 2(a)–(c)). The black dashed line encloses the loss region where the key rate overcomes the repeaterless bound [10]. The experimental parameters used in the simulations are given in table 1.

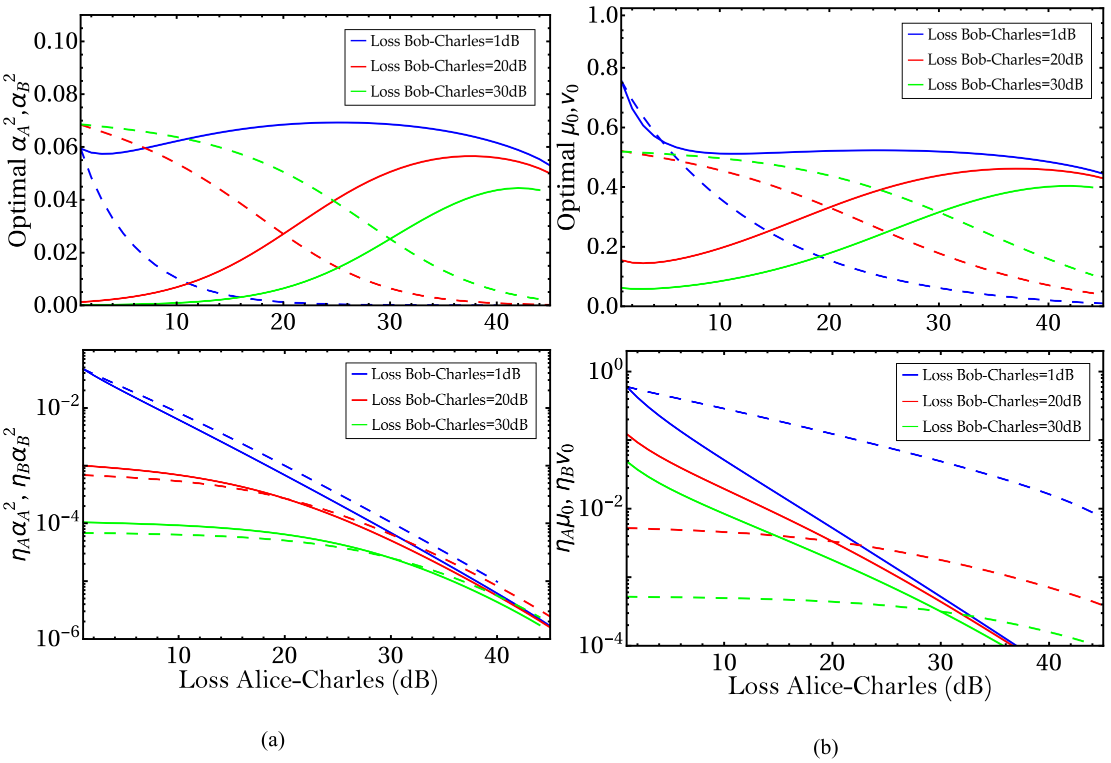

Figure 4. (a) Optimal values of the signal intensities (α_A^2 and α_B^2) and the arriving signal intensities ($\alpha_A^2\eta_A$ and $\alpha_B^2\eta_B$) both for Alice (solid lines) and Bob (dashed lines). (b) Optimal values of the strongest decoy intensities (μ_0 and ν_0) and the arriving strongest decoy intensities ($\mu_0\eta_A$ and $\nu_0\eta_B$) both for Alice (solid lines) and Bob (dashed lines). All the figures are plotted as a function of the loss in the channel Alice-Charles for three different values of the loss in the channel Bob-Charles. The corresponding optimized key rate is given in figure 3(b), where each party has independently three decoy intensities. We observe that it is optimal for the parties to prepare the intensities of their pulses such that the signals arriving to Charles have similar intensities, especially for the X-basis rounds. The experimental parameters used for the simulations are given in table 1.

We note that the optimal signal intensities α_A^2 of Alice (solid lines) become greater than the correspondent ones α_B^2 of Bob (dashed lines) as soon as the loss in Alice's side is greater than in Bob's side. The same happens for the decoy intensities (μ_0 of Alice and ν_0 of Bob) over which the key rate is optimized. Besides, when the losses at Alice's and Bob's sides are equal (symmetric scenario), the optimal values of both the signal and decoy intensities coincide for Alice and Bob, as expected. Moreover, the bottom plots in figure 4 show that the signal intensities *arriving* at the untrusted node, i.e. $\eta_A\alpha_A^2$ and $\eta_B\alpha_B^2$, are very similar to each other, while this is less pronounced in the case of the arriving decoy intensities. This is expected since the signal intensities are used to generate the raw keys. Thus it is optimal to minimize the bit error rate with a clean interference by tuning the signals so that the

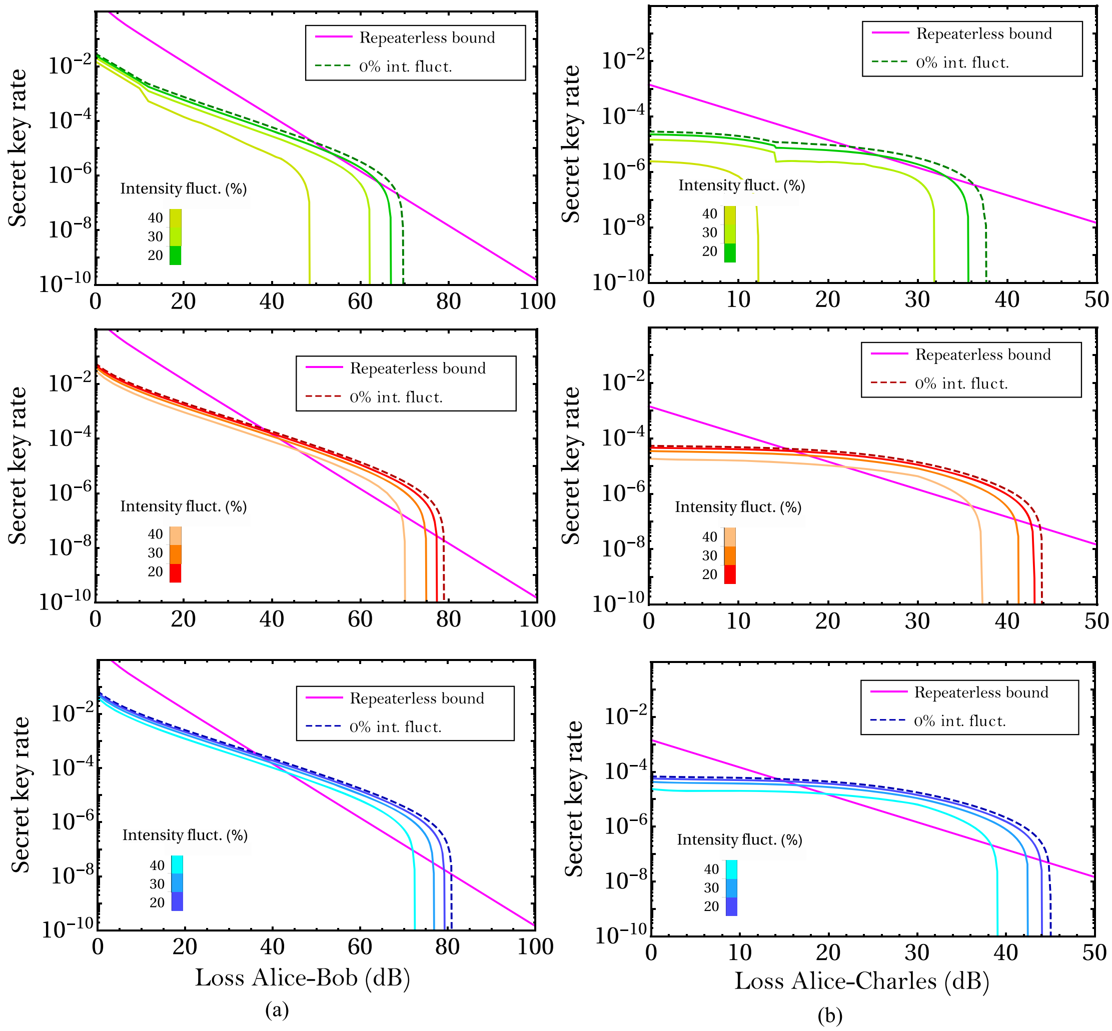

Figure 5. Comparison between the secret key rate with optimal signal and decoys intensities (dashed lines) with the secret key rates affected by increasing intensity fluctuations (solid lines): 20%, 30% and 40% (brighter colors; right to left). The number of decoy intensity settings are two (green lines), three (red lines) and four (blue lines). In (a) the losses at Alice's and Bob's sides are equal (symmetric-loss scenario) while in (b) the loss in the channel Bob-Charles is fixed to 30 dB. We assume that the fluctuations affect each decoy intensity and each signal intensity of both parties in a independent way, i.e. the fluctuations are uncorrelated. The plots show that the TF-QKD protocol is quite robust against intensity fluctuations and that it can beat the repeaterless bound [10] even with 40% intensity fluctuations, when Alice and Bob use either three of four decoy intensities. The weaker decoy intensities have been fixed to the following values: $\mu_1 = \nu_1 = 10^{-5}$ for two decoy intensity settings, $\mu_2 = \nu_2 = 10^{-3}$ and $\mu_1 = \nu_1 = 10^{-2}$ for three decoy intensity settings, and $\mu_2 = \nu_2 = 10^{-3}$, $\mu_1 = \nu_1 = 10^{-2}$ and $\mu_0 = \nu_0 = 10^{-1}$ for four decoy intensity settings. The other experimental parameters are given in table 1.

arriving pulses have similar intensities. Conversely, the decoy pulses are used to indirectly estimate the phase error rate by upper bounding several yields. Because of the complex mathematical structure of such estimation problem, it is not true in general that the optimal phase error rate estimation is achieved by interfering arriving pulses of similar intensity. For completeness, the analogous figures with the optimal arrival intensities in the two- and four-decoy cases are shown in appendix D.

Apart from the general improvement in the secret key rate that the yields bounds derived in this work entail in asymmetric-loss scenarios, the bounds also allow to incorporate uncorrelated intensity fluctuations into the model, guaranteeing security in more realistic conditions. Figure 5 illustrates how taking into account the possible intensity fluctuations at the transmitters' lasers affects the key rate. In particular, the dashed lines are obtained by optimizing the key rate over the signal and decoy intensities (we consider two, three and four decoy intensity settings) in the case of symmetric losses in the two quantum channels (figure 5(a)) and when Bob's loss is fixed to 30 dB (figure 5(b)). We then apply uncorrelated fluctuations of fixed magnitudes (20%, 30% and 40%) on all the signal and decoy intensities of both parties and take the worst-case key rate (solid lines), i.e. the one minimized by letting each intensity independently fluctuate in its fluctuation range. For instance, by fixing the fluctuation magnitude to 30%, every signal ($\alpha_{A,B}^2$) and decoy (μ_k, ν_k) intensities fluctuate independently in the following intervals centered on their optimal values (overlined terms): $\alpha_{A,B}^2 \in [0.7\,\bar{\alpha}_{A,B}^2,\, 1.3\,\bar{\alpha}_{A,B}^2]$,

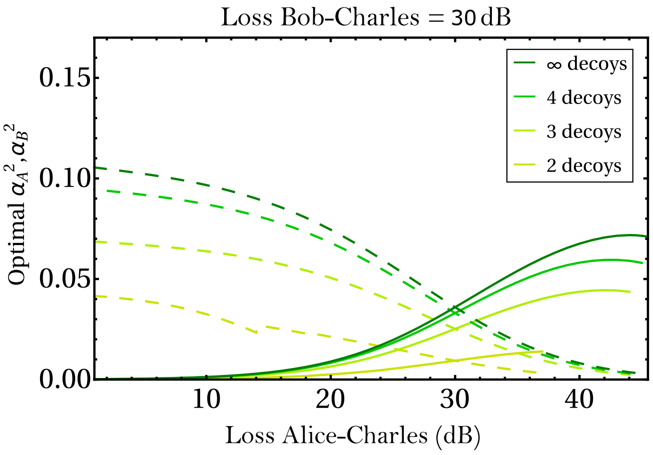

Figure 6. Optimal values of the signal intensities α_A^2 and α_B^2 (solid and dashed lines, respectively) as a function of the loss in the channel Alice-Charles for different levels of accuracy in the estimation of the yields, i.e. assuming that the parties have at their disposal two, three, four and infinite decoy intensity settings (bottom to top). The loss in the channel Bob-Charles is fixed to 30 dB. We observe that the optimal values of the signal intensities used to prepare states in the X basis increase with the number of decoys used in the Z basis. For the infinite decoy case, we assume that Alice and Bob can estimate the yields precisely and we used the theoretical values of the yields, which are given in appendix B. The experimental parameters used for the simulations are given in table 1.

$\mu_k \in [0.7\ \bar{\mu}_k,\ 1.3\ \bar{\mu}_k]$ and $\nu_k \in [0.7\ \bar{\nu}_k,\ 1.3\ \bar{\nu}_k]$. The secret key rate is then minimized over the fluctuations of all intensities constrained in their respective intervals. This effect has already been analyzed in [28] in the case of symmetric losses in the two quantum channels, where the fluctuations are, however, assumed to be perfectly correlated among the two users. This is a quite restrictive assumption, which only occurs in practice in certain experimental implementations based on the use of only one laser [24], but does not hold in general when two lasers are employed [25–27], even in a scenario with symmetric losses. In order to directly compare the effect of *uncorrelated* fluctuations with the results in [28], we fixed the weaker decoy intensities to exactly the same values used in the intensity fluctuations plots of [28], that is: $\mu_1 = \nu_1 = 10^{-5}$ for two decoy intensity settings, $\mu_2 = \nu_2 = 10^{-3}$ and $\mu_1 = \nu_1 = 10^{-2}$ for three decoy intensity settings, and $\mu_2 = \nu_2 = 10^{-3}$, $\mu_1 = \nu_1 = 10^{-2}$ and $\mu_0 = \nu_0 = 10^{-1}$ for four decoy intensity settings. The figures suggest that the protocol is quite robust against intensity fluctuations even when the fluctuations are uncorrelated among the two parties. In fact, the maximal tolerable loss in the overall Alice-Bob channel for both the three and four-decoy scenarios decreases less than 2 dB for a 20% fluctuation of the signal and decoy intensities. Remarkably, even with a fluctuation magnitude of 40% the decrease is still below 10 dB. Regarding the two-decoy case, it is important to mention that the abrupt change that the key rate suffers when considering intensity fluctuations is due to a sudden change in the optimal decoy intensities (see appendix E). In particular, a sudden increase of the optimal decoy intensity directly implies a sudden increase of its fluctuation magnitude in absolute terms What concluded for figure 5(a) also applies to the asymmetric scenario shown in figure 5(b), where the loss in the channel Bob-Charles is fixed to 30 dB.

Finally, it is also interesting to observe how the optimal values for the signal intensities in the X basis depend on the estimation of the yields in the Z basis. Figure 6 shows the variation of the optimal α_A^2 and α_B^2 (X basis) as a function of the loss in the channel Alice-Charles (the loss in the channel Bob-Charles is fixed to 30 dB) for four different levels of accuracy in the estimation of the yields (Z basis). One can see that, when the yields' estimation is not so tight, the X basis intensities α_A^2 and α_B^2 tend to be small in order to reduce the weights $c_{n,m}$ of the yields appearing in (3) and compensate the yields' loose upper bounds. By increasing the number of decoys in the Z basis and thus the tightness of the yields' bounds as well as the number of relevant yields which are non-trivially upper bounded, the optimal values of the signal intensities in the X basis also increase, showing that the optimal signal intensities in the X basis depend on the number of decoy states used in the Z basis.

6. Conclusion

In this paper we have investigated the performance of the TF-QKD protocol proposed in [19] under the realistic condition of asymmetric losses in the quantum channels linking Alice and Bob to the intermediate node. For this, we have derived analytical bounds on the relevant yields that appear in the phase error rate expression when the parties use either two, three or four decoy intensity settings. In contrast to previous results [28], the bounds derived here are valid in the general scenario of independent intensity settings for the two parties, thus optimizing the protocol's performance in the presence of asymmetric losses in the two quantum channels. The simulations show a significant improvement on the secret key rate when using independent signal and decoy intensity settings in several asymmetric-loss scenarios. In particular, the secret key rate is never enhanced by adding fiber in one of the channels in order to symmetrize their losses. Furthermore, we have demonstrated the robustness of the protocol against uncorrelated intensity fluctuations on the transmitters' lasers. These results clearly indicate the suitability of employing the considered TF-QKD protocol in practical QKD networks.

Acknowledgments

This work was supported by the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2017-88243-R, and the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 675662. AN gratefully acknowledges support from a FPU scholarship from the Spanish Ministry of Education.

Appendix A. Asymmetric channel model

Here, we present the expected values of the quantities required to calculate the lower bound on the secure key rate given by (1), in the case of the channel model described in [28]. The only difference is that here the losses in the channels Alice-Charles and Bob-Charles can differ and are modeled with a beamsplitter of transmittance η_A for Alice and η_B for Bob. Note that in this model the phase and polarization misalignments are independent from the channel's transmittance. In order to model them, let $\phi = \delta\pi$ be a phase shift at Bob's side for some parameter δ and let θ_A (θ_B) be the polarization shift angle at Alice's (Bob's) side. Finally, let p_d be the dark-count probability of Charles' detectors, which we assume to be the same for both detectors. Let us define for convenience

$$\gamma = \frac{\eta_A \alpha_A^2 + \eta_B \alpha_B^2}{2}, \tag{A.1}$$

$$\chi(\phi, \theta) = \alpha_A \alpha_B \sqrt{\eta_A \eta_B} \cos(\phi)\cos(\theta), \tag{A.2}$$

where $\theta = \theta_A - \theta_B$. Then it can be shown that the bit error rate $e_{X,\Omega}$ and the probability $p_X(\Omega)$ are given by

$$\mathrm{e}_{X,\Omega} = \frac{\mathrm{e}^{-\chi(\phi,\theta)} - (1 - p_d)\mathrm{e}^{-\gamma}}{\mathrm{e}^{-\chi(\phi,\theta)} + \mathrm{e}^{\chi(\phi,\theta)} - 2(1 - p_d)\mathrm{e}^{-\gamma}}, \tag{A.3}$$

and

$$p_X(\Omega) = \frac{1}{2}(1 - p_d)(\mathrm{e}^{-\chi(\phi,\theta)} + \mathrm{e}^{\chi(\phi,\theta)})\mathrm{e}^{-\gamma} - (1 - p_d)^2\mathrm{e}^{-2\gamma}. \tag{A.4}$$

Finally, the observed gains $Q^{k,l}$ used by Alice and Bob to calculate the upper bounds on the yields Y_{nm} are just the probabilities that the event Ω occurred when Alice and Bob chose intensities μ_k and ν_l for their PRCS. For this channel model it turns out that the gains read:

$$Q^{k,l} = (1 - p_d)[\mathrm{e}^{-(\mu_k\eta_A + \nu_l\eta_B)/2} I_0(\sqrt{\mu_k \nu_l \eta_A \eta_B}\cos(\theta)) - (1 - p_d)\mathrm{e}^{-(\mu_k\eta_A + \nu_l\eta_B)}], \tag{A.5}$$

where $I_0(x)$ is the modified Bessel function of the first kind. Note that due to the balanced redistribution of the incoming photons in the central beam splitter, all the quantities presented here are actually independent of which detector clicked, i.e. they read the same for $\Omega = \Omega_c, \Omega_d$.

In the simulations in the main text we assume that both the total polarization misalignment and phase mismatched are 2%, that is, we select $\theta = 2\arcsin(\sqrt{0.02})$ and $\delta = 0.02$.

Appendix B. Theoretical values for the yields

In order to check the quality of the analytical bounds on the yields, it is useful to compare them with their theoretical values, i.e. the values directly inferred from the channel model and that Alice and Bob would estimate when using an infinite number of decoy intensities. This is used, for instance, in figure 6. The theoretical values of the yields Y_{nm}, according to the channel model presented in appendix A, are given by

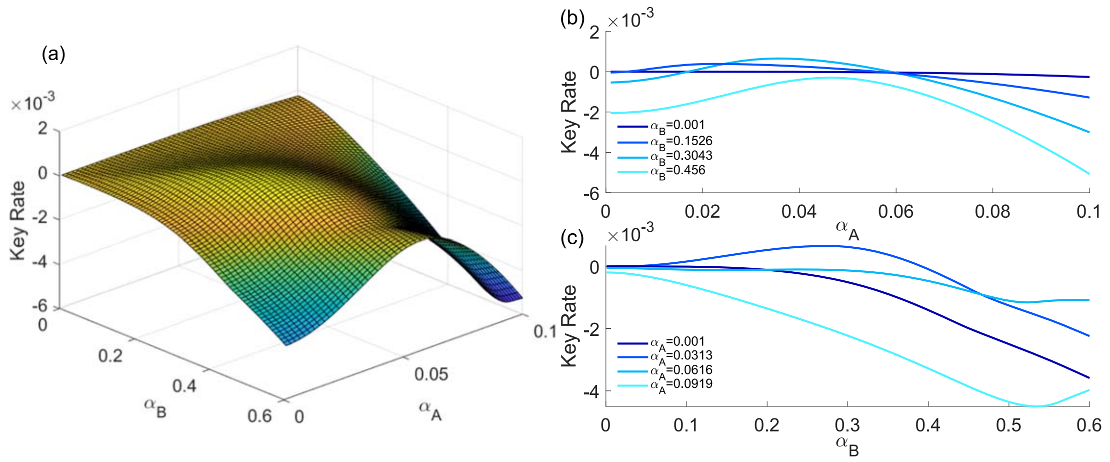

Figure C1. (a) Lower bound on the secret key rate as a function of α_A and α_B. Also, we show in (b) and (c) some specific slices of (a). Here we considered the ∞-decoy scenario, and the losses in Alice's and Bob's channels are 20 dB and 0 dB, respectively. It is easy to note that the secret key rate function is clearly not convex.

$$Y_{nm} = \sum_{k=0}^{n} C^{A}_{n,k} \sum_{t=0}^{m} C^{B}_{m,t} \sum_{i=0}^{k} \binom{k}{i} \sum_{j=0}^{t} \binom{t}{j} \sum_{p=\max(0,i+j-t)}^{\min(k,i+j)} \binom{k}{p} \binom{t}{i+j-p} \tan(\theta_A)^{i+p} \tan(\theta_B)^{i+2j-p} \times (k+t-i-j)!(i+j)! - (1-\eta_A)^n (1-\eta_B)^m, \tag{B.1}$$

where the coefficients $C^{A}_{n,k}$ and $C^{B}_{m,t}$ are given by

$$C^{A}_{n,k} = \frac{1}{k!2^k}\binom{n}{k}\eta_A^k(1-\eta_A)^{n-k}\cos(\theta_A)^{2k},$$
$$C^{B}_{m,t} = \frac{1}{t!2^t}\binom{m}{t}\eta_B^t(1-\eta_B)^{m-t}\cos(\theta_B)^{2t}.$$

Note that the values of the yields are independent of the event Ω.

Appendix C. Non-convexity of the secret key rate with respect to $\vec{p}$

As one can notice from equations (1)–(5), the dependence of the key rate R with its parameters is far from trivial. Here we numerically analyze the convexity of the key rate function $R(\vec{p})$, being $\vec{p}$ the vector of parameters to optimize by the users. It is well-known that this property is noticeably useful since convex functions permit to use efficient optimization methods, which are very important when the length of $\vec{p}$ increases. Unfortunately, it turns out that the key rate function is not convex in general, as shown in figure C1, therefore making many efficient optimization algorithms work poorly.

For instance, if we consider the coordinate descent algorithm [42], it is clear from the plots that it would not reach the optimal value if the starting point is any corner of the α_A–α_B plane and the first variable to optimize is α_B. Note that starting from a corner basically means that, in the first step, the algorithm have to maximize the darkest or the lightest line in figure C1(c), being both maximized when α_B is minimal. This means that, in the next step, the algorithm has always to optimize the darkest line in figure C1(b), which again has its maximum when α_A is minimal. In figure C1, for simplicity, we assume that Alice and Bob can estimate the yields precisely. That is, we assume they use an infinite number of decoy intensities.

Appendix D. Optimal signal and decoy intensities in the two- and four-decoy case

In figure D1 we show the arriving signal and decoy intensities for the two- and four-decoy case, corresponding to the optimal intensities employed in figures 3(a) and (c), respectively. Similarly to the three-decoy case (figure 4), it is optimal for the parties to prepare the intensities of their signal pulses such that the resulting intensities that arrive at Charles are of similar magnitude. This is true for both the two- and the four-decoy case.

Regarding the arriving strongest decoy intensity, the four-decoy scenario resembles again the three-decoy one, while the two-decoy case presents some differences. First of all, in contrast to the three- and four-decoy case, Bob's optimal decoy intensity when the channel loss between Bob and Charles is fixed to 1 dB is constant and equal to the lowest allowed intensity value, i.e. $\nu_0 = 10^{-4}$ (see section 5 for the intensity range in which the

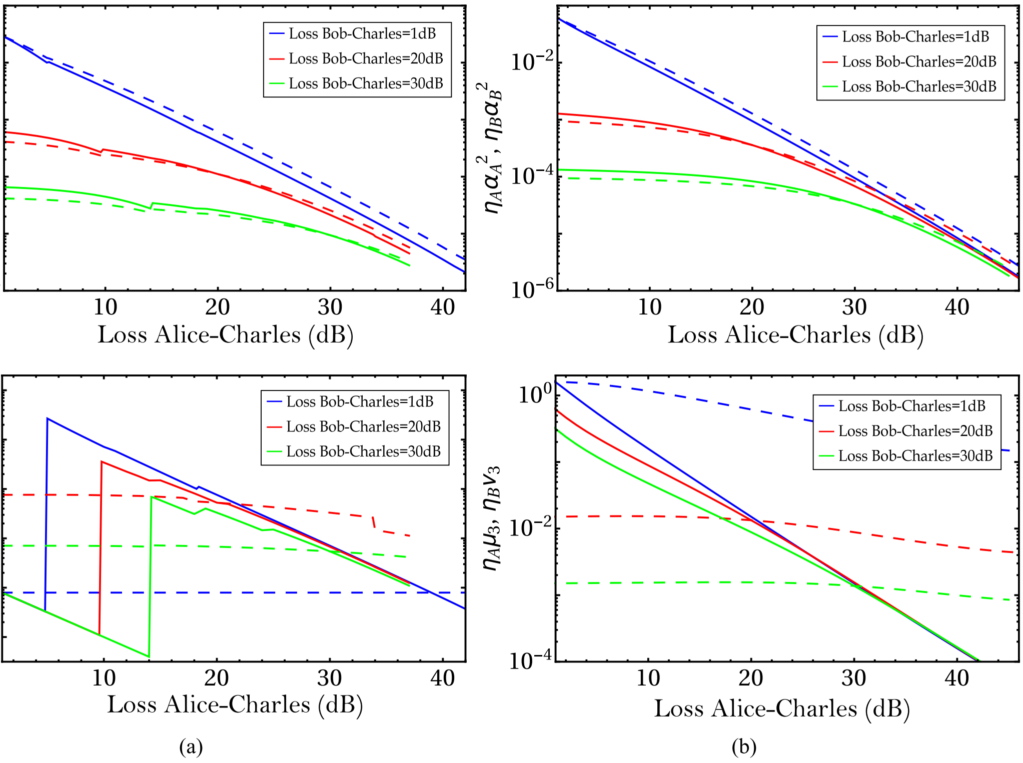

Figure D1. (a) Arriving signal intensities ($\alpha_A^2\eta_A$ and $\alpha_B^2\eta_B$) and arriving strongest decoy intensities ($\mu_0\eta_A$ and $\nu_0\eta_B$) both for Alice (solid lines) and Bob (dashed lines), in the case of two decoy intensities. (b) Arriving signal intensities ($\alpha_A^2\eta_A$ and $\alpha_B^2\eta_B$) and arriving strongest decoy intensities ($\mu_3\eta_A$ and $\nu_3\eta_B$) both for Alice (solid lines) and Bob (dashed lines), in the case of four decoy intensities. All the figures are plotted as a function of the loss in the channel Alice-Charles for three different values of the loss in the channel Bob-Charles. Like in the three-decoy case, we observe that it is optimal for the parties to prepare the intensities of their pulses such that the signals arriving to Charles have similar intensities, especially for the X-basis rounds. The arriving decoy intensities in the two-decoy case present instead discontinuities, that are probably caused by the inherent inefficiency of the yields bounds obtained in this scenario. The experimental parameters used for the simulations are given in table 1.

key rate optimization is performed). Moreover, even Alice's optimal decoy intensity is constant and equal to 10^{-4} at low losses, until it abruptly increases several orders of magnitude and behaves similarly to the three- and four-decoy case at higher losses. The reason for this peculiar behavior does not seem to lie in numerical optimization faults since it has been confirmed by different optimization routines. We also exclude that it is caused by suboptimal analytical bounds on the yields, since it remains present even when using linear programming in bounding the relevant yields. Instead, we believe that the effect of having an extremely low optimal decoy intensity at low losses followed by an abrupt increase at higher losses is inherent in the problem at hand. In particular, the fact that the parties have only two decoy intensity settings prevents them from obtaining sufficiently tight upper bounds on the yields. In other words, there exist relevant decoy intensities combinations for which the parties are unable to bound some yields in a non-trivial way, i.e. with a value strictly smaller than one. This is the reason why we explicitly present every yield upper bound, in the two-decoy case, as given by the minimum between the obtained analytical formula and 1 (see appendix F). The resulting yields bounds are non-smooth functions of the decoy intensities and so is the key rate. In turn, this can lead to discontinuities in the parameters over which the key rate is optimized, as observed.

Finally, we note that the loss thresholds where the discontinuities of the optimal decoy intensities take place, correspond to 'crossing the border' from one lobe to the other in the two-decoy contour plot (figure 3(a)), thus linking the peculiar shape of figure 3(a) to the above effect.

In order to have a better understanding of the special features arising in the two-decoy case discussed above, in appendix E we perform a further key rate optimization in this scenario, but allowing much smaller values for the intensity pulses.

Appendix E. Allowing lower intensities in the two-decoy case

In section 5 we observe a trilobal pattern affecting the two-decoy contour plot (figure 3(a)) and we then link it to the discontinuities affecting the optimal decoy intensities in appendix D. In particular, we observe that for both parties

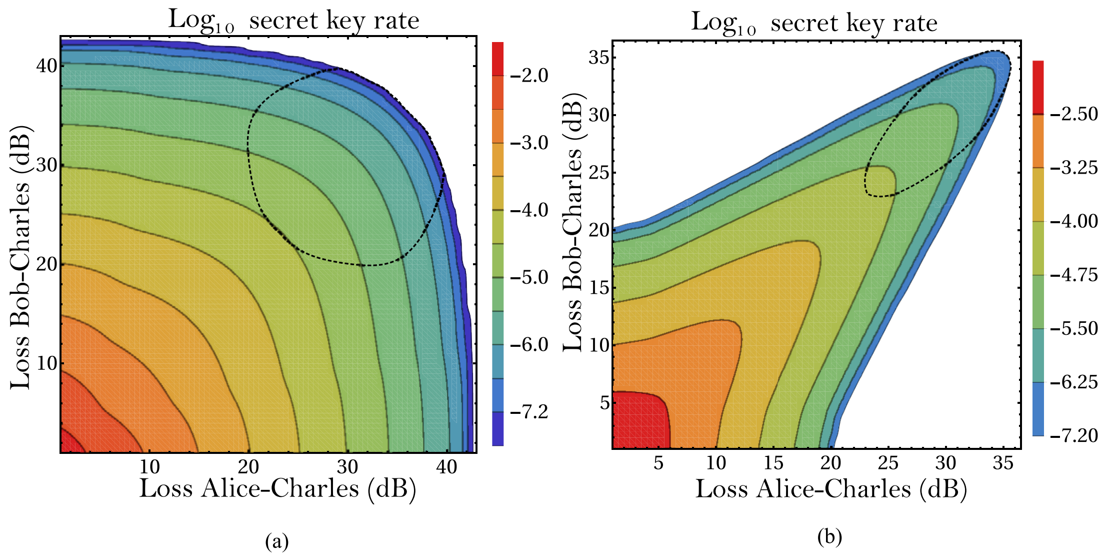

Figure E1. Contour lines for the secret key rate of the TF-QKD protocol introduced in [19] as a function of the channel loss in Alice's and Bob's sides assuming that both Alice and Bob use two decoy intensities each. In (a) the parties are assumed to use independent signal and decoy intensities, while in (b) they use the same signal and decoy intensities. The lowest allowed signal and decoy intensities are set to 10^{-10}. Both contour plots in (a) and (b) are now much more resembling the correspondent ones obtained in the three- and four-decoy case (figures 3 and 2, respectively). The black dashed line encloses the loss region where the key rate overcomes the repeaterless bound [10].

the optimal strongest decoy intensity acquires the *lowest possible* value at low losses (10^{-4}), but then it experiences a sudden increase after a certain loss threshold. In appendix D we argue that such discontinuities are inherent in the problem of optimizing the key rate when the parties have only two decoy intensity settings at their disposal.

In order to check whether these effects are enhanced or caused by the experimentally-reasonable lower bound (10^{-5}) that we imposed on the decoy intensities, we rederive the same plots obtained for the two-decoy case in the main text, but this time we allow both the signal and the decoy intensities to acquire much smaller (but probably unpractical) values. In particular, we fix the lowest decoy intensities to $\mu_1 = 10^{-10}$ for Alice and $\nu_1 = 10^{-10}$ for Bob (opposed to $\mu_1 = 10^{-5}$ and $\nu_1 = 10^{-5}$ of the main text) and we optimize the key rate over the signal intensities $\alpha_A^2 \geqslant 10^{-10}$ and $\alpha_B^2 \geqslant 10^{-10}$ and over the decoy intensity $\mu_0 > 10^{-10}$ for Alice and $\nu_0 > 10^{-10}$ for Bob. In order to make a fair comparison, we use the same experimental parameters used in the main text, given in table 1. Because of the unpractical values allowed for both the signal and decoy intensities, this study is driven by theoretical interest and is not intended to replace the practical one presented in the main text and in appendix D.

In the new contour plots obtained in this scenario (figure E1) the trilobal pattern is barely visible. Indeed, figure E1 now resembles much more the correspondent figures of the three- and four-decoy case (figures 3(b) and (c)). This is readily explained by considering that now we perform the key rate optimization on a wider range of intensities, thus allowing the key rate contour lines to reach areas (i.e. loss combinations) where previously no positive key could be extracted.

Despite the trilobal shape being almost vanished, the optimal decoy intensities (figure E2) still show the same discontinuous behavior already observed in appendix D and acquire the lowest allowed value at low losses. This further confirms that this effect is not due to limits in the numerical optimization or in the analytical bounds, but it is rather inherent in the nature of the problem.

Finally, we also report the effect of intensity fluctuations on the optimized key rate (figure E3). Similarly to the contour plots, having a wider range of intensities in the key rate optimization not only allows one to obtain more non-zero key points, but also has the general effect of making the single plot points more robust to intensity fluctuations. For instance, the optimal values of the decoy intensities at low losses are—in this case—lower than those of the main text (10^{-10} instead of 10^{-4} and 10^{-5}), thus reducing the fluctuations in absolute terms.

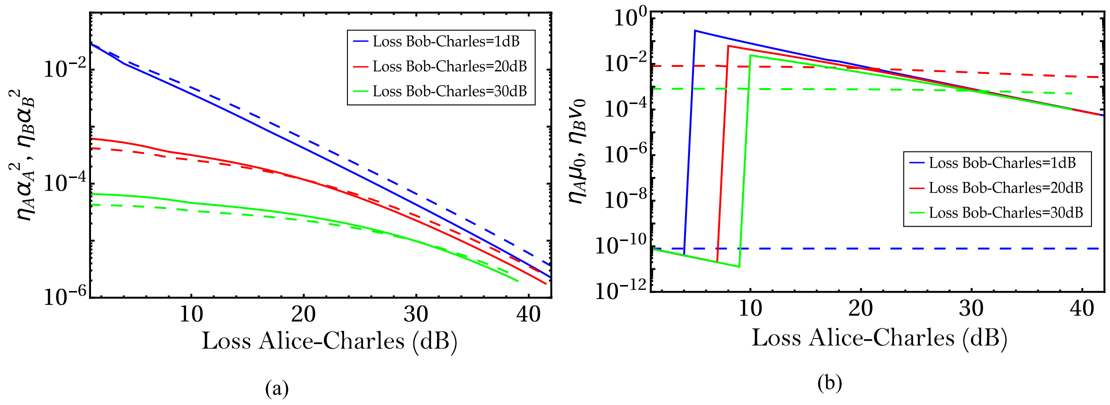

Figure E2. Arriving signal (a) and strongest decoy (b) intensity both for Alice (solid lines) and Bob (dashed lines). The lowest allowed signal and decoy intensities are set to 10^{-10}. The corresponding optimized key rate is given in figure E1(a), where each party has independently two decoy intensities. Like in the case with the higher allowed intensities (figure D1(a)), we still observe discontinuities for the arriving strongest decoy intensities, confirming that the effect is intrinsic to the optimization problem.

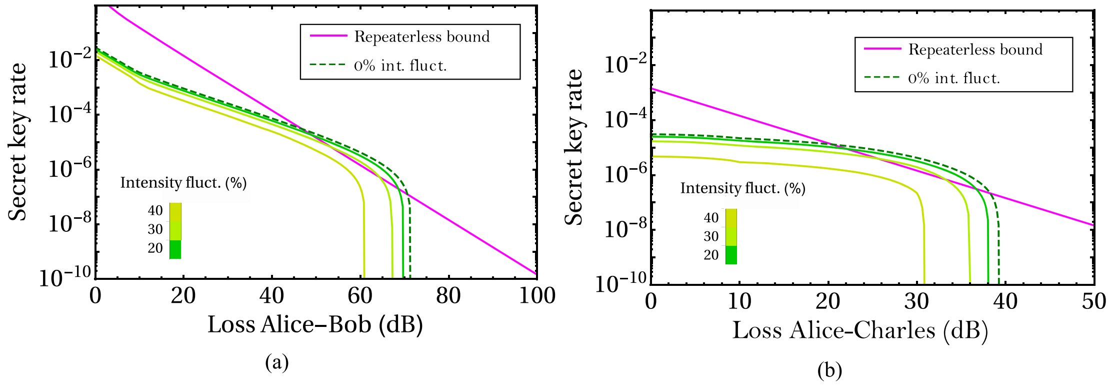

Figure E3. Comparison between the secret key rate with optimal signal and decoys intensities (dashed lines) with the secret key rates affected by increasing intensity fluctuations (solid lines): 20%, 30% and 40% (brighter colors; right to left), when the parties have two decoy intensity settings each. In (a) the losses at Alice's and Bob's sides are equal (symmetric-loss scenario) while in (b) the loss in the channel Bob-Charles is fixed to 30 dB. We assume that the fluctuations affect each decoy intensity and each signal intensity of both parties in a independent way, i.e. the fluctuations are uncorrelated. The lowest allowed signal and decoy intensities are set to 10^{-10}. The plots show that the robustness of the TF-QKD protocol is increased with respect to the case analyzed in the main text (figure 5, where instead the weakest decoy intensities are set to $\mu_1 = \nu_1 = 10^{-5}$).

Appendix F. Upper bounds on the yields with two decoy intensities

Here we derive analytical upper bounds on the yields for the two-decoy scenario with *independent* intensity settings for Alice and Bob. The three- and four-decoy cases follow a similar procedure and are presented in appendices G and H, respectively.

In this scenario each party prepares PRCS with two possible intensities, namely $\{\mu_0, \mu_1\}$ (with $\mu_0 > \mu_1$) for Alice and $\{\nu_0, \nu_1\}$ (with $\nu_0 > \nu_1$) for Bob. The yields are subjected to the following four equality constraints:

$$\tilde{Q}^{k,l} \equiv \mathrm{e}^{\mu_k+\nu_l}Q^{k,l} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}{\mu_k}^n{\nu_l}^m \quad k,\, l \in \{0,\,1\}, \tag{F.1}$$

and to the inequality constraints given in (7).

Below we derive analytical upper bounds on the yields Y_{00}, Y_{11}, Y_{02} and Y_{20}, while the other yields are trivially upper bounded by one. This means that we can rewrite equation (3) as

$$e_{Z,\Omega}^{\text{upp}} \times p_X(\Omega) = (c_{0,0}\sqrt{Y_{00}^{\Omega}} + c_{0,2}\sqrt{Y_{02}^{\Omega}} + c_{2,0}\sqrt{Y_{20}^{\Omega}} + \Delta_{\text{even}})^2 + (c_{1,1}\sqrt{Y_{11}^{\Omega}} + \Delta_{\text{odd}})^2, \tag{F.2}$$

where $\Delta_{\text{even}} = \sum_{(n,m)\in S_0}^{\infty} c_{n,m}$ ($\Delta_{\text{odd}} = \sum_{(n,m)\in S_1}^{\infty} c_{n,m}$), being S_0 (S_1) the subset of $2\mathbb{N}^0$ ($2\mathbb{N}^0 + 1$) which only includes the (n, m) pairs of those yields that are being trivially upper bounded by one.

F.1. Upper bound on Y_{11}

Consider the following combination of gains:

$$G_{11} = \tilde{Q}^{0,0} + \tilde{Q}^{1,1} - (\tilde{Q}^{0,1} + \tilde{Q}^{1,0}) = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\nu_0^m - \nu_1^m). \tag{F.3}$$

The subscript in G_{11} indicates the yield that is going to be bounded with this combination of gains, that is, Y_{11} in this case. In (F.3) the coefficients of the yields Y_{0m} and Y_{n0}, for any n and m, are identically zero. Thus (F.3) can be rewritten as:

$$G_{11} = Y_{11}(\mu_0 - \mu_1)(\nu_0 - \nu_1) + \sum_{\substack{n+m>2 \\ n,m=1}}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\nu_0^m - \nu_1^m). \tag{F.4}$$

Note that Y_{11} is now the yield with the 'highest weight' in (F.4) since it has the largest coefficient. All the yields' bounds presented in this work follow the same philosophy. A valid upper bound for Y_{11} is obtained considering the worst-case scenario for the other yields, taking into account that (7) holds. Since all the yields' coefficients carry the same sign in (F.4), the yield Y_{11} is maximal when all the other yields are minimal. Thus the upper bound on Y_{11} is extracted by setting all the other yields to zero in (F.4):

$$Y_{11}^U = \min\left\{\frac{G_{11}}{(\mu_0 - \mu_1)(\nu_0 - \nu_1)}, 1\right\}, \tag{F.5}$$

where G_{11} is defined in (F.3).

By taking the minimum between the analytical upper bound and 1 we enforce the validity of the inequality constraints (7). This is of particular importance in the two-decoys scenario since there exist relevant combinations of decoy intensities for which the analytical upper bounds would produce a value greater than one. As a consequence, we achieve a tighter estimation of the phase error rate (3) and thus a better performance of the key rate. However, the use of expressions like (F.5) can also affect the smoothness—i.e. the continuity of the first derivative—of the key rate as a function of the decoy intensities. This in turn can lead to discontinuities in the optimal decoy intensities as a function of the losses, as pointed out in appendices D and E.

F.2. Upper bound on Y_{02}

Consider the following combination of gains:

$$G_{02} = \mu_1\tilde{Q}^{0,0} + \mu_0\tilde{Q}^{1,1} - \mu_1\tilde{Q}^{0,1} - \mu_0\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_1\mu_0^n - \mu_0\mu_1^n)(\nu_0^m - \nu_1^m). \tag{F.6}$$

In (F.6) the coefficients of the yields Y_{n0} and Y_{1m} are identically zero. Thus (F.6) can be rewritten as:

$$G_{02} = \sum_{m=1}^{\infty} \frac{Y_{0m}}{m!}(\mu_1 - \mu_0)(\nu_0^m - \nu_1^m) + \sum_{\substack{m=1 \\ n=2}}^{\infty} \frac{Y_{nm}}{n!m!}\mu_0\mu_1(\mu_0^{n-1} - \mu_1^{n-1})(\nu_0^m - \nu_1^m). \tag{F.7}$$

Like in the derivation of the upper bound on Y_{11} in the previous subsection, a valid upper bound for the generic Y_{0m} (where $m \geqslant 1$ is fixed) is obtained by considering the worst-case scenario for the remaining yields in (F.7). More specifically, Y_{0m} is maximal when the yields whose coefficient has the same sign as the Y_{0m}'s coefficient are minimal, and the yields whose coefficient has opposite sign to the Y_{0m}'s coefficient are maximal. Recalling the constraint (7), this means setting all the yields of the form $Y_{0m'}$ (for $m' \neq m$) to zero and Y_{nm} with $n \geqslant 2$ and $m \geqslant 1$ to 1 in (F.7). In so doing, after summing the terms we obtain:

$$G_{02} = \frac{Y_{0m}^U}{m!}(\mu_1 - \mu_0)(\nu_0^m - \nu_1^m) + (\mathrm{e}^{\nu_0} - \mathrm{e}^{\nu_1})(\mu_1\mathrm{e}^{\mu_0} - \mu_0\mathrm{e}^{\mu_1} - \mu_1 + \mu_0), \tag{F.8}$$

which leads to the following upper bound on Y_{0m}, for $m \geqslant 1$:

$$Y_{0m}^U = \min\left\{\frac{m!}{(\mu_1 - \mu_0)(\nu_0^m - \nu_1^m)}[G_{02} - (\mathrm{e}^{\nu_0} - \mathrm{e}^{\nu_1})(\mu_0 - \mu_1 + \mu_1\mathrm{e}^{\mu_0} - \mu_0\mathrm{e}^{\mu_1})], 1\right\}. \tag{F.9}$$

By fixing $m = 2$, one gets the desired upper bound on Y_{02}.

F.3. Upper bound on Y_{20}

In a similar fashion, we consider the following combination of gains:

$$G_{20} = \nu_1\tilde{Q}^{0,0} + \nu_0\tilde{Q}^{1,1} - \nu_0\tilde{Q}^{0,1} - \nu_1\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}(\mu_0^n - \mu_1^n)(\nu_1\nu_0^m - \nu_0\nu_1^m). \tag{F.10}$$

In (F.10) the coefficients of the yields Y_{n1} and Y_{0m} are identically zero. Thus (F.10) can be rewritten as:

$$G_{20} = \sum_{n=1}^{\infty} \frac{Y_{n0}}{n!}(\mu_0^n - \mu_1^n)(\nu_1 - \nu_0)\sum_{\substack{m=2 \\ n=1}}^{\infty} \frac{Y_{nm}}{n!m!}\nu_0\nu_1(\mu_0^n - \mu_1^n)(\nu_0^{m-1} - \nu_1^{m-1}). \tag{F.11}$$

A valid upper bound on Y_{n0} (with $n \geqslant 1$ fixed) is obtained by setting to zero the yields whose coefficient has the same sign as the Y_{n0}'s coefficient, and by setting to 1 the yields whose coefficient has opposite sign to the Y_{n0}'s coefficient. In the case of (F.11), this means setting $Y_{n'0}$ (with $n' \neq n$) to zero and Y_{nm} with $n \geqslant 1$ and $m \geqslant 2$, to one. In this way we obtain:

$$G_{20} = \frac{Y^U_{n0}}{n!}(\mu_0^n - \mu_1^n)(\nu_1 - \nu_0) + (\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_1})(\nu_1\mathrm{e}^{\nu_0} - \nu_0\mathrm{e}^{\nu_1} - \nu_1 + \nu_0), \tag{F.12}$$

which leads to the following upper bound on Y_{n0}, for $n \geqslant 1$:

$$Y^U_{n0} = \min\left\{\frac{n!}{(\nu_1 - \nu_0)(\mu_0^n - \mu_1^n)}[G_{20} - (\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_1})(\nu_0 - \nu_1 + \nu_1\mathrm{e}^{\nu_0} - \nu_0\mathrm{e}^{\nu_1})],\ 1\right\}. \tag{F.13}$$

By fixing $n = 2$, one gets the desired upper bound on Y_{20}.

F.4. Upper bound on Y_{00}

Consider the following combination of gains:

$$G_{00} = \mu_1\nu_1\tilde{Q}^{0,0} + \mu_0\nu_0\tilde{Q}^{1,1} - \mu_1\nu_0\tilde{Q}^{0,1} - \mu_0\nu_1\tilde{Q}^{1,0} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^n\mu_1 - \mu_0\mu_1^n)(\nu_0^m\nu_1 - \nu_0\nu_1^m). \tag{F.14}$$

In (F.14) the coefficients of the yields Y_{1m} and Y_{n1}, for any n and m, are identically zero. Thus (F.14) can be rewritten as:

$$\begin{aligned} G_{00} = {} & Y_{00}(\mu_1 - \mu_0)(\nu_1 - \nu_0) + \nu_0\nu_1(\mu_1 - \mu_0)\sum_{m=2}^{\infty}\frac{Y_{0m}}{m!}(\nu_0^{m-1} - \nu_1^{m-1}) + \mu_0\mu_1(\nu_1 - \nu_0) \\ & \times \sum_{n=2}^{\infty}\frac{Y_{n0}}{n!}(\mu_0^{n-1} - \mu_1^{n-1}) + \mu_0\mu_1\nu_0\nu_1\sum_{n,m=2}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0^{n-1} - \mu_1^{n-1})(\nu_0^{m-1} - \nu_1^{m-1}). \end{aligned} \tag{F.15}$$

As usual we extract an upper bound on Y_{00} by setting to their lowest value the yields whose coefficient has the same sign as the Y_{00}'s coefficient (which correspond to the Y_{nm} with $n,\ m \geqslant 2$), and by setting to their maximum value the yields whose coefficient has opposite sign to the Y_{00}'s coefficient (which correspond to Y_{0m} and Y_{n0}). We know that every yield is trivially bounded by (7). However, in order to derive a tighter bound on Y_{00}, we employ non-trivial bounds for all the yields Y_{nm} with $n + m \leqslant 4$ in (F.15). The upper bound on Y_{00} thus reads:

$$\begin{aligned} Y^U_{00} = {} & \min\left\{\frac{G_{00}}{(\mu_0 - \mu_1)(\nu_0 - \nu_1)} + \frac{1}{2}(Y^U_{02}\nu_0\nu_1 + Y^U_{20}\mu_0\mu_1) + \frac{1}{6}[Y^U_{03}\nu_0\nu_1(\nu_0 + \nu_1) + Y^U_{30}\mu_0\mu_1(\mu_0 + \mu_1)]\right. \\ & + \frac{1}{24}[Y^U_{04}\nu_0\nu_1(\nu_0^2 + \nu_0\nu_1 + \nu_1^2) + Y^U_{40}\mu_0\mu_1(\mu_0^2 + \mu_0\mu_1 + \mu_1^2)] - \frac{\mu_0\mu_1\nu_0\nu_1}{4}Y^L_{22} \\ & - \frac{\nu_1}{\nu_1 - \nu_0}\left(\mathrm{e}^{\nu_0} - 1 - \frac{\nu_0^2}{2} - \frac{\nu_0^3}{6} - \frac{\nu_0^4}{24}\right) + \frac{\nu_0}{\nu_1 - \nu_0}\left(\mathrm{e}^{\nu_1} - 1 - \frac{\nu_1^2}{2} - \frac{\nu_1^3}{6} - \frac{\nu_1^4}{24}\right) \\ & \left. - \frac{\mu_1}{\mu_1 - \mu_0}\left(\mathrm{e}^{\mu_0} - 1 - \frac{\mu_0^2}{2} - \frac{\mu_0^3}{6} - \frac{\mu_0^4}{24}\right) + \frac{\mu_0}{\mu_1 - \mu_0}\left(\mathrm{e}^{\mu_1} - 1 - \frac{\mu_1^2}{2} - \frac{\mu_1^3}{6} - \frac{\mu_1^4}{24}\right),\ 1\right\}, \end{aligned} \tag{F.16}$$

where Y^U_{02}, Y^U_{03} and Y^U_{04} are given by (F.9), Y^U_{20}, Y^U_{30} and Y^U_{40} are given by (F.13) and Y^L_{22} can be bounded from (F.4) when all the other yields are maximal—since all the yields' coefficients have the same sign. Thus the lower bound on Y_{22} is extracted by setting all the other yields to 1 in (F.4):

$$G_{11} = \frac{Y^L_{22}}{4}(\mu_0^2 - \mu_1^2)(\nu_0^2 - \nu_1^2) + \sum_{n,m=1}^{\infty}\frac{\mu_0^n - \mu_1^n}{n!}\frac{\nu_0^m - \nu_1^m}{m!} - \frac{1}{4}(\mu_0^2 - \mu_1^2)(\nu_0^2 - \nu_1^2), \tag{F.17}$$

which leads to the following lower bound on Y_{22}:

$$Y^L_{22} = \max\left\{1 + \frac{4}{(\mu_0^2 - \mu_1^2)(\nu_0^2 - \nu_1^2)}[G_{11} - (\mathrm{e}^{\mu_0} - \mathrm{e}^{\mu_1})(\mathrm{e}^{\nu_0} - \mathrm{e}^{\nu_1})],\ 0\right\}. \tag{F.18}$$

We also note that the upper bounds derived on Y_{04} and Y_{40} in equations (F.9) and (F.13) could be used to improve the estimation of the phase error rate given in by (3). However, it can be shown that the resulting improvement in the secret key rate is very small in this case and we neglect it for simplicity.

Appendix G. Upper bounds on the yields with three decoy intensities

Here we derive the upper bounds on the yields Y_{00}, Y_{11}, Y_{02}, Y_{20}, Y_{22}, Y_{13}, Y_{31}, Y_{04} and Y_{40} presented in section 4.

G.1. Upper bound on Y_{22}

We consider the most general combination of the nine constraints (6):

$$G_{22} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n\nu_j^m\right], \tag{G.1}$$

and require that the terms proportional to Y_{0m}, Y_{1m}, Y_{n0} and Y_{n1} are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\text{removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right) = 0 \quad \forall n \quad \Leftarrow \quad c_{i,0}+c_{i,1}+c_{i,2} = 0 \quad \text{for } i = 0,\,1,\,2 \tag{G.2}$$

$$Y_{n1}\text{removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\nu_j c_{i,j}\right) = 0 \quad \forall n \quad \Leftarrow \quad \nu_0 c_{i,0}+\nu_1 c_{i,1}+\nu_2 c_{i,2} = 0 \quad \text{for } i = 0,\,1,\,2 \tag{G.3}$$

$$Y_{0m}\text{removed: } \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right) = 0 \quad \forall m \quad \Leftarrow \quad c_{0,j}+c_{1,j}+c_{2,j} = 0 \quad \text{for } j = 0,\,1,\,2 \tag{G.4}$$

$$Y_{1m}\text{removed: } \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}\mu_i c_{i,j}\right) = 0 \quad \forall m \quad \Leftarrow \quad \mu_0 c_{0,j}+\mu_1 c_{1,j}+\mu_2 c_{2,j} = 0 \quad \text{for } j = 0,\,1,\,2. \tag{G.5}$$

The linear system of equations given by (G.2)–(G.5) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

$$\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= \frac{\nu_2-\nu_0}{\nu_1-\nu_2},\\
c_{0,2} &= \frac{\nu_0-\nu_1}{\nu_1-\nu_2},\\
c_{1,0} &= \frac{\mu_2-\mu_0}{\mu_1-\mu_2},\\
c_{1,1} &= \frac{(\mu_0-\mu_2)(\nu_0-\nu_2)}{(\mu_1-\mu_2)(\nu_1-\nu_2)},\\
c_{1,2} &= \frac{(\mu_0-\mu_2)(\nu_0-\nu_1)}{(\mu_2-\mu_1)(\nu_1-\nu_2)},\\
c_{2,0} &= \frac{\mu_0-\mu_1}{\mu_1-\mu_2},\\
c_{2,1} &= \frac{(\mu_0-\mu_1)(\nu_0-\nu_2)}{(\mu_1-\mu_2)(\nu_2-\nu_1)},\\
c_{2,2} &= \frac{(\mu_0-\mu_1)(\nu_0-\nu_1)}{(\mu_1-\mu_2)(\nu_1-\nu_2)}.
\end{aligned} \tag{G.6}$$

By substituting the solution for the coefficients $c_{i,j}$ (G.6) back into (G.1) one gets:

$$G_{22} = \sum_{n,m=2}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,n)A_{22}(\nu_0,\,\nu_1,\,\nu_2,\,m)}{(\mu_1-\mu_2)(\nu_1-\nu_2)}, \tag{G.7}$$

where

$$A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,n) \equiv \mu_1^n(\mu_0-\mu_2)+\mu_2^n(\mu_1-\mu_0)+\mu_0^n(\mu_2-\mu_1), \tag{G.8}$$

is the function defined in [28] when obtaining the analogous bound on Y_{22} in the symmetric-intensities scenario (i.e. when the decoy intensities of Alice and Bob are drawn from the same set). Thus we can employ the result from [28] and recast (G.8) as follows:

$$A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,n) = (\mu_0-\mu_2)(\mu_2-\mu_1)\sum_{k=0}^{n-1}\mu_2^k(\mu_0^{n-1-k}-\mu_1^{n-1-k}). \tag{G.9}$$

Of course we can employ this expression also for $A_{22}(\nu_0, \nu_1, \nu_2, m)$ by making the proper substitutions. We will apply this consideration from now on to similar scenarios. By employing (G.9) into (G.7) one gets:

$$G_{22} = \sum_{n,m=2}^{\infty}\frac{Y_{nm}}{n!m!}(\mu_0-\mu_2)(\nu_0-\nu_2)\sum_{k=0}^{n-1}\mu_2^k(\mu_0^{n-1-k}-\mu_1^{n-1-k})\sum_{j=0}^{m-1}\nu_2^j(\nu_0^{m-1-j}-\nu_1^{m-1-j}). \tag{G.10}$$

From (G.10) we deduce that the sign of Y_{nm}'s coefficient is independent of n and m and it is the same for all terms in the sum. Thus a valid upper bound for Y_{22} is obtained by setting all the other yields to zero in (G.10), except for Y_{22}. By doing this, we obtain (12).

G.2. Upper bound on Y_{11}

We consider the most general combination of the nine equality constraints:

$$G_{11} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n \nu_j^m\right], \tag{G.11}$$

and require that the terms proportional to Y_{0m}, Y_{2m}, Y_{n0} and Y_{n2} are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\,\text{removed:}\ \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right) = 0 \quad \forall\, n \quad \Leftarrow \quad c_{i,0} + c_{i,1} + c_{i,2} = 0 \quad \text{for } i = 0,\,1,\,2 \tag{G.12}$$

$$Y_{n2}\,\text{removed:}\ \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\nu_j^2 c_{i,j}\right) = 0 \quad \forall\, n \quad \Leftarrow \quad \nu_0^2 c_{i,0} + \nu_1^2 c_{i,1} + \nu_2^2 c_{i,2} = 0 \quad \text{for } i = 0,\,1,\,2 \tag{G.13}$$

$$Y_{0m}\,\text{removed:}\ \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right) = 0 \quad \forall\, m \quad \Leftarrow \quad c_{0,j} + c_{1,j} + c_{2,j} = 0 \quad \text{for } j = 0,\,1,\,2 \tag{G.14}$$

$$Y_{2m}\,\text{removed:}\ \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}\mu_i^2 c_{i,j}\right) = 0 \quad \forall\, m \quad \Leftarrow \quad \mu_0^2 c_{0,j} + \mu_1^2 c_{1,j} + \mu_2^2 c_{2,j} = 0 \quad \text{for } j = 0,\,1,\,2. \tag{G.15}$$

The linear system of equations given by (G.12)–(G.15) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

$$\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= \frac{\nu_2^2 - \nu_0^2}{\nu_1^2 - \nu_2^2},\\
c_{0,2} &= \frac{\nu_0^2 - \nu_1^2}{\nu_1^2 - \nu_2^2},\\
c_{1,0} &= \frac{\mu_2^2 - \mu_0^2}{\mu_1^2 - \mu_2^2},\\
c_{1,1} &= \frac{(\mu_0^2 - \mu_2^2)(\nu_0^2 - \nu_2^2)}{(\mu_1^2 - \mu_2^2)(\nu_1^2 - \nu_2^2)},\\
c_{1,2} &= \frac{(\mu_0^2 - \mu_2^2)(\nu_0^2 - \nu_1^2)}{(\mu_2^2 - \mu_1^2)(\nu_1^2 - \nu_2^2)},\\
c_{2,0} &= \frac{\mu_0^2 - \mu_1^2}{\mu_1^2 - \mu_2^2},\\
c_{2,1} &= \frac{(\mu_0^2 - \mu_1^2)(\nu_0^2 - \nu_2^2)}{(\mu_1^2 - \mu_2^2)(\nu_2^2 - \nu_1^2)},\\
c_{2,2} &= \frac{(\mu_0^2 - \mu_1^2)(\nu_0^2 - \nu_1^2)}{(\mu_1^2 - \mu_2^2)(\nu_1^2 - \nu_2^2)}.
\end{aligned} \tag{G.16}$$

By substituting the solution for the coefficients $c_{i,j}$ (G.16) back into (G.11) one gets:

$$\begin{aligned}
G_{11} = {} & Y_{11}\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} + \sum_{m=3}^{\infty}\frac{Y_{1m}}{m!}\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)}{(\mu_1 + \mu_2)(\nu_1^2 - \nu_2^2)}A_{11}(\nu_0,\,\nu_1,\,\nu_2,\,m)\\
& + \sum_{n=3}^{\infty}\frac{Y_{n1}}{n!}\frac{(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\nu_1 + \nu_2)(\mu_1^2 - \mu_2^2)}A_{11}(\mu_0,\,\mu_1,\,\mu_2,\,n) + \sum_{n,m=3}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{11}(\mu_0,\,\mu_1,\,\mu_2,\,n)A_{11}(\nu_0,\,\nu_1,\,\nu_2,\,m)}{(\mu_1^2 - \mu_2^2)(\nu_1^2 - \nu_2^2)}.
\end{aligned} \tag{G.17}$$

The function $A_{11}(\mu_0, \mu_1, \mu_2, n)$ is defined in [28] when deriving the analogous bound in the symmetric-intensities scenario. It reads:

$$A_{11}(\mu_0, \mu_1, \mu_2, n) \equiv \mu_1^n(\mu_0^2 - \mu_2^2) + \mu_2^n(\mu_1^2 - \mu_0^2) + \mu_0^n(\mu_2^2 - \mu_1^2), \tag{G.18}$$

and can be recast as:

$$A_{11}(\mu_0, \mu_1, \mu_2, n) = (\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_1 - \mu_0)F(\mu_0, \mu_1, \mu_2, n) \quad \text{for } n \geqslant 3, \tag{G.19}$$

with $F(\mu_0, \mu_1, \mu_2, n)$ being a non-negative quantity independently of the intensities, defined as:

$$F(\mu_0, \mu_1, \mu_2, n) \equiv \sum_{k=0}^{n-3} \mu_2^k \left[(\mu_2 + \mu_0) \sum_{j=0}^{n-3-k} \mu_1^{n-2-k-j}\mu_0^j + \mu_2\mu_0^{n-2-k} \right]. \tag{G.20}$$

By employing the expression (G.19) in (G.17) we obtain:

$$\begin{aligned} G_{11} = {} & Y_{11}\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \\ & + \sum_{m=3}^{\infty} \frac{Y_{1m}}{m!}\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)}(\nu_0 - \nu_2)(\nu_1 - \nu_0)F(\nu_0, \nu_1, \nu_2, m) \\ & + \sum_{n=3}^{\infty} \frac{Y_{n1}}{n!}\frac{(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\nu_1 + \nu_2)(\mu_1 + \mu_2)}(\mu_0 - \mu_2)(\mu_1 - \mu_0)F(\mu_0, \mu_1, \mu_2, n) \\ & + \sum_{n,m=3}^{\infty} \frac{Y_{nm}}{n!m!}\frac{(\mu_0 - \mu_2)(\mu_1 - \mu_0)F(\mu_0, \mu_1, \mu_2, n)(\nu_0 - \nu_2)(\nu_1 - \nu_0)F(\nu_0, \nu_1, \nu_2, m)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)}. \end{aligned} \tag{G.21}$$

By looking at (G.21), we deduce that a valid upper bound on Y_{11} is obtained by setting the yields Y_{1m} and Y_{n1} to their maximum allowed value and by setting to zero the yields Y_{nm}, for $n, m \geqslant 3$. In particular, we use the upper bounds derived in (G.5) and (G.6) to bound Y_{13} and Y_{31}, respectively, while we set to 1 all the other yields Y_{1m} and Y_{n1}, for $n, m \geqslant 4$. In so doing, we obtain:

$$\begin{aligned} G_{11} = {} & Y_{11}^U\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)} \\ & + \frac{Y_{13}^U}{6}\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)}{(\mu_1 + \mu_2)(\nu_1 + \nu_2)}(\nu_0 - \nu_2)(\nu_1 - \nu_0)(\nu_1\nu_2 + \nu_0\nu_1 + \nu_2\nu_0) \\ & + \frac{Y_{31}^U}{6}\frac{(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\nu_1 + \nu_2)(\mu_1 + \mu_2)}(\mu_0 - \mu_2)(\mu_1 - \mu_0)(\mu_1\mu_2 + \mu_0\mu_1 + \mu_2\mu_0) \\ & + \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)}{(\mu_1 + \mu_2)(\nu_1^2 - \nu_2^2)}\sum_{m=4}^{\infty}\left[\frac{\nu_1^m}{m!}(\nu_0^2 - \nu_2^2) + \frac{\nu_2^m}{m!}(\nu_1^2 - \nu_0^2) + \frac{\nu_0^m}{m!}(\nu_2^2 - \nu_1^2)\right] \\ & + \frac{(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\nu_1 + \nu_2)(\mu_1^2 - \mu_2^2)}\sum_{n=4}^{\infty}\left[\frac{\mu_1^n}{n!}(\mu_0^2 - \mu_2^2) + \frac{\mu_2^n}{n!}(\mu_1^2 - \mu_0^2) + \frac{\mu_0^n}{n!}(\mu_2^2 - \mu_1^2)\right]. \end{aligned} \tag{G.22}$$

By isolating the bound on Y_{11} and summing the series, we obtain (11).

G.3. Upper bound on Y_{02} and Y_{04}

We consider the most general combination of the nine equality constraints:

$$G_{02} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n\nu_j^m\right], \tag{G.23}$$

and require that the terms proportional to Y_{1m}, Y_{2m}, Y_{n0} and Y_{n1} are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\text{removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right) = 0 \quad \forall n \quad \Leftarrow \quad c_{i,0} + c_{i,1} + c_{i,2} = 0 \quad \text{for } i = 0, 1, 2 \tag{G.24}$$

$$Y_{n1}\text{removed: } \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\nu_j c_{i,j}\right) = 0 \quad \forall n \quad \Leftarrow \quad \nu_0 c_{i,0} + \nu_1 c_{i,1} + \nu_2 c_{i,2} = 0 \quad \text{for } i = 0, 1, 2 \tag{G.25}$$

$$Y_{1m}\text{removed: } \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}\mu_i c_{i,j}\right) = 0 \quad \forall m \quad \Leftarrow \quad \mu_0 c_{0,j} + \mu_1 c_{1,j} + \mu_2 c_{2,j} = 0 \quad \text{for } j = 0, 1, 2 \tag{G.26}$$

$$Y_{2m}\text{removed: } \sum_{j=0}^{2} \nu_j^m \left(\sum_{i=0}^{2} \mu_i^2 c_{i,j}\right) = 0 \quad \forall m \quad \Leftarrow \quad \mu_0^2 c_{0,j} + \mu_1^2 c_{1,j} + \mu_2^2 c_{2,j} = 0 \quad \text{for } j = 0, 1, 2. \tag{G.27}$$

The linear system of equations given by (G.24)–(G.27) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

$$\begin{aligned} c_{0,0} &= 1, \\ c_{0,1} &= \frac{\nu_2 - \nu_0}{\nu_1 - \nu_2}, \\ c_{0,2} &= \frac{\nu_0 - \nu_1}{\nu_1 - \nu_2}, \\ c_{1,0} &= \frac{\mu_0(\mu_2 - \mu_0)}{\mu_1(\mu_1 - \mu_2)}, \\ c_{1,1} &= \frac{\mu_0(\mu_0 - \mu_2)(\nu_0 - \nu_2)}{\mu_1(\mu_1 - \mu_2)(\nu_1 - \nu_2)}, \\ c_{1,2} &= -\frac{\mu_0(\mu_0 - \mu_2)(\nu_0 - \nu_1)}{\mu_1(\mu_1 - \mu_2)(\nu_1 - \nu_2)}, \\ c_{2,0} &= \frac{\mu_0(\mu_0 - \mu_1)}{\mu_2(\mu_1 - \mu_2)}, \\ c_{2,1} &= \frac{\mu_0(\mu_0 - \mu_1)(\nu_0 - \nu_2)}{\mu_2(\mu_2 - \mu_1)(\nu_1 - \nu_2)}, \\ c_{2,2} &= \frac{\mu_0(\mu_0 - \mu_1)(\nu_0 - \nu_1)}{\mu_2(\mu_1 - \mu_2)(\nu_1 - \nu_2)}. \end{aligned} \tag{G.28}$$

By substituting the solution for the coefficients $c_{i,j}$ (G.28) back into (G.23) one gets:

$$\begin{aligned} G_{02} &= \sum_{m=2}^{\infty} \frac{Y_{0m}}{m!}(-1)\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)A_{22}(\nu_0, \nu_1, \nu_2, m)}{\mu_1\mu_2(\nu_1 - \nu_2)} \\ &+ \sum_{\substack{n=3\\m=2}}^{\infty} \frac{Y_{nm}}{n!m!}(-1)\frac{B_{02}(\mu_0, \mu_1, \mu_2, n)A_{22}(\nu_0, \nu_1, \nu_2, m)}{\mu_1\mu_2(\mu_1 - \mu_2)(\nu_1 - \nu_2)}, \end{aligned} \tag{G.29}$$

where A_{22} is given in (G.8) and B_{02} can be written as follows for $n \geqslant 3$ [28]:

$$B_{02}(\mu_0, \mu_1, \mu_2, n) = \mu_0\mu_1\mu_2(\mu_1 - \mu_2)(\mu_0 - \mu_2)\sum_{k=0}^{n-2} \mu_2^k(\mu_0^{n-2-k} - \mu_1^{n-2-k}). \tag{G.30}$$

We thus conclude that the sign of Y_{0m} and Y_{nm}'s coefficients are always equal in (G.29), regardless of the values of the intensities. Therefore a valid upper bound on Y_{0m}—for $m = 2, 4$—is obtained by setting to zero all the other yields in (G.29). By doing so, we obtain the upper bounds on Y_{02} and Y_{04} given in equations (13) and (14).

G.4. Upper bound on Y_{20} and Y_{40}

We consider the most general combination of the nine equality constraints:

$$G_{20} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n \nu_j^m\right], \tag{G.31}$$

and require that the terms proportional to Y_{0m}, Y_{1m}, Y_{n1} and Y_{n2} are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n1}\text{ removed: } \sum_{i=0}^{2} \mu_i^n \left(\sum_{j=0}^{2} \nu_j c_{i,j}\right) = 0 \quad \forall n \quad \Leftarrow \quad \nu_0 c_{i,0} + \nu_1 c_{i,1} + \nu_2 c_{i,2} = 0 \quad \text{for } i = 0, 1, 2 \tag{G.32}$$

$$Y_{n2}\text{ removed: } \sum_{i=0}^{2} \mu_i^n \left(\sum_{j=0}^{2} \nu_j^2 c_{i,j}\right) = 0 \quad \forall n \quad \Leftarrow \quad \nu_0^2 c_{i,0} + \nu_1^2 c_{i,1} + \nu_2^2 c_{i,2} = 0 \quad \text{for } i = 0, 1, 2 \tag{G.33}$$

$$Y_{0m}\text{ removed: } \sum_{j=0}^{2} \nu_j^m \left(\sum_{i=0}^{2} c_{i,j}\right) = 0 \quad \forall m \quad \Leftarrow \quad c_{0,j} + c_{1,j} + c_{2,j} = 0 \quad \text{for } j = 0, 1, 2 \tag{G.34}$$

$$Y_{1m}\ \text{removed:}\ \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}\mu_i c_{i,j}\right)=0\quad\forall m\quad\Leftarrow\quad \mu_0 c_{0,j}+\mu_1 c_{1,j}+\mu_2 c_{2,j}=0\quad\text{for } j=0,\,1,\,2. \tag{G.35}$$

The linear system of equations given by (G.32)–(G.35) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0}=1$), which reads as follows:

$$\begin{aligned}
c_{0,0}&=1,\\
c_{0,1}&=\frac{\nu_0(\nu_2-\nu_0)}{\nu_1(\nu_1-\nu_2)},\\
c_{0,2}&=\frac{\nu_0(\nu_0-\nu_1)}{\nu_2(\nu_1-\nu_2)},\\
c_{1,0}&=\frac{\mu_2-\mu_0}{\mu_1-\mu_2},\\
c_{1,1}&=\frac{\nu_0(\mu_0-\mu_2)(\nu_0-\nu_2)}{\nu_1(\mu_1-\mu_2)(\nu_1-\nu_2)},\\
c_{1,2}&=\frac{\nu_0(\mu_0-\mu_2)(\nu_0-\nu_1)}{\nu_2(\mu_2-\mu_1)(\nu_1-\nu_2)},\\
c_{2,0}&=\frac{\mu_0-\mu_1}{\mu_1-\mu_2},\\
c_{2,1}&=-\frac{\nu_0(\mu_0-\mu_1)(\nu_0-\nu_2)}{\nu_1(\mu_1-\mu_2)(\nu_1-\nu_2)},\\
c_{2,2}&=\frac{\nu_0(\mu_0-\mu_1)(\nu_0-\nu_1)}{\nu_2(\mu_1-\mu_2)(\nu_1-\nu_2)}.
\end{aligned}\tag{G.36}$$

By substituting the solution for the coefficients $c_{i,j}$ (G.36) back into (G.31) one gets:

$$\begin{aligned}
G_{20}={}&\sum_{n=2}^{\infty}\frac{Y_{n0}}{n!}(-1)\frac{(\nu_0-\nu_1)(\nu_0-\nu_2)A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,n)}{\nu_1\nu_2(\mu_1-\mu_2)}\\
&+\sum_{\substack{n=2\\m=3}}^{\infty}\frac{Y_{nm}}{n!m!}(-1)\frac{A_{22}(\mu_0,\,\mu_1,\,\mu_2,\,n)B_{02}(\nu_0,\,\nu_1,\,\nu_2,\,m)}{\nu_1\nu_2(\mu_1-\mu_2)(\nu_1-\nu_2)},
\end{aligned}\tag{G.37}$$

where A_{22} is given in (G.8) and B_{02} in (G.30). From (G.37) we observe that the sign of Y_{n0} and Y_{nm}'s coefficients are always the same, regardless of the values of the intensities. Therefore a valid upper bound on Y_{n0}—for $n=2{,}4$—is obtained by setting to zero all the other yields in (G.37). By doing so, we obtain the upper bounds on Y_{20} and Y_{40} given in equations (15) and (16).

G.5. Upper bound on Y_{13}

We consider the most general combination of the nine equality constraints:

$$G_{13}=\sum_{i,j=0}^{2}c_{i,j}\tilde{Q}^{i,j}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2}c_{i,j}\mu_i^n\nu_j^m\right],\tag{G.38}$$

and require that the terms proportional to Y_{0m}, Y_{2m}, Y_{n0} and Y_{n1} are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n0}\,\text{removed:}\ \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}c_{i,j}\right)=0\quad\forall n\quad\Leftarrow\quad c_{i,0}+c_{i,1}+c_{i,2}=0\quad\text{for } i=0,\,1,\,2 \tag{G.39}$$

$$Y_{n1}\,\text{removed:}\ \sum_{i=0}^{2}\mu_i^n\left(\sum_{j=0}^{2}\nu_j c_{i,j}\right)=0\quad\forall n\quad\Leftarrow\quad \nu_0 c_{i,0}+\nu_1 c_{i,1}+\nu_2 c_{i,2}=0\quad\text{for } i=0,\,1,\,2 \tag{G.40}$$

$$Y_{0m}\,\text{removed:}\ \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}c_{i,j}\right)=0\quad\forall m\quad\Leftarrow\quad c_{0,j}+c_{1,j}+c_{2,j}=0\quad\text{for } j=0,\,1,\,2 \tag{G.41}$$

$$Y_{2m}\,\text{removed:}\ \sum_{j=0}^{2}\nu_j^m\left(\sum_{i=0}^{2}\mu_i^2 c_{i,j}\right)=0\quad\forall\, m\quad\Leftarrow\quad \mu_0^2 c_{0,j}+\mu_1^2 c_{1,j}+\mu_2^2 c_{2,j}=0\quad \text{for}\ j=0,\,1,\,2. \tag{G.42}$$

The linear system of equations given by (G.39)–(G.42) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0}=1$), which reads as follows:

$$\begin{aligned}
c_{0,0}&=1,\\
c_{0,1}&=\frac{\nu_2-\nu_0}{\nu_1-\nu_2},\\
c_{0,2}&=\frac{\nu_0-\nu_1}{\nu_1-\nu_2},\\
c_{1,0}&=\frac{\mu_2^2-\mu_0^2}{\mu_1^2-\mu_2^2},\\
c_{1,1}&=\frac{(\mu_0^2-\mu_2^2)(\nu_0-\nu_2)}{(\mu_1^2-\mu_2^2)(\nu_1-\nu_2)},\\
c_{1,2}&=\frac{(\mu_0^2-\mu_2^2)(\nu_0-\nu_1)}{(\mu_2^2-\mu_1^2)(\nu_1-\nu_2)},\\
c_{2,0}&=\frac{\mu_0^2-\mu_1^2}{\mu_1^2-\mu_2^2},\\
c_{2,1}&=\frac{(\mu_0^2-\mu_1^2)(\nu_0-\nu_2)}{(\mu_1^2-\mu_2^2)(\nu_2-\nu_1)},\\
c_{2,2}&=\frac{(\mu_0^2-\mu_1^2)(\nu_0-\nu_1)}{(\mu_1^2-\mu_2^2)(\nu_1-\nu_2)}.
\end{aligned} \tag{G.43}$$

By substituting the solution for the coefficients $c_{i,j}$ (G.43) back into (G.38) one gets:

$$G_{13}=\sum_{m=2}^{\infty}\frac{Y_{1m}}{m!}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)A_{22}(\nu_0,\,\nu_1,\,\nu_2,\,m)}{(\mu_1+\mu_2)(\nu_1-\nu_2)}+\sum_{\substack{n=3\\m=2}}^{\infty}\frac{Y_{nm}}{n!m!}\frac{A_{11}(\mu_0,\,\mu_1,\,\mu_2,\,n)A_{22}(\nu_0,\,\nu_1,\,\nu_2,\,m)}{(\mu_1^2-\mu_2^2)(\nu_1-\nu_2)}, \tag{G.44}$$

where A_{22} is given in (G.9) and A_{11} is given in (G.19). We thus conclude that Y_{1m} and Y_{nm}'s coefficients have always opposite sign in (G.44), regardless of the values of the intensities. Therefore a valid upper bound on Y_{13} is obtained by setting to zero all the yields of the form Y_{1m} for $m\neq 3$ and by setting to 1 all the other yields of the form Y_{nm} with $n\geqslant 3$ and $m\geqslant 2$. In so doing, we obtain the following expression:

$$\begin{aligned}
G_{13}={}&\frac{Y_{13}^U}{6}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)(\nu_0-\nu_2)(\nu_2-\nu_1)[\nu_0^2-\nu_1^2+\nu_2(\nu_0-\nu_1)]}{(\mu_1+\mu_2)(\nu_1-\nu_2)}\\
&+\sum_{\substack{n=3\\m=2}}^{\infty}\frac{[\mu_1^n(\mu_0^2-\mu_2^2)+\mu_2^n(\mu_1^2-\mu_0^2)+\mu_0^n(\mu_2^2-\mu_1^2)][\nu_1^m(\nu_0-\nu_2)+\nu_2^m(\nu_1-\nu_0)+\nu_0^m(\nu_2-\nu_1)]}{n!m!(\mu_1^2-\mu_2^2)(\nu_1-\nu_2)},
\end{aligned} \tag{G.45}$$

where we used in the series the original expressions of A_{22} and A_{11} that are given in (G.8) and (G.18), respectively. By summing and rearranging the terms, we obtain the upper bound on Y_{13} given in (17).

G.6. Upper bound on Y_{31}

In a similar fashion to Y_{13}'s bound, one first removes the terms proportional to Y_{0m}, Y_{1m}, Y_{n0} and Y_{n2} from the general combination of the nine gains:

$$G_{31}=\sum_{i,j=0}^{2}c_{i,j}\tilde{Q}^{i,j}=\sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2}c_{i,j}\mu_i^n\nu_j^m\right], \tag{G.46}$$

by properly fixing the coefficients $c_{i,j}$ as follows:

$$\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= \frac{\nu_2^2 - \nu_0^2}{\nu_1^2 - \nu_2^2},\\
c_{0,2} &= \frac{\nu_0^2 - \nu_1^2}{\nu_1^2 - \nu_2^2},\\
c_{1,0} &= \frac{\mu_2 - \mu_0}{\mu_1 - \mu_2},\\
c_{1,1} &= \frac{(\mu_0 - \mu_2)(\nu_0^2 - \nu_2^2)}{(\mu_1 - \mu_2)(\nu_1^2 - \nu_2^2)},\\
c_{1,2} &= \frac{(\mu_0 - \mu_2)(\nu_0^2 - \nu_1^2)}{(\mu_2 - \mu_1)(\nu_1^2 - \nu_2^2)},\\
c_{2,0} &= \frac{\mu_0 - \mu_1}{\mu_1 - \mu_2},\\
c_{2,1} &= \frac{(\mu_0 - \mu_1)(\nu_0^2 - \nu_2^2)}{(\mu_1 - \mu_2)(\nu_2^2 - \nu_1^2)},\\
c_{2,2} &= \frac{(\mu_0 - \mu_1)(\nu_0^2 - \nu_1^2)}{(\mu_1 - \mu_2)(\nu_1^2 - \nu_2^2)}.
\end{aligned} \tag{G.47}$$

Then one substitutes the solution (G.47) back into (G.46) and gets:

$$G_{31} = \sum_{n=2}^{\infty} \frac{Y_{n1}}{n!} \frac{(\nu_0 - \nu_1)(\nu_0 - \nu_2)A_{22}(\mu_0, \mu_1, \mu_2, n)}{(\nu_1 + \nu_2)(\mu_1 - \mu_2)} + \sum_{\substack{n=2\\m=3}}^{\infty} \frac{Y_{nm}}{n!m!} \frac{A_{22}(\mu_0, \mu_1, \mu_2, n)A_{11}(\nu_0, \nu_1, \nu_2, m)}{(\nu_1^2 - \nu_2^2)(\mu_1 - \mu_2)}, \tag{G.48}$$

where A_{22} and A_{11} are given in (G.9) and (G.19), respectively. By noting that the coefficients of the Y_{n1} terms have opposite sign to those of the Y_{nm} terms, we derive an upper bound on Y_{31} by setting to zero all the Y_{n1} yields (for $n \neq 3$) and to 1 all the other ones. The upper bound on Y_{31} is given in (18).

G.7. Upper bound on Y_{00}

We consider the most general combination of the nine equality constraints:

$$G_{00} = \sum_{i,j=0}^{2} c_{i,j}\tilde{Q}^{i,j} = \sum_{n,m=0}^{\infty} \frac{Y_{nm}}{n!m!}\left[\sum_{i,j=0}^{2} c_{i,j}\mu_i^n \nu_j^m\right], \tag{G.49}$$

and require that the terms proportional to Y_{1m}, Y_{2m}, Y_{n1} and Y_{n2} are removed in the combination. We achieve this by imposing proper conditions on the real coefficients $c_{i,j}$:

$$Y_{n1}\text{removed: } \sum_{i=0}^{2} \mu_i^n \left(\sum_{j=0}^{2} \nu_j c_{i,j}\right) = 0 \quad \forall\, n \quad \Leftarrow \quad \nu_0 c_{i,0} + \nu_1 c_{i,1} + \nu_2 c_{i,2} = 0 \quad \text{for } i = 0,\, 1,\, 2 \tag{G.50}$$

$$Y_{n2}\text{removed: } \sum_{i=0}^{2} \mu_i^n \left(\sum_{j=0}^{2} \nu_j^2 c_{i,j}\right) = 0 \quad \forall\, n \quad \Leftarrow \quad \nu_0^2 c_{i,0} + \nu_1^2 c_{i,1} + \nu_2^2 c_{i,2} = 0 \quad \text{for } i = 0,\, 1,\, 2 \tag{G.51}$$

$$Y_{1m}\text{removed: } \sum_{j=0}^{2} \nu_j^m \left(\sum_{i=0}^{2} \mu_i c_{i,j}\right) = 0 \quad \forall\, m \quad \Leftarrow \quad \mu_0 c_{0,j} + \mu_1 c_{1,j} + \mu_2 c_{2,j} = 0 \quad \text{for } j = 0,\, 1,\, 2 \tag{G.52}$$

$$Y_{2m}\text{removed: } \sum_{j=0}^{2} \nu_j^m \left(\sum_{i=0}^{2} \mu_i^2 c_{i,j}\right) = 0 \quad \forall\, m \quad \Leftarrow \quad \mu_0^2 c_{0,j} + \mu_1^2 c_{1,j} + \mu_2^2 c_{2,j} = 0 \quad \text{for } j = 0,\, 1,\, 2. \tag{G.53}$$

The linear system of equations given by (G.50)–(G.53) has a unique solution in the variables $c_{i,j}$ (up to a global factor that we fix by imposing $c_{0,0} = 1$), which reads as follows:

$$
\begin{aligned}
c_{0,0} &= 1,\\
c_{0,1} &= \frac{\nu_0(\nu_2-\nu_0)}{\nu_1(\nu_1-\nu_2)},\\
c_{0,2} &= \frac{\nu_0(\nu_0-\nu_1)}{\nu_2(\nu_1-\nu_2)},\\
c_{1,0} &= \frac{\mu_0(\mu_2-\mu_0)}{\mu_1(\mu_1-\mu_2)},\\
c_{1,1} &= \frac{\mu_0\nu_0(\mu_0-\mu_2)(\nu_0-\nu_2)}{\mu_1\nu_1(\mu_1-\mu_2)(\nu_1-\nu_2)},\\
c_{1,2} &= -\frac{\mu_0\nu_0(\mu_0-\mu_2)(\nu_0-\nu_1)}{\mu_1\nu_2(\mu_1-\mu_2)(\nu_1-\nu_2)},\\
c_{2,0} &= \frac{\mu_0(\mu_0-\mu_1)}{\mu_2(\mu_1-\mu_2)},\\
c_{2,1} &= \frac{\mu_0\nu_0(\mu_0-\mu_1)(\nu_0-\nu_2)}{\mu_2\nu_1(\mu_2-\mu_1)(\nu_1-\nu_2)},\\
c_{2,2} &= \frac{\mu_0\nu_0(\mu_0-\mu_1)(\nu_0-\nu_1)}{\mu_2\nu_2(\mu_1-\mu_2)(\nu_1-\nu_2)}.
\end{aligned} \tag{G.54}
$$

By substituting the solution for the coefficients $c_{i,j}$ (G.43) back into (G.38) one gets:

$$
\begin{aligned}
G_{00} \;=\; &\frac{Y_{00}(\mu_0-\mu_1)(\mu_0-\mu_2)(\nu_0-\nu_1)(\nu_0-\nu_2)}{\mu_1\mu_2\nu_1\nu_2} + \sum_{m=3}^{\infty}\frac{Y_{0m}}{m!}\frac{(\mu_0-\mu_1)(\mu_0-\mu_2)A_{00}(\nu_0,\nu_1,\nu_2,m)}{\mu_1\mu_2\nu_1\nu_2(\nu_1-\nu_2)}\\
&+\sum_{n=3}^{\infty}\frac{Y_{n0}}{n!}\frac{(\nu_0-\nu_1)(\nu_0-\nu_2)A_{00}(\mu_0,\mu_1,\mu_2,n)}{\mu_1\mu_2\nu_1\nu_2(\mu_1-\mu_2)} + \sum_{\substack{n=3\\m=3}}^{\infty}\frac{Y_{nm}}{m!}\frac{A_{00}(\mu_0,\mu_1,\mu_2,n)A_{00}(\nu_0,\nu_1,\nu_2,m)}{\mu_1\mu_2\nu_1\nu_2(\mu_1-\mu_2)(\nu_1-\nu_2)},
\end{aligned} \tag{G.55}
$$

where A_{00} is defined as [28]:

$$
A_{00}(\mu_0,\mu_1,\mu_2,n) \equiv \mu_1^n(\mu_2^2\mu_0-\mu_2\mu_0^2)+\mu_2^n(\mu_0^2\mu_1-\mu_0\mu_1^2)+\mu_0^n(\mu_1^2\mu_2-\mu_1\mu_2^2). \tag{G.56}
$$

Using the result in [28], one can recast the function A_{22} as follows:

$$
A_{00}(\mu_0,\mu_1,\mu_2,n) = \mu_0\mu_1\mu_2(\mu_0-\mu_2)(\mu_1-\mu_2)\sum_{k=0}^{n-2}\mu_2^k(\mu_0^{n-2-k}-\mu_1^{n-2-k}), \tag{G.57}
$$

and notice that all the yields in (G.55) have coefficients with equal sign, regardless of the intensities' values. Hence a valid upper bound on Y_{00} is obtained by setting all the other yields to zero (except for the yield to be bounded) in (G.55). The upper bound on Y_{00} is given in (10).

Appendix H. Upper bounds on the yields with four decoy intensities

In this case each party prepares PRCS with four possible intensities, namely $\{\mu_0, \mu_1, \mu_2, \mu_3\}$ for Alice and $\{\nu_0, \nu_1, \nu_2, \nu_3\}$ for Bob. The yields are then subjected to the following sixteen equality constraints:

$$
\tilde{Q}^{k,l} \equiv e^{\mu_k+\nu_l}Q^{k,l} = \sum_{n,m=0}^{\infty}\frac{Y_{nm}}{n!m!}{\mu_k}^n{\nu_l}^m \quad k,\, l\in\{0,\,1,\,2,\,3\}, \tag{H.1}
$$

and to the inequality constraints given in (7).

Below we derive tighter upper bounds on the yields Y_{04}, Y_{40}, Y_{13} and Y_{31}, since the bounds derived on the yields Y_{00}, Y_{11}, Y_{02}, Y_{20} and Y_{22} in appendix G are already good enough, i.e. bounding them with one additional decoy intensity would not result in a significant improvement of the performance of the protocol. Note that the bounds presented here are not valid when two decoy intensities of the same party have the same value. This case would then reduce to the three decoy intensity case. Thus, without loss of generality, we assume the following ordering within each set of intensities: $\mu_3 > \mu_0 > \mu_1 > \mu_2$ and $\nu_3 > \nu_0 > \nu_1 > \nu_2$.

H.1. Upper bound on Y_{04}

We consider the combination of gains (G.29) that leads to the bound on Y_{04} in the case of three decoy intensity settings:

$$
G_{02}^{0,1,2} = \sum_{n,m}^{\infty}\frac{Y_{nm}}{n!m!}C_{02}^{0,1,2}(n,\,m), \tag{H.2}
$$

where the function $C_{02}^{0,1,2}(n,\ m)$ is defined by the rhs of (G.29), while $G_{02}^{0,1,2}$ is the combination of gains given by (G.23), with the coefficients $c_{i,j}$ of the combination given in (G.28). The subscript indicates the combination of gains to which it refers, while the superscript indicates the decoy intensities that are involved, namely $\{\mu_0, \mu_1, \mu_2\}$ for Alice and $\{\nu_0, \nu_1, \nu_2\}$ for Bob. From (G.3) we know that the terms Y_{n0}, Y_{n1}, Y_{1m} and Y_{2m} are removed in (H.2), i.e. $C_{02}^{0,1,2}(n,\ 0) = C_{02}^{0,1,2}(n,\ 1) = C_{02}^{0,1,2}(1,\ m) = C_{02}^{0,1,2}(2,\ m) = 0$, for any n, m. Now that the parties have at their disposal the fourth decoy intensity (μ_3 for Alice and ν_3 for Bob), one can derive three additional combinations like (H.2) by simply replacing one of the first three intensities with the fourth one:

$$G_{02}^{0,1,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{02}^{0,1,3}(n,\ m), \tag{H.3}$$

$$G_{02}^{0,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{02}^{0,2,3}(n,\ m), \tag{H.4}$$

$$G_{02}^{1,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{02}^{1,2,3}(n,\ m). \tag{H.5}$$

For instance, the combination (H.3) is obtained by replacing $\mu_2 \to \mu_3$ and $\nu_2 \to \nu_3$ in the function $C_{02}^{0,1,2}(n,\ m)$, thus obtaining $C_{02}^{0,1,3}(n,\ m)$. Regarding the rhs, $G_{02}^{0,1,3}$ is obtained by replacing $\mu_2 \to \mu_3$ and $\nu_2 \to \nu_3$ in the coefficients $c_{i,j}$ appearing in the combination $G_{02}^{0,1,2}$, and by making the substitution $\tilde{Q}^{2,l} \to \tilde{Q}^{3,l}$ and $\tilde{Q}^{k,2} \to \tilde{Q}^{k,3}$ on the gains in $G_{02}^{0,1,2}$. In so doing, we obtain three more combinations of gains (H.3)–(H.5) in which the terms $Y_{n0},\ Y_{n1},\ Y_{1m}$ and Y_{2m} are removed.

At this point, we further combine the expressions (H.2), (H.3), (H.4), (H.5) with arbitrary real coefficients $d_{i,j,k}$[4]:

$$\begin{aligned} H_{04} &\equiv d_{0,1,2} G_{02}^{0,1,2} + d_{0,1,3} G_{02}^{0,1,3} + d_{0,2,3} G_{02}^{0,2,3} + d_{1,2,3} G_{02}^{1,2,3} \\ &= \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} [d_{0,1,2} C_{02}^{0,1,2}(n,\ m) + d_{0,1,3} C_{02}^{0,1,3}(n,\ m) + d_{0,2,3} C_{02}^{0,2,3}(n,\ m) + d_{1,2,3} C_{02}^{1,2,3}(n,\ m)], \end{aligned} \tag{H.6}$$

and impose that even the terms Y_{n2} and Y_{3m} are removed:

$$\begin{cases} d_{0,1,2} C_{02}^{0,1,2}(n,\ 2) + d_{0,1,3} C_{02}^{0,1,3}(n,\ 2) + d_{0,2,3} C_{02}^{0,2,3}(n,\ 2) + d_{1,2,3} C_{02}^{1,2,3}(n,\ 2) &= 0 \quad \forall n \\ d_{0,1,2} C_{02}^{0,1,2}(3,\ m) + d_{0,1,3} C_{02}^{0,1,3}(3,\ m) + d_{0,2,3} C_{02}^{0,2,3}(3,\ m) + d_{1,2,3} C_{02}^{1,2,3}(3,\ m) &= 0 \quad \forall m \\ d_{0,1,2} &= 1, \end{cases} \tag{H.7}$$

where we fixed the remaining degree of freedom (global factor on all the $d_{i,j,k}$) by requiring that $d_{0,1,2} = 1$. The solution of the linear system (H.7) reads:

$$\begin{aligned} d_{0,1,2} &= 1 \\ d_{0,1,3} &= \frac{(\mu_0 - \mu_2)(\nu_0 - \nu_2)[\mu_0(\nu_1 - \nu_3) + \mu_1(\nu_3 - \nu_0) + \mu_3(\nu_0 - \nu_1)]}{(\mu_0 - \mu_3)(\nu_0 - \nu_3)[\mu_0(\nu_2 - \nu_1) + \mu_1(\nu_0 - \nu_2) + \mu_2(\nu_1 - \nu_0)]} \\ d_{0,2,3} &= \frac{(\mu_0 - \mu_1)(\nu_0 - \nu_1)[\mu_0(\nu_2 - \nu_3) + \mu_2(\nu_3 - \nu_0) + \mu_3(\nu_0 - \nu_2)]}{(\mu_0 - \mu_3)(\nu_0 - \nu_3)[\mu_0(\nu_1 - \nu_2) + \mu_1(\nu_2 - \nu_0) + \mu_2(\nu_0 - \nu_1)]} \\ d_{1,2,3} &= \frac{\mu_0(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)[\mu_1(\nu_3 - \nu_2) + \mu_2(\nu_1 - \nu_3) + \mu_3(\nu_2 - \nu_1)]}{\mu_1(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\nu_1 - \nu_2)(\nu_1 - \nu_3)[\mu_0(\nu_1 - \nu_2) + \mu_1(\nu_2 - \nu_0) + \mu_2(\nu_0 - \nu_1)]}. \end{aligned} \tag{H.8}$$

By substituting the solution (H.8) back into (H.6) and by rearranging the rhs, one gets a combination of gains where all the terms $Y_{n0},\ Y_{n1},\ Y_{n2},\ Y_{1m},\ Y_{2m}$ and Y_{3m} are removed:

$$H_{04} = \sum_{m=3}^{\infty} \frac{Y_{0m}}{m!} A_{04}(\mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ \nu_0,\ \nu_1,\ \nu_2,\ \nu_3,\ m) + \sum_{\substack{n=4\\ m=3}}^{\infty} \frac{Y_{nm}}{n!m!} B_{04}(\mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ \nu_0,\ \nu_1,\ \nu_2,\ \nu_3,\ n,\ m), \tag{H.9}$$

where:

$$\begin{aligned} &A_{04}(\mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ \nu_0,\ \nu_1,\ \nu_2,\ \nu_3,\ m) \\ &\quad = -\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2) p_{04}(\mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ \nu_0,\ \nu_1,\ \nu_2,\ \nu_3)}{\mu_1 \mu_2 \mu_3 [\nu_0(\mu_1 - \mu_2) - \nu_1(\mu_0 - \mu_2) + \nu_2(\mu_0 - \mu_1)]} \\ &\quad\quad \times \left(\sum_{i_1 \leqslant i_2 \leqslant \ \ldots \ \leqslant i_{m-3}} \nu_{i_1} \nu_{i_2} \cdot \ldots \cdot \nu_{i_{m-3}} \right); \end{aligned} \tag{H.10}$$

[4] Note that we identify such a combination as H_{04} since it appears in bounding Y_{04}. However the elements in the combination, namely $G_{02}^{i,j,k}$, have a different subscript since they are borrowed from the bounds on Y_{02} and Y_{04} with three decoy intensity settings.

$$p_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) = \mu_0[\mu_1(\nu_0 - \nu_1)(\nu_2 - \nu_3) - \mu_2(\nu_0 - \nu_2)(\nu_1 - \nu_3) + \mu_3(\nu_0 - \nu_3) \times(\nu_1 - \nu_2)] + \mu_1[\mu_2(\nu_0 - \nu_3)(\nu_1 - \nu_2) - \mu_3(\nu_0 - \nu_2)(\nu_1 - \nu_3)] + \mu_2\mu_3(\nu_0 - \nu_1)(\nu_2 - \nu_3) \tag{H.11}$$

and

$$B_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, n, m) = -\mu_0\mu_1\mu_2\mu_3\, A_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, m) \times\left(\sum_{i_1\leqslant i_2\leqslant \,\ldots\, \leqslant i_{n-4}} \mu_{i_1}\mu_{i_2}\cdot \ldots\cdot\mu_{i_{n-4}}\right). \tag{H.12}$$

We assume that the indexes in the sums run over the set $\{0, 1, 2, 3\}$ and we define $\sum_{i_1\leqslant i_2\leqslant \,\ldots\, \leqslant i_{m-3}} \nu_{i_1}\nu_{i_2}\cdot \ldots\cdot\nu_{i_{m-3}}|_{m=3} = 1$. From (H.10) and (H.12) we deduce that the coefficients of Y_{0m} and Y_{nm} have always opposite sign, hence the upper bound on Y_{04} is obtained from (H.9) by setting all the yields Y_{0m} (with $m \neq 4$) to zero and the yields Y_{nm} (with $n \geqslant 4,\ m \geqslant 3$) to one. After rearranging the terms, we get the following expression for the upper bound on Y_{04}:

$$Y_{04}^{U} = \frac{24}{A_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, 4)}\left[H_{04} - \sum_{\substack{n=4\\m=3}}^{\infty} \frac{B_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, n, m)}{n!m!}\right], \tag{H.13}$$

where H_{04} is given in the first line of (H.6), the function A_{04} evaluated for $m = 4$ reads:

$$A_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, 4) = -\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_0 + \nu_1 + \nu_2 + \nu_3)p_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3)}{\mu_1\mu_2\mu_3[\nu_0(\mu_1 - \mu_2) - \nu_1(\mu_0 - \mu_2) + \nu_2(\mu_0 - \mu_1)]}, \tag{H.14}$$

and the series of B_{04} sums to:

$$\begin{aligned}
&\sum_{\substack{n=4\\m=3}}^{\infty} \frac{B_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, n, m)}{n!m!}\\
&= \frac{\mu_0\, p_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3)[\nu_2(\mu_0 - \mu_1) - \nu_1(\mu_0 - \mu_2) + \nu_0(\mu_1 - \mu_2)]^{-1}}{(\mu_0 - \mu_3)(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)(\nu_0 - \nu_3)(\nu_1 - \nu_2)(\nu_1 - \nu_3)(\nu_2 - \nu_3)}\\
&\times\left[\left(e^{\mu_0} - \frac{\mu_0^2}{2} - \mu_0 - 1\right)(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)\right.\\
&- \left(e^{\mu_1} - \frac{\mu_1^2}{2} - \mu_1 - 1\right)(\mu_0 - \mu_2)(\mu_0 - \mu_3)(\mu_2 - \mu_3)\\
&+ \left(e^{\mu_2} - \frac{\mu_2^2}{2} - \mu_2 - 1\right)(\mu_0 - \mu_1)(\mu_0 - \mu_3)(\mu_1 - \mu_3)\\
&\left.- \left(e^{\mu_3} - \frac{\mu_3^2}{2} - \mu_3 - 1\right)(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)\right]\\
&\times\left[\left(e^{\nu_0} - \frac{\nu_0^2}{2} - \nu_0 - 1\right)(\nu_1 - \nu_2)(\nu_1 - \nu_3)(\nu_2 - \nu_3)\right.\\
&- \left(e^{\nu_1} - \frac{\nu_1^2}{2} - \nu_1 - 1\right)(\nu_0 - \nu_2)(\nu_0 - \nu_3)(\nu_2 - \nu_3)\\
&+ \left(e^{\nu_2} - \frac{\nu_2^2}{2} - \nu_2 - 1\right)(\nu_0 - \nu_1)(\nu_0 - \nu_3)(\nu_1 - \nu_3)\\
&\left.-\left(e^{\nu_3} - \frac{\nu_3^2}{2} - \nu_3 - 1\right)(\nu_0 - \nu_1)(\nu_0 - \nu_2)(\nu_1 - \nu_2)\right].
\end{aligned} \tag{H.15}$$

We remark that in deriving the bound (H.13) we implicitly assumed that at least one of the following equalities does not hold: $\nu_0 = \mu_0, \nu_1 = \mu_1$ and $\nu_2 = \mu_2$. Indeed, when all three equalities hold (i.e. when Alice and Bob are using the same intensities settings for three out of four decoy pulses) one gets a '$\frac{0}{0}$ form' in the bound expression (H.13). In order to overcome this issue (which is not likely to happen in practice due to intensity fluctuations), we derive an additional upper bound on Y_{04} which is valid in the particular case of: $\nu_0 = \mu_0, \nu_1 = \mu_1$ and $\nu_2 = \mu_2$.

The procedure resembles that used in deriving (H.13). We start by considering the four combinations of gains (H.2), (H.3), (H.4) and (H.5) and we impose the conditions: $\nu_0 = \mu_0, \nu_1 = \mu_1$ and $\nu_2 = \mu_2$. Let us indicate the resulting gains combinations as follows:

$$\tilde{G}_{02}^{0,1,2} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} \tilde{C}_{02}^{0,1,2}(n,\, m), \tag{H.16}$$

$$\tilde{G}_{02}^{0,1,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} \tilde{C}_{02}^{0,1,3}(n,\, m), \tag{H.17}$$

$$\tilde{G}_{02}^{0,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} \tilde{C}_{02}^{0,2,3}(n,\, m), \tag{H.18}$$

$$\tilde{G}_{02}^{1,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} \tilde{C}_{02}^{1,2,3}(n,\, m). \tag{H.19}$$

The tilde symbol above the gains combinations G_{02} and the corresponding yields coefficients C_{02} indicates that we operated the substitutions $\nu_0 \longrightarrow \mu_0, \nu_1 \longrightarrow \mu_1$ and $\nu_2 \longrightarrow \mu_2$ in their original expressions.

We further combine the expressions (H.16), (H.17), (H.18) and (H.19) with arbitrary real coefficients $\tilde{d}_{i,j,k}$:

$$\begin{aligned}\tilde{H}_{04} &\equiv \tilde{d}_{0,1,2}\tilde{G}_{02}^{0,1,2} + \tilde{d}_{0,1,3}\tilde{G}_{02}^{0,1,3} + \tilde{d}_{0,2,3}\tilde{G}_{02}^{0,2,3} + \tilde{d}_{1,2,3}\tilde{G}_{02}^{1,2,3}\\ &= \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!}[\tilde{d}_{0,1,2}\tilde{G}_{02}^{0,1,2}(n,\, m) + \tilde{d}_{0,1,3}\tilde{G}_{02}^{0,1,3}(n,\, m) + \tilde{d}_{0,2,3}\tilde{G}_{02}^{0,2,3}(n,\, m) + \tilde{d}_{1,2,3}\tilde{G}_{02}^{1,2,3}(n,\, m)],\end{aligned} \tag{H.20}$$

and impose that even the terms Y_{n2} and Y_{3m} are removed. The solution for the coefficients $\tilde{d}_{i,j,k}$ reads:

$$\begin{aligned}\tilde{d}_{0,1,2} &= 0\\ \tilde{d}_{0,1,3} &= \mu_3\\ \tilde{d}_{0,2,3} &= -\frac{(\mu_0 - \mu_1)\mu_3}{\mu_0 - \mu_2}\\ \tilde{d}_{1,2,3} &= \frac{\mu_0\mu_3(\mu_0 - \mu_1)(\mu_0 - \mu_3)(\mu_0 - \nu_3)}{\mu_1(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_1 - \nu_3)}.\end{aligned} \tag{H.21}$$

By substituting the solution (H.8) back into (H.6) and by rearranging the rhs, one gets a combination of gains where all the terms $Y_{n0}, Y_{n1}, Y_{n2}, Y_{1m}, Y_{2m}$ and Y_{3m} are removed:

$$\tilde{H}_{04} = \sum_{m=3}^{\infty} \frac{Y_{0m}}{m!}\tilde{A}_{04}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_3,\, m) + \sum_{\substack{n=4\\ m=3}}^{\infty} \frac{Y_{nm}}{n!m!}\tilde{B}_{04}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_3,\, n,\, m), \tag{H.22}$$

where:

$$\begin{aligned}\tilde{A}_{04}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_3,\, m) = &-\frac{(\mu_0 - \mu_1)^2(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_3)(\mu_0 - \nu_3)}{\mu_1\mu_2}\\ &\times\left(\sum_{i_1\leqslant i_2\leqslant \,\ldots\, \leqslant i_{m-3}} \mu_{i_1}\mu_{i_2}\cdot \ldots\cdot\mu_{i_{m-3}}\right)\Bigg|_{\mu_3\longrightarrow\nu_3}\end{aligned} \tag{H.23}$$

and

$$\tilde{B}_{04}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_3,\, n,\, m) = -\mu_0\mu_1\mu_2\mu_3\,\tilde{A}_{04}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_3,\, m) \times \left(\sum_{i_1\leqslant i_2\leqslant \,\ldots\, \leqslant i_{n-4}} \mu_{i_1}\mu_{i_2}\cdot \ldots\cdot\mu_{i_{n-4}}\right). \tag{H.24}$$

We assume that the indexes in the sums run over the set $\{0, 1, 2, 3\}$, we define $\sum_{i_1\leqslant i_2\leqslant \,\ldots\, \leqslant i_{m-3}} \nu_{i_1}\nu_{i_2}\cdot \ldots\cdot\nu_{i_{m-3}}|_{m=3} = 1$ and with $\mu_3 \longrightarrow \nu_3$ in (H.23) we intend that every μ_3 contained in the sum must be replaced with a ν_3.

From (H.23) and (H.24) we deduce that the coefficients of Y_{0m} and Y_{nm} have always opposite sign, hence the upper bound on Y_{04} is obtained from (H.22) by setting all the yields Y_{0m} (with $m \neq 4$) to zero and the yields Y_{nm} (with $n \geqslant 4,\ m \geqslant 3$) to one. After rearranging the terms, we get the following expression for the upper bound on Y_{04} under the conditions $\nu_0 = \mu_0, \nu_1 = \mu_1$ and $\nu_2 = \mu_2$:

$$\tilde{Y}_{04}^{U} = \frac{24}{\tilde{A}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, 4)}\left[\tilde{H}_{04} - \sum_{\substack{n=4\\m=3}}^{\infty}\frac{\tilde{B}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, n, m)}{n!m!}\right], \tag{H.25}$$

where $\tilde{H}_{04}$ is given in the first line of (H.20), the function $\tilde{A}_{04}$ evaluated for $m = 4$ reads:

$$\tilde{A}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, 4) = -\frac{(\mu_0 - \mu_1)^2(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_0 - \mu_3)(\mu_0 - \nu_3)}{\mu_1\mu_2}(\mu_0 + \mu_1 + \mu_2 + \nu_3), \tag{H.26}$$

and the series of $\tilde{B}_{04}$ sums to:

$$\begin{aligned}
\sum_{\substack{n=4\\m=3}}^{\infty}\frac{\tilde{B}_{04}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_3, n, m)}{n!m!} &= \frac{\mu_0\mu_3}{(\mu_0 - \mu_2)(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)(\mu_1 - \nu_3)(\mu_2 - \nu_3)}\\
&\times\left[\left(e^{\mu_0} - \frac{\mu_0^2}{2} - \mu_0 - 1\right)(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)\right.\\
&- \left(e^{\mu_1} - \frac{\mu_1^2}{2} - \mu_1 - 1\right)(\mu_0 - \mu_2)(\mu_0 - \mu_3)(\mu_2 - \mu_3)\\
&+ \left(e^{\mu_2} - \frac{\mu_2^2}{2} - \mu_2 - 1\right)(\mu_0 - \mu_1)(\mu_0 - \mu_3)(\mu_1 - \mu_3)\\
&\left.- \left(e^{\mu_3} - \frac{\mu_3^2}{2} - \mu_3 - 1\right)(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)\right]\\
&\times\left[\left(e^{\mu_0} - \frac{\mu_0^2}{2} - \mu_0 - 1\right)(\mu_1 - \mu_2)(\mu_1 - \nu_3)(\mu_2 - \nu_3)\right.\\
&- \left(e^{\mu_1} - \frac{\mu_1^2}{2} - \mu_1 - 1\right)(\mu_0 - \mu_2)(\mu_0 - \nu_3)(\mu_2 - \nu_3)\\
&+ \left(e^{\mu_2} - \frac{\mu_2^2}{2} - \mu_2 - 1\right)(\mu_0 - \mu_1)(\mu_0 - \nu_3)(\mu_1 - \nu_3)\\
&\left.- \left(e^{\nu_3} - \frac{\nu_3^2}{2} - \nu_3 - 1\right)(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_1 - \mu_2)\right].
\end{aligned} \tag{H.27}$$

H.2. Upper bound on Y_{40}

Similarly to the bound on Y_{04}, we consider the combination of gains (G.37) that leads to the bound on Y_{40} in the case of three decoy intensity settings:

$$G_{20}^{0,1,2} = \sum_{n,m}^{\infty}\frac{Y_{nm}}{n!m!}C_{20}^{0,1,2}(n, m), \tag{H.28}$$

where the function $C_{20}^{0,1,2}(n, m)$ is defined by the rhs of (G.37), while $G_{20}^{0,1,2}$ is the combination of gains given by (G.31), with the coefficients $c_{i,j}$ of the combination given in (G.36). From G.4 we know that the terms Y_{n1}, Y_{n2}, Y_{0m} and Y_{1m} are removed in (H.28). Following the same procedure described in (H.1), we derive three additional combinations of gains in which the terms Y_{n1}, Y_{n2}, Y_{0m} and Y_{1m} are removed:

$$G_{20}^{0,1,3} = \sum_{n,m}^{\infty}\frac{Y_{nm}}{n!m!}C_{20}^{0,1,3}(n, m), \tag{H.29}$$

$$G_{20}^{0,2,3} = \sum_{n,m}^{\infty}\frac{Y_{nm}}{n!m!}C_{20}^{0,2,3}(n, m), \tag{H.30}$$

$$G_{20}^{1,2,3} = \sum_{n,m}^{\infty}\frac{Y_{nm}}{n!m!}C_{20}^{1,2,3}(n, m). \tag{H.31}$$

Now we further combine these expressions with arbitrary real coefficients $d_{i,j,k}$:

$$\begin{aligned} H_{40} &\equiv d_{0,1,2}G_{20}^{0,1,2} + d_{0,1,3}G_{20}^{0,1,3} + d_{0,2,3}G_{20}^{0,2,3} + d_{1,2,3}G_{20}^{1,2,3} \\ &= \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!}[d_{0,1,2}C_{20}^{0,1,2}(n, m) + d_{0,1,3}C_{20}^{0,1,3}(n, m) + d_{0,2,3}C_{20}^{0,2,3}(n, m) + d_{1,2,3}C_{20}^{1,2,3}(n, m)], \end{aligned} \tag{H.32}$$

and impose that even the terms Y_{n3} and Y_{2m} are removed from the rhs of (H.32). This yields a linear system of equations in the variables $d_{i,j,k}$, whose unique solution (up to a global rescaling) reads as follows:

$$\begin{aligned} d_{0,1,2} &= 1 \\ d_{0,1,3} &= \frac{(\mu_0 - \mu_2)(\nu_0 - \nu_2)[\mu_0(\nu_1 - \nu_3) + \mu_1(\nu_3 - \nu_0) + \mu_3(\nu_0 - \nu_1)]}{(\mu_0 - \mu_3)(\nu_0 - \nu_3)[\mu_0(\nu_2 - \nu_1) + \mu_1(\nu_0 - \nu_2) + \mu_2(\nu_1 - \nu_0)]} \\ d_{0,2,3} &= \frac{(\mu_0 - \mu_1)(\nu_0 - \nu_1)[\mu_0(\nu_2 - \nu_3) + \mu_2(\nu_3 - \nu_0) + \mu_3(\nu_0 - \nu_2)]}{(\mu_0 - \mu_3)(\nu_0 - \nu_3)[\mu_0(\nu_1 - \nu_2) + \mu_1(\nu_2 - \nu_0) + \mu_2(\nu_0 - \nu_1)]} \\ d_{1,2,3} &= \frac{\nu_0(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)[\mu_1(\nu_3 - \nu_2) + \mu_2(\nu_1 - \nu_3) + \mu_3(\nu_2 - \nu_1)]}{\nu_1(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\nu_1 - \nu_2)(\nu_1 - \nu_3)[\mu_0(\nu_1 - \nu_2) + \mu_1(\nu_2 - \nu_0) + \mu_2(\nu_0 - \nu_1)]}. \end{aligned} \tag{H.33}$$

By substituting the solution (H.33) back into (H.32) and by rearranging the rhs, one gets a combination of gains where all the terms Y_{n1}, Y_{n2}, Y_{n3}, Y_{0m}, Y_{1m} and Y_{2m} are removed:

$$H_{40} = \sum_{n=3}^{\infty} \frac{Y_{n0}}{n!} A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, n) + \sum_{\substack{n=3\\m=4}}^{\infty} \frac{Y_{nm}}{n!m!} B_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, m, n), \tag{H.34}$$

where the functions A_{04} and B_{04} are the same found in bounding Y_{04} with four decoys and are given by (H.10) and (H.12), respectively. Note that in this case the roles of the intensities μ_i and ν_i are exchanged with respect to the bound on Y_{04} (see (H.9)), as well as the roles of n and m. Following the same reasoning of (H.1), we can conclude that the coefficients of Y_{n0} and Y_{nm} have always opposite sign. Hence the upper bound on Y_{40} is obtained from (H.34) by setting all the yields Y_{n0} (with $n \neq 4$) to zero and the yields Y_{nm} (with $n \geqslant 3$, $m \geqslant 4$) to one. After rearranging the terms, we get the following expression for the upper bound on Y_{40}:

$$Y_{40}^{U} = \frac{24}{A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 4)} \left[H_{40} - \sum_{\substack{n=3\\m=4}}^{\infty} \frac{B_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, m, n)}{n!m!} \right], \tag{H.35}$$

where H_{40} is given in the first line of (H.32), while $A_{04}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 4)$ and the sum of the series are given in (H.14) and (H.15), respectively, under the replacement $\mu_i \leftrightarrow \nu_i$ for $i = 0, 1, 2, 3$.

We remark that in deriving the bound (H.35) we implicitly assumed –as in the Y_{04} case–that at least one of the following equalities does not hold: $\nu_0 = \mu_0, \nu_1 = \mu_1$ and $\nu_2 = \mu_2$. Indeed, when all three equalities hold (i.e. when Alice and Bob are using the same intensities settings for three out of four decoy pulses) one gets a '$\frac{0}{0}$ form' in the bound expression (H.35). In order to overcome this issue, one can follow an analogous procedure to that performed for the same issue affecting the bound on Y_{04} (see last paragraph in (H.1)), and obtain an additional upper bound on Y_{40} which is valid in the particular case of: $\nu_0 = \mu_0, \nu_1 = \mu_1$ and $\nu_2 = \mu_2$. The new bound on Y_{40} reads:

$$\tilde{Y}_{40}^{U} = \frac{24}{\tilde{A}_{04}(\mu_0, \mu_1, \mu_2, \nu_3, \mu_3, 4)} \left[\tilde{H}_{40} - \sum_{\substack{n=3\\m=4}}^{\infty} \frac{\tilde{B}_{04}(\mu_0, \mu_1, \mu_2, \nu_3, \mu_3, n, m)}{n!m!} \right], \tag{H.36}$$

where $\tilde{H}_{40}$ is given by:

$$\tilde{H}_{40} = \tilde{d}_{0,1,2}\tilde{G}_{20}^{0,1,2} + \tilde{d}_{0,1,3}\tilde{G}_{20}^{0,1,3} + \tilde{d}_{0,2,3}\tilde{G}_{20}^{0,2,3} + \tilde{d}_{1,2,3}\tilde{G}_{20}^{1,2,3}, \tag{H.37}$$

where:

$$\begin{aligned} \tilde{d}_{0,1,2} &= 0 \\ \tilde{d}_{0,1,3} &= \nu_3 \\ \tilde{d}_{0,2,3} &= -\frac{(\mu_0 - \mu_1)\nu_3}{\mu_0 - \mu_2} \\ \tilde{d}_{1,2,3} &= \frac{\mu_0\nu_3(\mu_0 - \mu_1)(\mu_0 - \mu_3)(\mu_0 - \nu_3)}{\mu_1(\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_1 - \nu_3)}, \end{aligned} \tag{H.38}$$

and $\tilde{G}_{20}$ are the same gains combinations (H.28), (H.29), (H.30) and (H.31) derived at the beginning of this Subsection, under the replacements: $\nu_0 \longrightarrow \mu_0$, $\nu_1 \longrightarrow \mu_1$ and $\nu_2 \longrightarrow \mu_2$. The quantity $\tilde{A}_{04}$ and the sum of the series are instead given in (H.26) and (H.27), respectively, under the replacement $\mu_3 \leftrightarrow \nu_3$.

H.3. Upper bound on Y_{13}

We follow the same procedure used in bounding the other yields in the case of four decoy intensity settings. We start by considering the four combination of gains in which the terms Y_{n0}, Y_{n1}, Y_{0m} and Y_{2m} are removed:

$$G_{13}^{0,1,2} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{13}^{0,1,2}(n,\, m), \tag{H.39}$$

$$G_{13}^{0,1,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{13}^{0,1,3}(n,\, m), \tag{H.40}$$

$$G_{13}^{0,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{13}^{0,2,3}(n,\, m), \tag{H.41}$$

$$G_{13}^{1,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{13}^{1,2,3}(n,\, m), \tag{H.42}$$

where the last three combinations are derived from the first one as described in (H.1), while the first combination is given by (G.44). Now we further combine these expressions with arbitrary real coefficients $d_{i,j,k}$:

$$\begin{aligned} H_{13} &\equiv d_{0,1,2}G_{13}^{0,1,2} + d_{0,1,3}G_{13}^{0,1,3} + d_{0,2,3}G_{13}^{0,2,3} + d_{1,2,3}G_{13}^{1,2,3} \\ &= \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!}[d_{0,1,2}C_{13}^{0,1,2}(n,\, m) + d_{0,1,3}C_{13}^{0,1,3}(n,\, m) + d_{0,2,3}C_{13}^{0,2,3}(n,\, m) + d_{1,2,3}C_{13}^{1,2,3}(n,\, m)], \end{aligned} \tag{H.43}$$

and impose that even the terms Y_{n2} and Y_{3m} are removed from the rhs of (H.43). This yields a linear system of equations in the variables $d_{i,j,k}$, whose unique solution (up to a global rescaling) reads as follows:

$$\begin{aligned} &d_{0,1,2} = 1 \\ &d_{0,1,3} = \frac{(\mu_0 - \mu_2)(\mu_1 + \mu_3)(\nu_0 - \nu_2)}{(\mu_0 - \mu_3)(\mu_1 + \mu_2)(\nu_0 - \nu_3)} \\ &\times \{\mu_0^2(\mu_1 + \mu_2)(\mu_2 + \mu_3)(\nu_1 - \nu_3) + (\mu_0 + \mu_2)[\mu_1^2(\mu_2 + \mu_3)(\nu_3 - \nu_0) + \mu_3^2(\mu_1 + \mu_2)(\nu_0 - \nu_1)]\} \\ &/\{-\mu_0^2(\mu_1 + \mu_3)(\mu_2 + \mu_3)(\nu_1 - \nu_2) + (\mu_0 + \mu_3)[\mu_1^2(\mu_2 + \mu_3)(\nu_0 - \nu_2) + \mu_2^2(\mu_1 + \mu_3)(\nu_1 - \nu_0)]\} \\ &d_{0,2,3} = -\frac{(\mu_0 - \mu_1)(\mu_2 + \mu_3)(\nu_0 - \nu_1)}{(\mu_0 - \mu_3)(\mu_1 + \mu_2)(\nu_0 - \nu_3)} \\ &\times \{\mu_0^2(\mu_1 + \mu_2)(\mu_1 + \mu_3)(\nu_2 - \nu_3) + (\mu_0 + \mu_1)[\mu_2^2(\mu_1 + \mu_3)(\nu_3 - \nu_0) + \mu_3^2(\mu_1 + \mu_2)(\nu_0 - \nu_2)]\} \\ &/\{-\mu_0^2(\mu_1 + \mu_3)(\mu_2 + \mu_3)(\nu_1 - \nu_2) + (\mu_0 + \mu_3)[\mu_1^2(\mu_2 + \mu_3)(\nu_0 - \nu_2) + \mu_2^2(\mu_1 + \mu_3)(\nu_1 - \nu_0)]\} \\ &d_{1,2,3} = \frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\mu_2 + \mu_3)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1^2 - \mu_2^2)(\mu_1 - \mu_3)(\nu_1 - \nu_2)(\nu_1 - \nu_3)}\{\mu_0^2[\mu_1^2(\nu_3 - \nu_2) + \mu_2^2(\nu_1 - \nu_3) + \mu_3^2(\nu_2 - \nu_1)] \\ &+ (\mu_0\mu_1\mu_2 + \mu_0\mu_1\mu_3 + \mu_0\mu_2\mu_3 + \mu_1\mu_2\mu_3)[\mu_1(\nu_3 - \nu_2) + \mu_2(\nu_1 - \nu_3) + \mu_3(\nu_2 - \nu_1)]\} \\ &/\{\mu_0^2(\mu_1 + \mu_3)(\mu_2 + \mu_3)(\nu_1 - \nu_2) + (\mu_0 + \mu_3)[-\mu_1^2(\mu_2 + \mu_3)(\nu_0 - \nu_2) + \mu_2^2(\mu_1 + \mu_3)(\nu_0 - \nu_1)]\}. \end{aligned} \tag{H.44}$$

By substituting the solution (H.44) back into (H.43) and by rearranging the rhs, one gets a combination of gains where all the terms Y_{n0}, Y_{n1}, Y_{n2}, Y_{0m}, Y_{2m} and Y_{3m} are removed:

$$\begin{aligned} H_{13} = &\sum_{m=3}^{\infty} \frac{Y_{1m}}{m!} A_{13}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_0,\, \nu_1,\, \nu_2,\, \nu_3,\, m) \\ &+ \sum_{\substack{n=4 \\ m=3}}^{\infty} \frac{Y_{nm}}{n!m!} A_{13}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_0,\, \nu_1,\, \nu_2,\, \nu_3,\, m) D_n(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3), \end{aligned} \tag{H.45}$$

where:

$$\begin{aligned} &A_{13}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_0,\, \nu_1,\, \nu_2,\, \nu_3,\, m) = -\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)} \\ &\times \frac{p_{13}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_0,\, \nu_1,\, \nu_2,\, \nu_3)}{q_{13}(\mu_0,\, \mu_1,\, \mu_2,\, \mu_3,\, \nu_0,\, \nu_1,\, \nu_2,\, \nu_3)}\left(\sum_{i_1 \leqslant i_2 \leqslant \ldots \leqslant i_{m-3}} \nu_{i_1}\nu_{i_2} \cdot \ldots \cdot \nu_{i_{m-3}}\right); \end{aligned} \tag{H.46}$$

$$\begin{aligned} p_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) &= \mu_1^2[\mu_2^2(\nu_0 - \nu_3)(\nu_1 - \nu_2) - \mu_3^2(\nu_0 - \nu_2)(\nu_1 - \nu_3)] \\ &+ \mu_0^2[\mu_1^2(\nu_0 - \nu_1)(\nu_2 - \nu_3) - \mu_2^2(\nu_0 - \nu_2)(\nu_1 - \nu_3) + \mu_3^2(\nu_0 - \nu_3)(\nu_1 - \nu_2)] \\ &+ \mu_2^2\mu_3^2(\nu_0 - \nu_1)(\nu_2 - \nu_3); \end{aligned} \tag{H.47}$$

$$\begin{aligned} q_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3) &= \mu_0^2(\mu_1 + \mu_3)(\mu_2 + \mu_3)(\nu_1 - \nu_2) - \mu_1^2(\mu_0 + \mu_3)(\mu_2 + \mu_3)(\nu_0 - \nu_2) \\ &+ \mu_2^2(\mu_0 + \mu_3)(\mu_1 + \mu_3)(\nu_0 - \nu_1), \end{aligned} \tag{H.48}$$

and D_n is defined recursively as [28]:

$$\begin{cases} D_n(\mu_0, \mu_1, \mu_2, \mu_3) = \dfrac{\sum_{j=1}^{n-4}(\mu_0^j + \mu_1^j + \mu_2^j + \mu_3^j)D_{n-j}(\mu_0, \mu_1, \mu_2, \mu_3) - \mu_0\mu_1\mu_2\mu_3\left(\sum_{i_1 \leqslant i_2 \leqslant \ldots \leqslant i_{n-5}} \mu_{i_1}\mu_{i_2} \cdot \ldots \cdot \mu_{i_{n-5}}\right)}{n - 4} \\ D_4(\mu_0, \mu_1, \mu_2, \mu_3) = \mu_0\mu_1\mu_2 + \mu_0\mu_1\mu_3 + \mu_0\mu_2\mu_3 + \mu_1\mu_2\mu_3. \end{cases} \tag{H.49}$$

We assume that the indexes in the sums run over the set $\{0, 1, 2, 3\}$ and we define $\sum_{i_1 \leqslant i_2 \leqslant \ldots \leqslant i_{m-3}} \nu_{i_1}\nu_{i_2} \cdot \ldots \cdot \nu_{i_{m-3}}|_{m=3} = 1$. Since $D_n \geqslant 0$ for every $n \geqslant 4$, we deduce that the coefficients of Y_{1m} and Y_{nm} in (H.45) have always equal sign. Hence the upper bound on Y_{13} is obtained from (H.45) by setting all the other yields to zero. After rearranging the terms, we get the following expression for the upper bound on Y_{13}:

$$Y_{13}^U = \frac{6\ H_{13}}{A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, 3)}, \tag{H.50}$$

where H_{13} is given in the first line of (H.43), while $A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, 3)$ is given by:

$$\begin{aligned} A_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3, 3) = &-\frac{(\mu_0 - \mu_1)(\mu_0 - \mu_2)(\nu_0 - \nu_1)(\nu_0 - \nu_2)}{(\mu_1 + \mu_2)}. \\ &\times \frac{p_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3)}{q_{13}(\mu_0, \mu_1, \mu_2, \mu_3, \nu_0, \nu_1, \nu_2, \nu_3)} \end{aligned} \tag{H.51}$$

H.4. Upper bound on Y_{31}

We follow the same procedure used in bounding the other yields in the case of four decoy intensity settings. We start by considering the four combination of gains in which the terms Y_{n0}, Y_{n2}, Y_{0m} and Y_{1m} are removed:

$$G_{31}^{0,1,2} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{31}^{0,1,2}(n, m), \tag{H.52}$$

$$G_{31}^{0,1,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{31}^{0,1,3}(n, m), \tag{H.53}$$

$$G_{31}^{0,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{31}^{0,2,3}(n, m), \tag{H.54}$$

$$G_{31}^{1,2,3} = \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!} C_{31}^{1,2,3}(n, m), \tag{H.55}$$

where the last three combinations are derived from the first one as described in (H.1), while the first combination is given by (G.48). Now we further combine these expressions with arbitrary real coefficients $d_{i,j,k}$:

$$\begin{aligned} H_{31} &\equiv d_{0,1,2}G_{31}^{0,1,2} + d_{0,1,3}G_{31}^{0,1,3} + d_{0,2,3}G_{31}^{0,2,3} + d_{1,2,3}G_{31}^{1,2,3} \\ &= \sum_{n,m}^{\infty} \frac{Y_{nm}}{n!m!}[d_{0,1,2}C_{31}^{0,1,2}(n, m) + d_{0,1,3}C_{31}^{0,1,3}(n, m) + d_{0,2,3}C_{31}^{0,2,3}(n, m) + d_{1,2,3}C_{31}^{1,2,3}(n, m)], \end{aligned} \tag{H.56}$$

and impose that even the terms Y_{n3} and Y_{2m} are removed from the rhs of (H.56). This yields a linear system of equations in the variables $d_{i,j,k}$, whose unique solution (up to a global rescaling) is given in (H.44), under the replacement: $\mu_i \leftrightarrow \nu_i$ for $i = 0, 1, 2, 3$. By substituting the solution back into (H.56) and by rearranging the rhs, one gets a combination of gains where all the terms Y_{n0}, Y_{n2}, Y_{n3}, Y_{0m}, Y_{1m} and Y_{2m} are removed:

$$\begin{aligned} H_{31} = &\sum_{n=3}^{\infty} \frac{Y_{n1}}{n!} A_{13}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, n) \\ &+ \sum_{\substack{n=3 \\ m=4}}^{\infty} \frac{Y_{nm}}{n!m!} A_{13}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, n) D_m(\nu_0, \nu_1, \nu_2, \nu_3), \end{aligned} \tag{H.57}$$

where the functions A_{13} and D_m are defined in (H.46) and (H.49), respectively. Since $D_m \geqslant 0$ for every $m \geqslant 4$, we deduce that the coefficients of Y_{n1} and Y_{nm} in (H.57) have always equal sign. Hence the upper bound on Y_{31} is obtained from (H.57) by setting all the other yields to zero. After rearranging the terms, we get the following expression for the upper bound on Y_{31}:

$$Y_{31}^{U} = \frac{6\ H_{31}}{A_{13}(\nu_0,\ \nu_1,\ \nu_2,\ \nu_3,\ \mu_0,\ \mu_1,\ \mu_2,\ \mu_3,\ 3)}, \tag{H.58}$$

where H_{31} is given in the first line of (H.56), while $A_{13}(\nu_0, \nu_1, \nu_2, \nu_3, \mu_0, \mu_1, \mu_2, \mu_3, 3)$ is given by (H.51) under the substitution: $\mu_i \leftrightarrow \nu_i$ for $i = 0, 1, 2, 3$.

ORCID iDs

Federico Grasselli https://orcid.org/0000-0003-2966-7813

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India)* (Piscataway, NJ: IEEE) pp 175–9

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3

[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[4] Lo H K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595–604

[5] Pirandola S *et al* 2019 arXiv:1906.01645

[6] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502

[7] Liao S K *et al* 2017 *Nature* **549** 43

[8] Takenaka H, Carrasco-Casado A, Fujiwara M, Kitamura M, Sasaki M and Toyoshima M 2017 *Nat. Photon.* **11** 502

[9] Takeoka M, Guha S and Wilde M M 2014 *Nat. Commun.* **5** 5235

[10] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043

[11] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932–5

[12] Duan L M, Lukin M, Cirac J I and Zoller P 2001 *Nature* **414** 413

[13] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 *Rev. Mod. Phys.* **83** 33–80

[14] Abruzzo S, Kampermann H and Bruß D 2014 *Phys. Rev.* A **89** 012301

[15] Panayi C, Razavi M, Ma X and Lütkenhaus N 2014 *New J. Phys.* **16** 043005

[16] Azuma K, Tamaki K and Munro W J 2015 *Nat. Commun.* **6** 10171

[17] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400

[18] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev.* A **98** 062323

[19] Curty M, Azuma K and Lo H K 2019 *NPJ Quantum Inf.* **5** 64

[20] Ma X, Zeng P and Zhou H 2018 *Phys. Rev.* X **8** 031043

[21] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053

[22] Tamaki K, Lo H K, Wang W and Lucamarini M 2018 arXiv:1805.05511

[23] Lin J and Lütkenhaus N 2018 *Phys. Rev.* A **98** 042332

[24] Zhong X, Hu J, Curty M, Qian L and Lo H K 2019 *Phys. Rev. Lett.* **123** 100506

[25] Minder M, Pittaluga M, Roberts G, Lucamarini M, Dynes J, Yuan Z and Shields A 2019 *Nat. Photon.* **13** 334–8

[26] Liu Y *et al* 2019 *Phys. Rev. Lett.* **123** 100505

[27] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C and Han Z F 2019 *Phys. Rev.* X **9** 021046

[28] Grasselli F and Curty M 2019 *New J. Phys.* **21** 073001

[29] Wang W, Xu F and Lo H K 2018 *Phys. Rev.* X **9** 041012

[30] Zhou X Y, Zhang C H, Zhang C M and Wang Q 2019 *Phys. Rev.* A **99** 062316

[31] Wang X B, Peng C Z and Pan J W 2007 *Appl. Phys. Lett.* **90** 031110

[32] Wang X B 2007 *Phys. Rev.* A **75** 052301

[33] Chi H H, Yu Z W and Wang X B 2012 *Phys. Rev.* A **86** 042307

[34] Wang Y, Bao W S, Zhou C, Jiang M S and Li H W 2016 *Phys. Rev.* A **94** 032335

[35] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[36] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[37] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[38] Xu F, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007

[39] Xu F, Sajeed S, Kaiser S, Tang Z, Qian L, Makarov V and Lo H K 2015 *Phys. Rev.* A **92** 032305

[40] Liu H *et al* 2019 *Phys. Rev. Lett.* **122** 160501

[41] Xu F, Xu H and Lo H K 2014 *Phys. Rev.* A **89** 052333

[42] Boyd S and Vandenberghe L 2004 *Convex Optimization* (Cambridge: Cambridge University Press)

[43] Wolfram Research, Inc. 2016 Mathematica, Version 11.0, Champaign, IL

[44] Wang W and Lo H K 2019 arXiv:1907.05291

Conference key agreement with single-photon interference

Title:	Conference key agreement with single-photon interference
Authors:	Federico Grasselli, Hermann Kampermann and Dagmar Bruß
Journal:	New Journal of Physics
Impact factor:	3.783 (2018)
Date of submission:	29 July 2019
Publication status:	Published
Contribution by FG:	First author (input approx. 90%)

This publication corresponds to reference [GKB19]. A summary of its content is presented in chapter 7.

The idea for this project was jointly conceived by me, my co-authors and Prof. Curty. I developed the primitive idea until it reached the final form presented in the paper. Specifically, I found the type of multipartite beam splitter useful for our needs and established the general form of the new CKA protocol. I independently performed all the analytical computations needed to derive the protocol's secret key length. I proved its security in the finite-key regime and performed the numerical simulations with new Mathematica code written by me specifically for this CKA protocol. I conceived the newly-introduced direct transmission bound and decided which performance comparisons would be best to include in the paper. During the development of the project, I had some discussions with my co-authors on the project's outcomes and on possible ways to improve them. I drew the conclusions of the project and wrote the whole manuscript. My co-authors proofread the manuscript and improved it with their comments.

New Journal of Physics

The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

CrossMark

OPEN ACCESS

RECEIVED
29 July 2019

REVISED
27 September 2019

ACCEPTED FOR PUBLICATION
13 November 2019

PUBLISHED
11 December 2019

Original content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence.

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

PAPER

Conference key agreement with single-photon interference

Federico Grasselli, **Hermann Kampermann** and **Dagmar Bruß**

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225, Düsseldorf, Germany

E-mail: federico.grasselli@hhu.de

Keywords: multipartite QKD, single-photon interference, conference key agreement, W-state, finite-key, TF-QKD

Abstract

The intense research activity on Twin-Field (TF) quantum key distribution (QKD) is motivated by the fact that two users can establish a secret key by relying on single-photon interference in an untrusted node. Thanks to this feature, variants of the protocol have been proven to beat the point-to-point private capacity of a lossy quantum channel. Here we generalize the main idea of the TF-QKD protocol introduced by Curty *et al* to the multipartite scenario, by devising a conference key agreement (CKA) where the users simultaneously distill a secret conference key through single-photon interference. The new CKA is better suited to high-loss scenarios than previous multipartite QKD schemes and it employs for the first time a W-class state as its entanglement resource. We prove the protocol's security in the finite-key regime and under general attacks. We also compare its performance with the iterative use of bipartite QKD protocols and show that our truly multipartite scheme can be advantageous, depending on the loss and on the state preparation.

The most mature and developed application of quantum communication [1, 2] is certainly quantum key distribution (QKD) [3–8]. The majority of the QKD protocols proposed so far involve just two end-users, Alice and Bob, who want to establish a secret shared key. Nowadays there is a vibrant research towards protocols which are proven to be secure in the most adversarial situation possible (i.e. reducing the assumption on the devices) [9–14], but at the same time are also implementable with today's technology [15–18]. In this context, a protocol which recently received great attention is the Twin-Field (TF) QKD protocol originally proposed by Lucamarini *et al* [19], further developed to prove its security [20–27] and experimentally implemented [28–31]. Indeed, the TF-QKD protocol relies only on single-photon interference occurring in an untrusted node, making it a measurement-device-independent (MDI) QKD protocol capable of overcoming the repeaterless bounds [32, 33].

In a scenario where several users are required to share a common secret key, one can for instance perform bipartite QKD protocols between pairs of users and then use the secret keys established in this way to encode the final common secret key. Alternatively, one can perform a truly multipartite QKD scheme—also known as conference key agreement (CKA)—whose purpose is to deliver the *same* secret key to *all* the parties involved in the protocol [35–39]. In order to accomplish such a task, a resource which seems necessary is the multipartite Greenberger–Horne–Zeilinger (GHZ) state [34–38] or a multipartite private state—a 'twisted' version of the GHZ state [40, 41].

In this work we introduce a CKA which exploits for the first time the multipartite entanglement of a W-class state [42], in order to deliver the same secret key to all users. Despite having a number of users involved, the scheme relies on single-photon interference in an untrusted node and it is inspired by the bipartite TF-QKD protocol by Curty *et al* [24]. We prove the security of our CKA in the finite-key scenario, allowing Eve to perform the most general attacks (coherent attacks) on the transmitted signals. We compare the performance of our genuinely multipartite QKD scheme with the iterative use of bipartite QKD protocols, both in the asymptotic regime and in the finite-key regime. In doing so, we show that performing a truly multipartite scheme can yield a higher secret key rate, depending on the loss and on the state preparation.

The paper is structured as follows. In section 1 we present the CKA based on single-photon interference, while in section 2 we discuss the establishment of a secret conference key where the entanglement resource is a W

© 2019 The Author(s). Published by IOP Publishing Ltd on behalf of the Institute of Physics and Deutsche Physikalische Gesellschaft

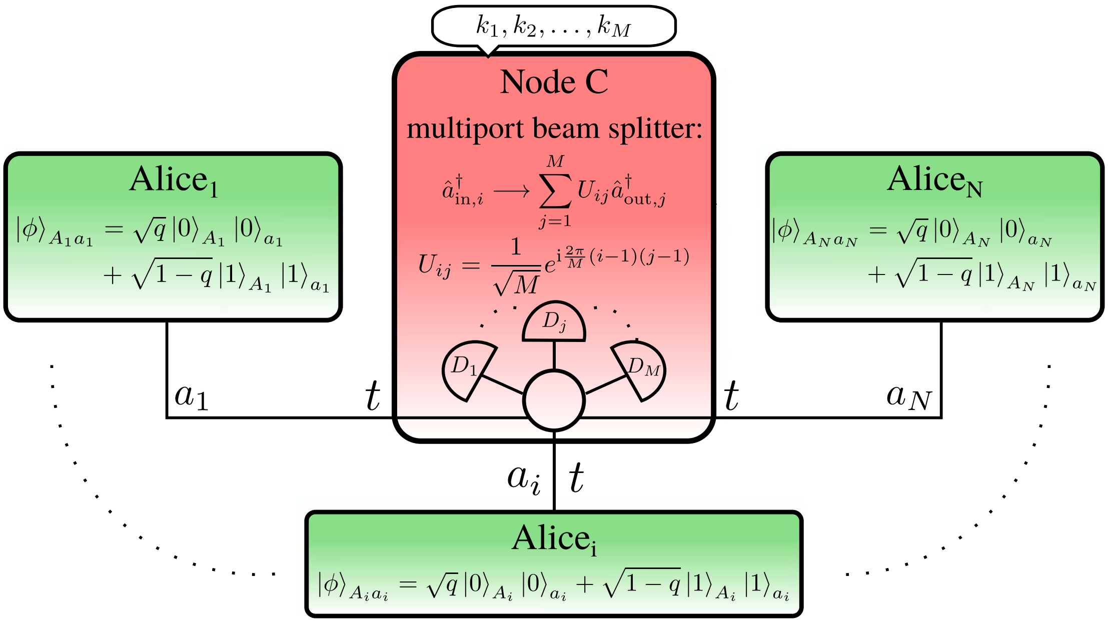
$k_1, k_2, \ldots, k_M$
Node C
multiport beam splitter:
$\hat{a}^{\dagger}_{\text{in},i} \longrightarrow \sum_{j=1}^{M} U_{ij}\hat{a}^{\dagger}_{\text{out},j}$
$U_{ij} = \frac{1}{\sqrt{M}} e^{\mathrm{i}\frac{2\pi}{M}(i-1)(j-1)}$
D_1
D_j
D_M
Alice$_1$
$|\phi\rangle_{A_1 a_1} = \sqrt{q}\,|0\rangle_{A_1}|0\rangle_{a_1} + \sqrt{1-q}\,|1\rangle_{A_1}|1\rangle_{a_1}$
Alice$_N$
$|\phi\rangle_{A_N a_N} = \sqrt{q}\,|0\rangle_{A_N}|0\rangle_{a_N} + \sqrt{1-q}\,|1\rangle_{A_N}|1\rangle_{a_N}$
a_1
t
t
a_N
a_i
t
Alice$_i$
$|\phi\rangle_{A_i a_i} = \sqrt{q}\,|0\rangle_{A_i}|0\rangle_{a_i} + \sqrt{1-q}\,|1\rangle_{A_i}|1\rangle_{a_i}$

Figure 1. The CKA based on single-photon interference in the untrusted central node and on trusted measurements performed on each party's (Alice$_i$) qubit.

state. In section 3 we prove the CKA security in the finite-key scenario (the detailed proof is given in appendix A). In section 4 we provide simulations of the protocol's secret key rate and compare them with the repeated use of bipartite schemes (further comparisons in appendix C). We present our conclusions in section 5. In appendix B we report in detail the calculations of the relevant parameters for an honest implementation of the protocol.

1. Conference key agreement

As anticipated in the introduction, our CKA scheme is an extension of the original bipartite TF-QKD protocol [24], Protocol 1 to a scenario with N users who want to establish a secret conference key. The parties distill the secret key by sending optical pulses to an untrusted node and by performing suitable measurements on a qubit they hold. In order to keep the notation symmetric, the N parties involved in the multipartite QKD protocol are named: Alice$_1$, Alice$_2$, ..., Alice$_N$. The protocol is composed of L rounds, each round is characterized by the following eight steps (see figure 1):

(i) Every party (Alice$_i$) prepares an optical pulse a_i in an entangled state with a qubit A_i, given by:

$$|\phi\rangle_{A_i a_i} = \sqrt{q}|0\rangle_{A_i}|0\rangle_{a_i} + \sqrt{1-q}|1\rangle_{A_i}|1\rangle_{a_i} \quad \forall\, i \in \{1,\, 2, \ldots, N\}, \tag{1.1}$$

where $0 \leqslant q \leqslant 1$, $|0\rangle_{a_i}$ is the vacuum state, $|1\rangle_{a_i}$ is the single-photon state, and $\{|0\rangle_{A_i},\ |1\rangle_{A_i}\}$ is the computational basis of qubit A_i.

(ii) Every party sends her optical pulse a_i to the untrusted node via optical channels characterized by transmittance t, in a synchronized manner.

(iii) The central node applies a Bell-multiport beam splitter [43–48] with M input and output ports[1] to the incoming pulses and features a threshold detector D_i at each output port ($i = 1, \ldots, M$). The action of the multiport beam splitter is defined by the unitary transformation given in figure 1.

(iv) The central node announces the measurement outcome k_i for every detector D_i, with $k_i = 0$ and $k_i = 1$ corresponding to a no-click and a click event, respectively. The round gets discarded if $\sum_{i=1}^{M} k_i \neq 1$, i.e. whenever single-photon interference did not occur in the central node. The probability that only detector D_j clicked is p_j.

[1] We assume that there are at least as many input ports of the beam splitter as parties taking part to the protocol, i.e. $M \geqslant N$.

(v) According to a preshared secret key of $L \cdot h(p_{\rm PE})$ bits[2], the round is classified as a parameter-estimation (PE) round with probability $p_{\rm PE}$ or as a key-generation (KG) round with probability $1 - p_{\rm PE}$. There are on average $m = Mp_j Lp_{\rm PE}$ PE rounds that do not get discarded.

(a) In case of a PE round, every party measures her qubit in the Z-basis and then announces the measurement outcome to compute the frequency: $Q_Z^m = (1 + \langle Z^{\otimes N}\rangle_m)/2$.

(b) In case of a KG round, conditioned on detector D_j clicking, Alice$_i$ measures her qubit in the basis of the operator $O_{XY}(\varphi_i) = \cos\varphi_i X + \sin\varphi_i Y$ (where X and Y are the Pauli operators), with $\varphi_i = \arg(U_{ij})$ (U_{ij} is given in figure 1). The parties announce m randomly chosen measurement results in order to estimate the quantum bit error rate (QBER) by computing the frequency: $Q_{A_1A_i}^m = (1 - \langle O_{XY}(\varphi_1)O_{XY}(\varphi_i)\rangle_m)/2$, i.e. the frequency of discordant outcomes.

(vi) The secret key shared by the N users is extracted from the remaining $n = Mp_j L - 2m$ raw key bits of the KG rounds.

(vii) Alice$_1$ broadcasts the error correction information that every other party uses to correct her raw key to Alice$_1$'s raw key.

(viii) Alice$_1$ broadcasts a suitable two-universal hash function and every party applies it to her key for privacy amplification.

Remarks. Note that the quantity Q_Z^m is the frequency of the outcome $+1$ when the parties measure the operator $Z^{\otimes N}$. By making an analogy with the bipartite scenario, one can view Q_Z^m as an estimation of the phase-error rate between Alice$_1$ and the other $N - 1$ parties (when the phase-error rate is defined as in [24]).

Since the Bell-multiport beam splitter redirects each incoming photon with equal probability to each potential output port, the probability of having a click in only one specific detector is the same for all detectors, i.e. p_j reads the same for $j = 1, \ldots, M$. For this reason, the total probability of having exactly one click in any detector is given by Mp_j.

In an honest implementation of the protocol, where the parties' state preparation and the operations of the central node are carried out as described above, the state of the qubits $A_1, \ldots, A_N$ from which the parties distill a secret key is approximately a W-class state of N qubits [42], as we show in section 2. Therefore, the protocol here introduced represents an alternative to other multipartite QKD protocols [34–38] where the entanglement resource used to generate the key is, instead, a noisy version of the GHZ state of N qubits. Moreover, the W-class state used by the CKA is an entangled state which is post-selected after the interference of one single photon at the multiport beam splitter. Thus the resulting key rate scales *linearly* with the transmittance t of one of the quantum channels linking the parties to the central node. This is in contrast to the other mentioned multipartite QKD protocols [34–38], where the distribution of an N-qubit GHZ state (e.g. encoded in orthogonal polarizations of a photon) would lead to a key rate which scales with t^N (with t being the transmittance of the link between one party and the node distributing the GHZ state). This makes our CKA much more suited to high-loss scenarios than previously proposed multipartite QKD protocols.

2. Multipartite QKD with a *W* state

As mentioned at the end of section 1, the entanglement resource exploited to distill the secret key is a noisy W-class state of N qubits [42], which is post-selected after single-photon interference occurred in the central node. In fact, the optimization of the CKA key rate (section 4) over the parameter q weighting the initial superposition of the qubit-photon state always yields values of q close to 1. This means that the quantum signal sent by the parties is strongly unbalanced towards the vacuum. Thus the events in which one of the detectors clicks are mainly caused by the arrival and detection of one photon. However, because of the balanced superposition generated by the multiport beam splitter, the detected photon could be sent by any party with equal probability. Since the photon is initially entangled to the qubit in state $|1\rangle$, the qubits' state conditioned on the detection is a coherent superposition of states in which one qubit is in state $|1\rangle$ and all the others are in state $|0\rangle$, that is the mentioned W-class state. A secret conference key can then be extracted by proper measurements performed on such a state.

[2] Where $h(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$ is the binary entropy function.

Let us start by considering the simplistic scenario in which the parties share the N-partite W state:

$$|W\rangle_N = \frac{1}{\sqrt{N}}[|00\ldots01\rangle + |00\ldots10\rangle + \ldots + |10\ldots00\rangle]. \tag{2.1}$$

It has been proven [35] that the parties cannot extract perfectly correlated outcomes in any set of local measurement bases (for $N \geqslant 3$). Indeed, the only N-qubit state achieving that and yielding uniformly distributed random measurement outcomes is the GHZ state. Nevertheless, the N-partite W state can still be used to extract a secret conference key. The key bits are given by the outcomes of the X-basis measurements performed by the N parties on their respective qubit. The expected QBER between any two parties is given by $1/2 - 1/N$, which amounts to subtracting the fraction $h(1/2 - 1/N)$ from the secret key rate due to error correction ($h(x)$ is the binary entropy). On the other hand, the eavesdropper's knowledge about the key can be estimated via the phase-error rate Q_Z (as defined in section 1, more details in appendix A), which turns out to be zero on the W state. This is crucial for having a non-zero key rate even when the number of parties is large. The resulting asymptotic key rate, when the parties share an N-partite W state, is given by $1 - h(1/2 - 1/N)$.

Our CKA is constructed following the same philosophy. The only difference is that the conditional state shared by the parties after the detector's click is not exactly the W state given by (2.1), but rather a noisy W-class state (the full expression is given in appendix B). Indeed, the multiport beam splitter introduces complex phases in the balanced superposition of states shared by the parties, that depend on which detector clicked. For this reason, we require the parties to adjust their KG measurements in the X, Y plane in order to remove such phases and obtain the same QBER $(1/2 - 1/N)$ they would observe by measuring in the X-basis had they shared the standard W state (2.1). However, the adjusted KG measurements do not commute with the operations performed in the untrusted node and prevent the CKA from being recast as an MDI prepare-and-measure scheme, opposed to its bipartite version [24]. Consequently, the multipartite scheme presented here is more challenging to implement than its bipartite counterpart, i.e. the TF-QKD protocol. In particular, it cannot be reformulated as a scheme where the parties prepare coherent states and send them to node C for measurement. Nonetheless, the operations that the parties are required to perform seem to be within technological reach [49, 50]. In particular, the qubit system could be realized by a nitrogen-vacancy electron spin, whose coherence time has recently reached the order of seconds [51]. The entanglement between the electron spin and the photon's Fock state would then be generated via selective optical pulses and coherent rotations [49], which would entangle the electron spin with the presence or absence of a photon.

3. Finite-key analysis

The protocol presented in section 1 can be effectively regarded as an N-partite QKD protocol solely characterized by the unknown quantum state $\rho^{Mp_jL}_{A_1A_2\ldots A_N}$, which is the global state of the parties' qubits in all the rounds that were not discarded[3]. In this way we allow the eavesdropper, who is in total control of the untrusted node, to perform any kind of operation (coherent attacks) on the whole set of signals sent by the parties in the different rounds. As described above, in each round the parties perform trusted measurements on the state $\rho^{Mp_jL}_{A_1A_2\ldots A_N}$, according to the preshared key they hold. The security of such a multipartite QKD protocol can be proven thanks to the finite-key analysis developed in [37]. In particular, since Alice$_1$ (who holds the key to which all the other parties correct their raw key) measures her qubit only in the two mutually unbiased bases Z and X, the protocol's security proof follows analogous lines to the one of the N-BB84 protocol presented in [37]. The security is guaranteed even when the state preparation and the measurement devices of the other parties (Alice$_2$,…,Alice$_N$) are not trusted (a detailed proof is given in appendix A).

Theorem 1. *The CKA in section 1, with the optimal 1-way error-correction protocol (which is $\varepsilon_{\rm EC}$-fully secure and $2(N-1)\varepsilon_{\rm PE}$ -robust) and where the secret key generated by two-universal hashing has length*

$$\ell(N) = n\left[1 - h(Q_Z^m + \gamma(n, m, Q_Z^m, \varepsilon_z) - \max_i h(Q^m_{A_1A_i} + \gamma(n, m, Q^m_{A_1A_i}, \varepsilon_x)\right] - \log_2\frac{2(N-1)}{\varepsilon_{\rm EC}}$$
$$- 2\log_2\frac{1-2(N-1)\varepsilon_{\rm PE}}{2\,\varepsilon_{\rm PA}}, \tag{3.1}$$

is $\varepsilon_{\rm tot}$-secure with $\varepsilon_{\rm tot} = 2\varepsilon_{\rm PE} + \varepsilon_{\rm EC} + \varepsilon_{\rm PA}$, where $\varepsilon_{\rm PE}$ is defined as:

$$\varepsilon_{\rm PE} \equiv \sqrt{(N-1)\varepsilon_x + \varepsilon_z} \tag{3.2}$$

[3] On average, the number of rounds that are not discarded by the CKA is Mp_jL.

and $\gamma(n, m, \Lambda_m, \varepsilon)$ *is the positive root of the following equation:*

$$\ln\left(\frac{n(\Lambda_m+\gamma)+m\Lambda_m}{m\Lambda_m}\right)+\ln\left(\frac{(n+m)(1-\Lambda_m)-n\gamma}{m(1-\Lambda_m)}\right)=\ln\binom{n+m}{m}+\ln\varepsilon. \tag{3.3}$$

We remark that the length $L\cdot h(p_{\mathrm{PE}})$ of the preshared key must be subtracted from the secret key length in order to have the net amount of fresh secret key bits. We also remark that our leakage estimation considers the *worst-case* QBER affecting the parties' raw keys, which is (with high probability) not larger than the QBER observed in appositely designated KG rounds with the appropriate statistical correction. This is in contrast to several other finite-key analyses [52–55], where either the QBER is assumed to be known *a priori* or its estimation does not account for statistical fluctuations.In the asymptotic regime ($L \to \infty$), the finite-size effects are not present and the secret key rate ($r = \ell/L$) reads:

$$r(N)=Mp_j\left[1-h(Q_Z)-\max_{i\in\{1,\ldots,N\}}h(Q_{A_1A_i})\right], \tag{3.4}$$

where Q_Z and $Q_{A_1A_i}$ are the probabilities correspondent to the frequencies defined in section 1.

4. Simulations

In this section we provide plots of the secret key rate—number of secret key bits per round—achieved by the CKA both with finite-key effects (3.1) and in the asymptotic regime (3.4), as a function of the loss in one of the channels linking a party to the central node, measured in dB ($-10\log_{10}t$). We assume that the protocol is honestly implemented as described in section 1 and we account for a dark count probability of $p_d = 10^{-9}$ in every detector (which can be attained with superconducting nanowire single photon detectors [29]) and for a polarization and a phase misalignment between Alice$_1$ and each other party of 2%. The relevant error rates and probabilities for this configuration are given in appendix B. The plots are optimized over the parameter q of the initial superposition between the two qubit-photon states, unless otherwise stated. The finite-key plots are further optimized over the probability p_{PE} of performing a PE round and over the security parameters ε_x, ε_z, $\varepsilon_{\mathrm{EC}}$ and $\varepsilon_{\mathrm{PA}}$, constrained by a fixed total security parameter of $\varepsilon_{\mathrm{tot}} = 10^{-8}$.

In order to assess the performance of our CKA with an untrusted node, we consider the situation in which the central node is removed and the N parties are linked by a star network, where the transmittance of the link between any two parties is t^2. For this configuration, we consider the conference key rate generated by the following strategy and compare it to our CKA key rate. One selected party performs the best possible bipartite QKD scheme with every other party in the network, i.e. $N-1$ times. Because of the network symmetry, every bipartite secret key has the same length and its asymptotic rate is upper bounded by the Pirandola–Laurenza–Ottaviani–Banchi bound [33] given by: $-\log_2(1-t^2)$. Then, the selected party encodes the final conference key by using the keys she/he established singularly with each other party. Hence, the conference key length is equal to the bipartite keys' lengths, but the total number of rounds[4] needed to establish the conference key is given by the number of rounds performed by a pair of parties, multiplied by the number of bipartite schemes ($N-1$). Thus the conference key rate achieved by this strategy is upper bounded by:

$$r_{\mathrm{direct}}(N)=\frac{-\log_2(1-t^2)}{N-1}. \tag{4.1}$$

We will refer to (4.1) as the *direct-transmission bound*, even though we emphasize that it only upper bounds the achievable conference key rate when the strategy we just described is employed. Indeed, we do not claim that this strategy yields the highest possible conference key rate for the considered network configuration. In this section we show that our CKA provides an advantage, in terms of performance, with respect to the above strategy (4.1).

4.1. Asymptotic regime

In figure 2 we plot the asymptotic key rate of the CKA (equation (3.4), solid and dotted lines) as a function of the loss in one of the quantum channels, for different number parties establishing the secret conference key. In particular, the solid lines are obtained by fixing $M = N$, i.e. the number of input (output) ports of the beam splitter is given by the number of parties taking part to the protocol. The dotted lines are instead obtained by fixing the number of ports to $M = 10$. Finally, the dashed lines represent the direct-transmission bound (4.1) for the correspondent number of parties.

We observe that the CKA key rate can surpass the direct-transmission bound for sufficiently high losses. This is expected since the CKA key rate basically scales linearly with the transmittance t of the quantum channel

[4] By round we mean a set of steps of a given QKD protocol which contains only one transmission of quantum signals (more parties at the same time can transmit a quantum signal).

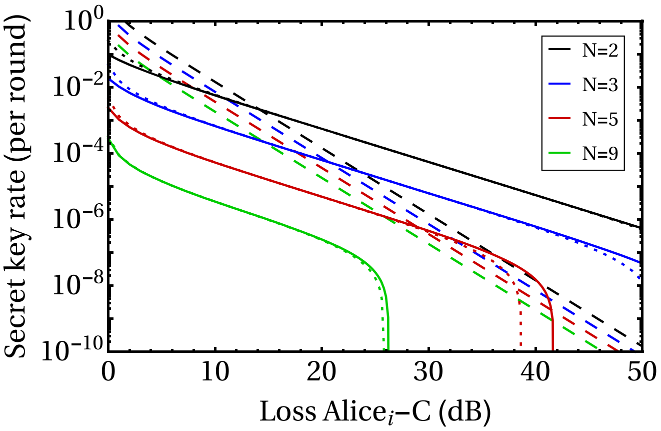

Figure 2. The CKA key rate (equation (3.4), solid and dotted lines) and the direct-transmission bound (equation (4.1), dashed lines), as a function of the loss in the channel linking one party to the central node, for different number of parties $N = 2, 3, 5$ and 9 (black, blue, red and green; top to bottom). The CKA key rate overcomes the correspondent direct-transmission bound for increasing losses, as the number of parties increases. For instance, the CKA performed by 5 parties becomes advantageous at distances larger than 150 km (assuming a fiber attenuation of $\alpha = 0.2$ dB km^{-1}). We also observe that having more ports in the beam splitter than parties involved in the protocol is advantageous at low losses (dotted lines are above the solid lines) but disadvantageous at high losses, where more ports imply a higher chance of having a dark count.

linking one party to the central node, while the direct-transmission rate scales linearly with the transmittance (t^2) of the whole channel linking two parties [33]. We note, however, that the performance advantage of the CKA with respect to the direct-transmission bound decreases for increasing number of parties. This is due to the fact that an increase of the number of parties is more detrimental for the CKA rate as it severely affects the QBER[5], than for the direct-transmission bound, where it simply increases the total number of rounds dividing the key length. Moreover, the presence of dark counts in the detectors prevents the CKA from outperforming the direct-transmission bound if the number of parties is too large (see the $N = 9$ case in figure 2). Indeed, they are the cause of the sudden drop of the key rate at high losses, i.e. where the probability of detecting one photon becomes comparable to the probability of having a dark count. Moreover, their effect increases with the number of parties since the key rate optimization yields a lower probability of having a single click in one of the detectors, when more parties are involved. Note, however, that while the CKA rate accounts for devices' imperfections (e.g. dark counts), the direct-transmission bound is attained only in the ideal scenario of no imperfections.

From figure 2 we also deduce that performing the CKA with a higher number of ports in the beam splitter (dotted lines, where $M = 10$) is advantageous at low losses and disadvantageous at high losses. The advantage of having more output ports is that the probability that two photons arrive at the same detector diminishes (this is an error source in our CKA). However, these errors could only occur if there is a non-negligible probability that two photons arrive at the central node, i.e. when the losses are low. At the same time, the presence of more output ports—and thus detectors—increases the chances of a dark count. And the negative effect of dark counts on the performance becomes tangible when their probability is comparable to the probability of having a click in a detector, i.e. at high losses.

Another relevant scenario for assessing the CKA performance in comparison to the iteration of bipartite protocols could be the following. The parties are given the same CKA experimental setup but they are now allowed to use it in pairs (or larger subgroups) in consecutive runs, effectively performing the original TF-QKD protocol [24], Protocol 1 between one selected party and every other party. The different established keys are then used to encode the final conference key, similarly to the direct-transmission scenario. This strategy can then be compared to the case where the parties choose to use the CKA setup all at once, thus performing a truly multipartite QKD scheme. A detailed analysis of this comparison in the asymptotic regime is given in appendix C. It turns out that, depending on the loss and on the state preparation, it is still advantageous to perform a multipartite protocol instead of iteratively executing bipartite protocols, on the CKA experimental setup.

4.2. Finite-key effects

In figure 3(a) we plot the finite-key conference rate (equation (3.1) divided by L) as a function of the number of rounds L, for different fixed values of the loss (20 and 30 dB, solid and dotted–dashed lines) and different number of parties. We stress the fact that we normalize the key length to the *total* number of rounds (L), i.e. we

[5] The QBER scales with the number of parties as $1/2 - 1/N$, see section 2.

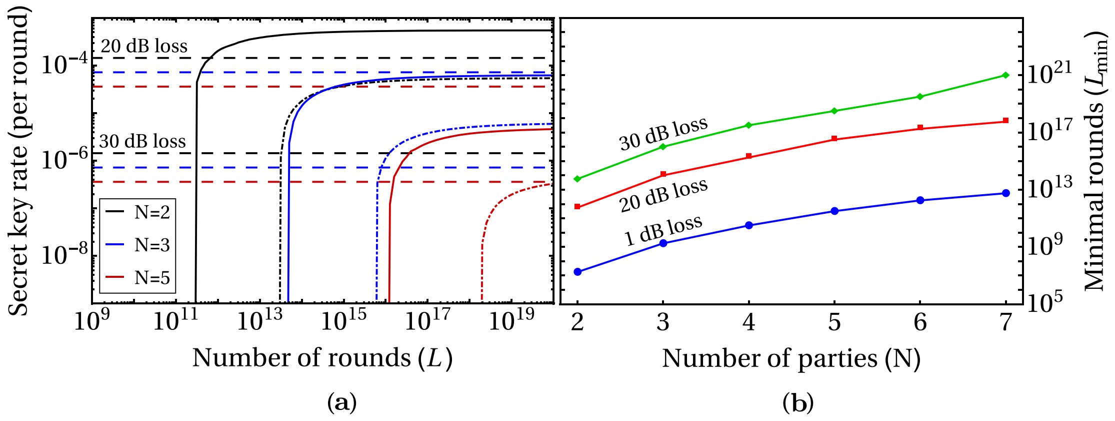

Figure 3. (a) Finite-key conference rate (equation (3.1) over L) as a function of the number of rounds L, for fixed losses of 20 dB (solid lines) and 30 dB (dotted–dashed lines), and different number of parties: $N = 2$, 3 and 5 (black, blue and red; top to bottom). We observe that the rates quickly achieve their asymptotic value once the number of non-discarded rounds is enough to get a non-zero key. The CKA key rates overcome the direct-transmission bound (dashed lines) even in the finite-key scenario. (b) Minimum number of rounds such that the finite-key rate (equation (3.1) over L) is at least 10% of its asymptotic value, as a function of the number of parties and for fixed losses (1 dB blue circles, 20 dB red squares and 40 dB green diamonds). We notice that increasing the number of parties and/or the losses is more detrimental for the finite-key rate than for the asymptotic one, due to an increase of the fraction of discarded rounds and thus of the statistical fluctuations. Here we study the finite-key effects on our CKA. The number of ports in the beam splitter is given by the number of parties taking part to the protocol: $M = N$.

also take into account the rounds that get discarded due to double-clicks or no click in the detectors. The horizontal dashed lines correspond to the value of the direct-transmission bound (4.1) for the various combinations of losses and number of parties. We observe that the number of rounds leading to a non-zero key rate is in general higher than other multipartite schemes (see for example [37]). This is caused by the fact that the CKA devised here relies on single-photon interference events, which are only a fraction of all the events occurring in an experiment run. A considerable amount of rounds gets thus discarded, but still contributes to the rounds' count. Nevertheless, the number of rounds needed for a non-zero key rate is comparable to other bipartite TF-QKD protocols [56, 57]. On the other hand, the advantage of relying on single-photon interference in a multipartite scenario is the excellent scaling of the protocol's key rate with respect to losses, which allows it to overcome the asymptotic direct-transmission bound (dashed lines) even with a finite number of rounds.

In figure 3(b) we instead plot the minimum number of rounds ($L_{\min}$) such that the finite-key rate (ℓ/L) does not decrease more than 90% with respect to its asymptotic value r (3.4), i.e.: $\ell(L_{\min})/L_{\min} \geqslant r/10$. The threshold $L_{\min}$ is plotted as a function of the number of parties (N) and for fixed values of the loss. We observe that $L_{\min}$ increases both with the number of parties and with the loss. The reason is that, in both cases, the fraction of the total number of rounds that gets discarded increases. This has a negative effect both on the asymptotic rate and on the finite-key rate, however the effect on the latter is greater, thus requiring a larger number of rounds $L_{\min}$ to maintain the finite-key rate within 90% range of the asymptotic one. Indeed, a larger fraction of discarded rounds decreases the prefactor Mp_j in both the finite- and the asymptotic-key rates, but it additionally decreases the number of rounds used for PE in the finite-key regime. This causes larger statistical fluctuations and thus a smaller finite-key rate.

5. Conclusions

In this work we introduced a new multipartite QKD protocol that exploits for the first time the correlations derived from an N-partite W state [42] to establish a secret conference key among the N users. In an honest implementation of the protocol, the W state is post-selected thanks to the interference of a *single* photon in a central node, extending the idea of the bipartite TF QKD protocol devised in [24] to the multipartite scenario. Hence the resulting key rate scales linearly with the transmittance of one of the quantum channels linking the parties to the central node, making the protocol particularly suited for conference keys established in high-loss scenarios.

We prove the protocol's security in the finite-key regime by considering the most adversarial situation possible, i.e. coherent attacks are allowed by the eavesdropper. In order to achieve this, we rely on previous results on the finite-key security of multipartite QKD schemes derived in [37] and employ the entropic uncertainty relation [58].

We provide simulations of the conference key rate both in the finite- and in the asymptotic-key regime. We compare the performance of our CKA to that achieved by performing bipartite QKD schemes between one party and each of the others and then using the established keys to encode the conference key. In particular, we analyze the cases where the bipartite schemes are performed with the same setup used for the CKA (in appendix C) and in the direct-transmission scenario (i.e. the central node is removed and the optimal bipartite QKD scheme is performed). We show that, in both cases, the execution of a truly multipartite scheme could be advantageous even when finite-key effects are accounted for.

Although the feasibility of the proposed CKA requires further investigation, with this work we demonstrate that, in principle, multipartite QKD does not necessarily need a GHZ-class state as its entanglement resource and that it can be implemented even in high-loss scenarios.

Acknowledgments

We thank Marcos Curty, Daniel Miller and Hua-Lei Yin for helpful discussions. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675662.

Appendix A. Security proof

In order to prove the security of our CKA in the finite-key scenario, we start from the general security statement given in [37, theorem 1]. The resulting secret key length is thus determined by the amount of information the eavesdropper has about the secret key and by the information the parties leak during the classical post-processing. The former is quantified by the min-entropy $H_{\min}^{\varepsilon}(\rho_{XE}^{n}|E)$, where ρ_{XE}^{n} is the classical-quantum state of Alice$_1$'s raw key and the eavesdropper's quantum system E which is partially correlated to it. Since the eavesdropper's system is unknown, one cannot directly compute the mentioned min-entropy. Nevertheless, it can be bounded by means of the uncertainty relation [58] for smooth-entropies as follows:

$$H_{\min}^{\varepsilon}(\rho_{XE}^{n}|E) \geqslant n - H_{\max}^{\varepsilon}(\rho_{Z_1\ldots Z_N}^{n}|Z_2\ldots Z_N), \tag{A.1}$$

where the max-entropy on the rhs quantifies the uncertainty of Alice$_1$'s Z-measurement results when the Z-outcomes of the remaining $N-1$ parties are known, if all parties would measure Z in the n rounds yielding the raw-key. The max-entropy can be upper bounded via the phase-error rate Q_Z^n—as defined in section 1—of the n raw-key rounds. We get:

$$H_{\min}^{\varepsilon}(\rho_{XE}^{n}|E) \geqslant n - n\,h(Q_Z^n), \tag{A.2}$$

where $h(\cdot)$ is the binary entropy function: $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. Finally, since the parties do not directly observe the phase-error rate Q_Z^n of the n rounds producing the raw key, this can be inferred through the theory of random sampling without replacement. In particular, the phase-error rate of the raw key (Q_Z^n) can be upper bounded with high probability, once the observed phase-error rate (Q_Z^m) is known. For this, we make use of the following tail inequality [56, lemma 1] which features a tighter bound with respect to the Serfling inequality.

Lemma 1. *[56]. Let $\mathcal{X}_{n+m}$ be a random binary string of $n+m$ bits, $\mathcal{X}_m$ be a random sample (without replacement) of m entries from the string $\mathcal{X}_{n+m}$ and $\mathcal{X}_n$ be the remaining bit string. Upon calling Λ_m and Λ_n the frequencies of bit value 1 in string $\mathcal{X}_m$ and $\mathcal{X}_n$, respectively, for any $\varepsilon > 0$ it holds:*

$$\Pr[\Lambda_n \leqslant \Lambda_m + \gamma(n, m, \Lambda_m, \varepsilon)] > 1 - \varepsilon, \tag{A.3}$$

where $\gamma(n, m, \Lambda_m, \varepsilon)$ is the positive root of the following equation:

$$\ln\left(\frac{n(\Lambda_m+\gamma) + m\Lambda_m}{m\Lambda_m}\right) + \ln\left(\frac{(n+m)(1-\Lambda_m) - n\gamma}{m(1-\Lambda_m)}\right) = \ln\binom{n+m}{m} + \ln\varepsilon. \tag{A.4}$$

By applying lemma 1 to the case of Q_Z^n, we can finally bound the eavesdropper knowledge about the secret key as follows:

$$H_{\min}^{\varepsilon}(\rho_{XE}^{n}|E) \geqslant n - n\,h(Q_Z^m + \gamma(n, m, Q_Z^m, \varepsilon_z)). \tag{A.5}$$

The remaining part of the secret key length that needs to be estimated is the error-correction information sent through the classical public channel, and thus leaked to the eavesdropper. Since we consider a one-way scheme where Alice$_1$ broadcasts the same error-correction information to all the parties through the public channel, the information gained by the eavesdropper is bounded by the binary entropy of the worst QBER between Alice$_1$ and any other party, by means of [37, theorem 2].

Putting these considerations together, we obtain the security statement given in theorem 1.

We remark that the only requirements needed for the security proof to hold are that Alice$_1$ is actually measuring qubits and that her measurement device is working as expected (i.e. it measures in the X and Z basis) [58, 59]. This means that we do not need to trust the measurement devices of the other parties (as long as they are memoryless), nor their state preparation (including Alice$_1$'s).

Appendix B. Channel model

In this section we compute the QBER ($Q_{A_1A_k}$), the phase-error rate (Q_Z) and the probability that a given detector clicked (p_j), assuming that the protocol is implemented as described in section 1. We also account for a dark count probability p_d in each detector and we consider the specific scenario in which there are a polarization and a phase misalignment of angles θ and ϕ, respectively, between Alice$_1$ and each other party. In the simulations of section 4 we set: $p_d = 10^{-9}$ and $\theta = \phi = \arcsin\sqrt{0.02}$. For simplicity, we assume that the input signals of the N parties enter the first N ports of the M-port beam splitter. Nevertheless, the results in terms of achieved key rate are independent of which input ports are used, thanks to the balanced redistribution of the input photons to the output ports of the considered Bell-multiport beam splitter (see figure 1). We remark that the expressions derived here together with the asymptotic key rate given in (3.4) reproduce those of the original TF-QKD protocol [24, Protocol 1] in the case of two parties ($N = 2$) with a balanced 2-port beam splitter ($M = 2$).

We first derive the QBER, the phase-error rate and the probability p_j assuming no dark counts in the detectors, i.e. every click is caused by the arrival of one or more photons. In the last Subsection we use the derived expressions to obtain analogous quantities, with the assumption that every detector has a probability p_d of clicking conditioned on no photon arriving.

B.1. Qubits' state conditioned on one click

According to the protocol, the global state of the parties' qubits and signals, before sending the signals to the central node, reads:

$$|\Phi_1\rangle = \bigotimes_{k=1}^{N} |\phi\rangle_{A_k a_k} = \bigotimes_{k=1}^{N} (\sqrt{q}\,|0\rangle_{A_k}|0\rangle_{a_k} + \sqrt{1-q}\,\mathrm{e}^{\mathrm{i}\phi_k}|1\rangle_{A_k} a_k^{\dagger}|0\rangle_{a_k}), \tag{B.1}$$

where the phase mismatch ϕ_k is defined as zero if $k = 1$ and as ϕ if $k \neq 1$, which means that every other party has the same phase mismatch with respect to Alice$_1$. The signals a_k are then sent to the central node through lossy optical channels, which are modeled as beam splitters with transmittance t. The global state after the transmission of the signals to the untrusted relay reads:

$$\begin{aligned} |\Phi_2\rangle &= \bigotimes_{k=1}^{N} [\sqrt{q}\,|0\rangle_{A_k}|0\rangle + \sqrt{1-q}\,\mathrm{e}^{\mathrm{i}\phi_k}|1\rangle_{A_k}(\sqrt{t}\ a_k^{\dagger} + \sqrt{1-t}\ l_k^{\dagger})|0\rangle] \\ &= \sum_{g(\vec{b})=0}^{2^N-1} q^{\frac{N-|\vec{b}|}{2}}(1-q)^{\frac{|\vec{b}|}{2}}|\vec{b}\rangle_{A_1\ldots A_N} \otimes_{k=1}^{N}\ \mathrm{e}^{\mathrm{i}b_k\phi_k}(\sqrt{t}\ a_k^{\dagger} + \sqrt{1-t}\ l_k^{\dagger})^{b_k}|0\rangle, \end{aligned} \tag{B.2}$$

where $l_k^{\dagger}$ is the creation operator of the lost photon in channel k, $\vec{b}$ is a N-bit vector that runs from 0 to $2^N - 1$ in binary notation (covering all the possible combinations of qubit states) and $|\vec{b}|$ is the Hamming weight of vector $\vec{b}$. From now on, we denote as $g(\cdot)$ the bijective function that takes as input a binary vector and outputs the correspondent decimal number.

We assume now that the polarization of the photons sent by Alice$_2$,... Alice$_N$ is rotated by an angle θ with respect to Alice$_1$'s signal:

$$|\Phi_3\rangle = \sum_{g(\vec{b})=0}^{2^N-1} q^{\frac{N-|\vec{b}|}{2}}(1-q)^{\frac{|\vec{b}|}{2}}|\vec{b}\rangle_{A_1\ldots A_N} \otimes_{k=1}^{N}\ \mathrm{e}^{\mathrm{i}b_k\phi_k}(\sqrt{t}\ \cos\theta_k a_{k,\mathrm{P}}^{\dagger} - \sqrt{t}\ \sin\theta_k a_{k,\mathrm{P}_{\perp}}^{\dagger} + \sqrt{1-t}\ l_k^{\dagger})^{b_k}|0\rangle, \tag{B.3}$$

where θ_k is defined as zero if $k = 1$ and as θ if $k \neq 1$, while the subscripts $_\mathrm{P}$ and $_{\mathrm{P}_\perp}$ indicate the polarization of Alice$_1$'s signal and its orthogonal direction, respectively.

Finally, the global state after the application of the Bell-multiport beam splitter on the incoming signals (its action on the incoming creation operators is reported in figure 1) is:

$$|\Phi_4\rangle = \sum_{g(\vec{b})=0}^{2^N-1} q^{\frac{N-|\vec{b}|}{2}}(1-q)^{\frac{|\vec{b}|}{2}}|\vec{b}\rangle_{A_1\ldots A_N}$$
$$\otimes \prod_{k=1}^{N} \mathrm{e}^{\mathrm{i}b_k\phi_k}\left(\sqrt{t}\,\cos\theta_k\sum_{j=1}^{M}U_{kj}\sigma^{\dagger}_{j,\mathrm{P}} - \sqrt{t}\,\sin\theta_k\sum_{j=1}^{M}U_{kj}\sigma^{\dagger}_{j,\mathrm{P}_\perp} + \sqrt{1-t}\;l_k^{\dagger}\right)^{b_k}|0\rangle, \tag{B.4}$$

where $\sigma^{\dagger}_{j,\mathrm{P}}$ and $\sigma^{\dagger}_{j,\mathrm{P}_\perp}$ are the creation operators of the output signals in the two orthogonal polarizations and U_{kj} is reported in figure 1. At this point, every output signal is measured in the respective threshold detector. Since the detectors do not distinguish the polarization of the output signals, we will use the subscript $_{\sigma_j}$ to indicate the combined Hilbert space of the signals exiting port j, when there is no ambiguity.

We are now ready to compute the conditional state of the qubits $A_1,\ldots,A_N$ when only detector D_j clicked:

$$p_j\rho^{j}_{A_1\ldots A_N} = \mathrm{Tr}_{\substack{\sigma_1,\ldots,\sigma_M\\ l_1,\ldots,l_N}}[(\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}})\otimes_{i\neq j}P_{|0\rangle_{\sigma_i}}|\Phi_4\rangle\langle\Phi_4|(\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}})\otimes_{i\neq j}P_{|0\rangle_{\sigma_i}}], \tag{B.5}$$

where p_j is the probability that only detector D_j clicked, $\rho^{j}_{A_1\ldots A_N}$ is the normalized conditional state of the qubits and $P_{|0\rangle_{\sigma_j}}$ is the projector on the vacuum state of output signal j. In order to compute (B.5), we start by calculating the following quantity:

$$(\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}})\otimes_{i\neq j}P_{|0\rangle_{\sigma_i}}|\Phi_4\rangle = \sum_{g(\vec{b})=1}^{2^N-1} q^{\frac{N-|\vec{b}|}{2}}(1-q)^{\frac{|\vec{b}|}{2}}|\vec{b}\rangle_{A_1\ldots A_N}$$
$$\otimes(\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}})\otimes_{i\neq j}P_{|0\rangle_{\sigma_i}}\prod_{k=1}^{N}\mathrm{e}^{\mathrm{i}b_k\phi_k}[\sqrt{t}\,U_{kj}(\cos\theta_k\sigma^{\dagger}_{j,\mathrm{P}} - \sin\theta_k\sigma^{\dagger}_{j,\mathrm{P}_\perp}) + \sqrt{1-t}\;l_k^{\dagger}]^{b_k}|0\rangle$$
$$\equiv \sum_{g(\vec{b})=1}^{2^N-1} q^{\frac{N-|\vec{b}|}{2}}(1-q)^{\frac{|\vec{b}|}{2}}|\vec{b}\rangle_{A_1\ldots A_N}\otimes(\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}})\otimes_{i\neq j}P_{|0\rangle_{\sigma_i}}|\psi\rangle_{\sigma_j,l}, \tag{B.6}$$

where the effect of the projectors is to select the outcome signal σ_j and to remove the case $g(\vec{b}) = 0$, since it would correspond to a vacuum state for the outcome signal σ_j. We now focus on rewriting the following term:

$$|\psi\rangle_{\sigma_j,l} = \prod_{k=1}^{N}\mathrm{e}^{\mathrm{i}b_k\phi_k}[\sqrt{t}\,U_{kj}(\cos\theta_k\sigma^{\dagger}_{j,\mathrm{P}} - \sin\theta_k\sigma^{\dagger}_{j,\mathrm{P}_\perp}) + \sqrt{1-t}\;l_k^{\dagger}]^{b_k}|0\rangle$$
$$= \mathrm{e}^{\mathrm{i}(|\vec{b}|-b_1)\phi}\sum_{\substack{g(\vec{d})=0\text{ s.t.}\\ \vec{d}\wedge\vec{b}=\vec{d}}}^{2^N-1}\prod_{k=1}^{N}[\sqrt{t}\;U_{kj}(\cos\theta_k\sigma^{\dagger}_{j,\mathrm{P}} - \sin\theta_k\sigma^{\dagger}_{j,\mathrm{P}_\perp})]^{d_k}(\sqrt{1-t}\;l_k^{\dagger})^{(\vec{b}\oplus\vec{d})_k}|0\rangle \tag{B.7}$$

$$= \mathrm{e}^{\mathrm{i}(|\vec{b}|-b_1)\phi}\sum_{\substack{g(\vec{d})=0\text{ s.t.}\\ \vec{d}\wedge\vec{b}=\vec{d}}}^{2^N-1}\mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^{N}d_k(k-1)}\left(\sqrt{\frac{t}{M}}\right)^{|\vec{d}|}(\sqrt{1-t})^{|\vec{b}\oplus\vec{d}|}$$
$$\times\prod_{k=1}^{N}(\cos\theta_k\sigma^{\dagger}_{j,\mathrm{P}} - \sin\theta_k\sigma^{\dagger}_{j,\mathrm{P}_\perp})^{d_k}|0\rangle\otimes|\vec{b}\oplus\vec{d}\rangle_{l_1,\ldots,l_N}, \tag{B.8}$$

where we expanded the product in the first line of (B.7) by introducing a sum over the binary vector $\vec{d}$. The sum runs over all the N-bit vectors $\vec{d}$ for which $d_k = 0$ whenever $b_k = 0$, for all k–the condition $d_k \wedge b_k = d_k\ \forall\ k$. This is to make sure that the kth factor in the first line does not contribute to the expanded product in the second line whenever $b_k = 0$. The remaining bits of $\vec{d}$ that are not affected by the mentioned condition, can be either 1 or 0. If $d_k = 1$ we intend that, for this particular term in the sum, the contribution of the kth factor in the first line of (B.7) is given by its first addend $(\sqrt{t}\ U_{kj}(\ldots))$. While if $d_k = 0$ and $b_k = 1$, we mean that the contribution is coming from the second addend $(\sqrt{1-t}\ l_k^{\dagger})$. The exponents in the second line of (B.7) are chosen according to these rules. Finally, (B.8) is obtained by using the definition of U_{kj} from figure 1 and by applying the creation operators on the vacuum. We now expand the remaining product in (B.8) with the same technique and obtain the following expression:

$$
\begin{aligned}
|\psi\rangle_{\sigma_j,l} = {}& \mathrm{e}^{\mathrm{i}(|\vec{b}|-b_1)\phi} \sum_{\substack{g(\vec{d})=0 \text{ s.t.}\\ \vec{d}\wedge\vec{b}=\vec{d}}}^{2^N-1} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^{N} d_k(k-1)} \left(\sqrt{\frac{t}{M}}\right)^{|\vec{d}|} (\sqrt{1-t})^{|\vec{b}\oplus\vec{d}|} \\
& \times \sum_{\substack{g(\vec{f})=0 \text{ s.t.}\\ \vec{f}\wedge\vec{d}=\vec{f}}}^{2^N-1} \prod_{k=1}^{N} (\cos\theta_k\,)^{f_k} (-\sin\theta_k)^{(\vec{d}\oplus\vec{f})_k} \sqrt{|\vec{f}|!}\sqrt{|\vec{d}\oplus\vec{f}|!}\; ||\vec{f}|\rangle_{\sigma_j,\mathrm{P}} \otimes ||\vec{d}\oplus\vec{f}|\rangle_{\sigma_j,\mathrm{P}_\perp} \otimes |\vec{b}\oplus\vec{d}\rangle_{l_1,\ldots,l_N} \\
= {}& \mathrm{e}^{\mathrm{i}(|\vec{b}|-b_1)\phi} \sum_{\substack{g(\vec{d})=0 \text{ s.t.}\\ \vec{d}\wedge\vec{b}=\vec{d}}}^{2^N-1} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^{N} d_k(k-1)} \left(\sqrt{\frac{t}{M}}\right)^{|\vec{d}|} (\sqrt{1-t})^{|\vec{b}\oplus\vec{d}|} \\
& \times \sum_{\substack{g(\vec{f})=0 \text{ s.t.}\\ \vec{f}\wedge\vec{d}=\vec{f}}}^{2^N-1} (\cos\theta)^{|\vec{f}|-f_1} (-\sin\theta)^{|\vec{d}\oplus\vec{f}|} \delta_{(\vec{d}\oplus\vec{f})_1,0}\sqrt{|\vec{f}|!}\sqrt{|\vec{d}\oplus\vec{f}|!}\; ||\vec{f}|\rangle_{\sigma_j,\mathrm{P}} \\
& \otimes ||\vec{d}\oplus\vec{f}|\rangle_{\sigma_j,\mathrm{P}_\perp} \otimes |\vec{b}\oplus\vec{d}\rangle_{l_1,\ldots,l_N}.
\end{aligned}
\tag{B.9}
$$

We now substitute (B.9) back into (B.6) and note that the effect of the projectors $(\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}}) \otimes_{i\neq j} P_{|0\rangle_{\sigma_i}}$ is to remove the case $g(\vec{d}) = 0$ from (B.9). Hence we get:

$$
\begin{aligned}
& (\mathrm{id}_{\sigma_j} - P_{|0\rangle_{\sigma_j}}) \otimes_{\mathrm{i}\neq j} P_{|0\rangle_{\sigma_\mathrm{i}}}|\Phi_4\rangle \\
& = \sum_{g(\vec{b})=1}^{2^N-1} q^{\frac{N-|\vec{b}|}{2}}(1-q)^{\frac{|\vec{b}|}{2}}\mathrm{e}^{\mathrm{i}(|\vec{b}|-b_1)\phi}|\vec{b}\rangle_{A_1\ldots A_N} \otimes \sum_{\substack{g(\vec{d})=1 \text{ s.t.}\\ \vec{d}\wedge\vec{b}=\vec{d}}}^{2^N-1} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^{N} d_k(k-1)} \left(\sqrt{\frac{t}{M}}\right)^{|\vec{d}|} (\sqrt{1-t})^{|\vec{b}\oplus\vec{d}|} \\
& \times \sum_{\substack{g(\vec{f})=0: f_1=d_1\\ \vec{f}\wedge\vec{d}=\vec{f}}}^{2^N-1} (\cos\theta)^{|\vec{f}|-f_1} (-\sin\theta)^{|\vec{d}\oplus\vec{f}|} \sqrt{|\vec{f}|!}\sqrt{|\vec{d}\oplus\vec{f}|!}\; ||\vec{f}|\rangle_{\sigma_j,\mathrm{P}} \otimes ||\vec{d}\oplus\vec{f}|\rangle_{\sigma_j,\mathrm{P}_\perp} \otimes |\vec{b}\oplus\vec{d}\rangle_{l_1,\ldots,l_N}.
\end{aligned}
\tag{B.10}
$$

By substituting (B.10) into (B.5) we finally get the state of the qubits conditioned on D_j clicking:

$$
\begin{aligned}
p_j\rho^j_{A_1\ldots A_N} = {}& \sum_{g(\vec{b}),g(\vec{b}')=1}^{2^N-1} q^{N-\frac{|\vec{b}|+|\vec{b}'|}{2}}(1-q)^{\frac{|\vec{b}|+|\vec{b}'|}{2}}\mathrm{e}^{\mathrm{i}[|\vec{b}|-|\vec{b}'|-(b_1-b_1')]\phi}|\vec{b}\rangle\langle\vec{b}'| \\
& \times \sum_{\substack{g(\vec{d}),g(\vec{d}')=1:\ \vec{d}\wedge\vec{b}=\vec{d}\\ \vec{d}'\wedge\vec{b}'=\vec{d}'}}^{2^N-1} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^{N}(k-1)(d_k-d_k')} \left(\sqrt{\frac{t}{M}}\right)^{|\vec{d}|+|\vec{d}'|} (\sqrt{1-t})^{|\vec{b}\oplus\vec{d}|+|\vec{b}'\oplus\vec{d}'|} \\
& \times \sum_{\substack{g(\vec{f})=0: f_1=d_1\\ \vec{f}\wedge\vec{d}=\vec{f}}}^{2^N-1} \sum_{\substack{g(\vec{f}')=0: f_1'=d_1'\\ \vec{f}'\wedge\vec{d}'=\vec{f}'}}^{2^N-1} (\cos\theta)^{|\vec{f}|+|\vec{f}'|-f_1-f_1'} (-\sin\theta)^{|\vec{d}\oplus\vec{f}|+|\vec{d}'\oplus\vec{f}'|} \\
& \times \sqrt{|\vec{f}|!\,|\vec{f}'|!\,|\vec{d}\oplus\vec{f}|!\,|\vec{d}'\oplus\vec{f}'|!}\; \delta_{|\vec{f}|,|\vec{f}'|}\,\delta_{|\vec{d}\oplus\vec{f}|,|\vec{d}'\oplus\vec{f}'|}\,\delta_{\vec{b}\oplus\vec{d},\vec{b}'\oplus\vec{d}'}.
\end{aligned}
\tag{B.11}
$$

We use the Kronecker deltas to reduce the sums over $\vec{d}$, $\vec{d}'$, $\vec{f}$ and $\vec{f}'$. The third delta fixes the value of $\vec{d}'$: $\vec{d}' = \vec{b}\oplus\vec{b}'\oplus\vec{d}$. The fixed value of $\vec{d}'$ combined with the other constraints on this vector imply additional constraints on $\vec{d}$. In particular, $\vec{d}' \neq 0$ implies $\vec{d} \neq \vec{b}\oplus\vec{b}'$ while $\vec{d}'\wedge\vec{b}' = \vec{d}'$ implies $\vec{b}'\wedge(\vec{b}\oplus\vec{d}) = \vec{b}\oplus\vec{d}$. Finally the first two deltas imply $|\vec{d}| = |\vec{d}'|$, which combined with the third delta yields $|\vec{b}| = |\vec{b}'|$. Putting everything together allows to simplify (B.11) as follows:

$$
\begin{aligned}
p_j\rho^j_{A_1\ldots A_N} = {}& \sum_{\substack{g(\vec{b}),g(\vec{b}')=1\\ |\vec{b}'|=|\vec{b}|}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\,\mathrm{e}^{\mathrm{i}[(b_1'-b_1)]\phi}|\vec{b}\rangle\langle\vec{b}'| \sum_{\vec{d}\in\mathcal{D}(\vec{b},\vec{b}')} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^{N}(k-1)(d_k-b_k\oplus d_k\oplus b_k')} \\
& \times \left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|} \sum_{\vec{f}\in\mathcal{F}(\vec{d})}^{2^N-1} \sum_{\vec{f}'\in\mathcal{F}'(\vec{f},\vec{d},\vec{b},\vec{b}')}^{2^N-1} |\vec{f}|!\,(|\vec{d}|-|\vec{f}|)!(\cos\theta)^{2|\vec{f}|-d_1-d_1\oplus b_1\oplus b_1'}(\sin\theta)^{2(|\vec{d}|-|\vec{f}|)},
\end{aligned}
\tag{B.12}
$$

where the sets of binary vectors $\mathcal{D}(\vec{b}, \vec{b}')$, $\mathcal{F}(\vec{d})$ and $\mathcal{F}'(\vec{f}, \vec{d}, \vec{b}, \vec{b}')$ are defined as follows:

$$\mathcal{D}(\vec{b}, \vec{b}') = \{\vec{d} \in g^{-1}([1, 2^N - 1]): \vec{d} \wedge \vec{b} = \vec{d},\ \vec{d} \neq \vec{b} \oplus \vec{b}', (\vec{b} \oplus \vec{d}) \wedge \vec{b}' = \vec{b} \oplus \vec{d}\} \tag{B.13}$$

$$\mathcal{F}(\vec{d}) = \{\vec{f} \in g^{-1}([0, 2^N - 1]): \vec{f} \wedge \vec{d} = \vec{f},\ f_1 = d_1\} \tag{B.14}$$

$$\mathcal{F}'(\vec{f}, \vec{d}, \vec{b}, \vec{b}') = \{\vec{f}' \in g^{-1}([0, 2^N - 1]): \vec{f}' \wedge (\vec{b} \oplus \vec{d} \oplus \vec{b}') = \vec{f}',\ f_1' = b_1 \oplus d_1 \oplus b_1',\ |\vec{f}'| = |\vec{f}|\}. \tag{B.15}$$

We can now sum over the vectors $\vec{f}'$ since no term depends on them in (B.12):

$$\begin{aligned} p_j \rho^j_{A_1 \ldots A_N} = & \sum_{\substack{g(\vec{b}), g(\vec{b}')=1 \\ |\vec{b}'|=|\vec{b}|}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|} \mathrm{e}^{\mathrm{i}[(b_1'-b_1)]\phi} |\vec{b}\rangle\langle\vec{b}'| \\ & \times \sum_{\vec{d} \in \mathcal{D}(\vec{b}, \vec{b}')} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum_{k=1}^N (k-1)(d_k - b_k \oplus d_k \oplus b_k')} \left(\frac{t}{M}\right)^{|\vec{d}|} (1-t)^{|\vec{b}|-|\vec{d}|} \\ & \times \sum_{\vec{f} \in \mathcal{F}(\vec{d})}^{2^N-1} \binom{|\vec{b} \oplus \vec{d} \oplus \vec{b}'| - b_1 \oplus d_1 \oplus b_1'}{|\vec{f}| - b_1 \oplus d_1 \oplus b_1'}^{*} |\vec{f}|!\,(|\vec{d}| - |\vec{f}|)!(\cos\theta)^{2|\vec{f}| - d_1 - d_1 \oplus b_1 \oplus b_1'} (\sin\theta)^{2(|\vec{d}| - |\vec{f}|)}, \end{aligned} \tag{B.16}$$

where the asterisk on the binomial coefficient means that it is defined as zero if $|\vec{f}| = 0$ and $b_1 \oplus d_1 \oplus b_1' = 1$. Finally, since every term just depends on $|\vec{f}|$, we can sum over all the vectors $\vec{f}$ with equal Hamming weight and obtain the final expression for the conditional state of the qubits when detector D_j clicked:

$$\begin{aligned} p_j \rho^j_{A_1 \ldots A_N} = & \sum_{\substack{g(\vec{b}), g(\vec{b}')=1 \\ |\vec{b}'|=|\vec{b}|}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|} \mathrm{e}^{\mathrm{i}[(b_1'-b_1)]\phi} |\vec{b}\rangle\langle\vec{b}'| \\ & \times \sum_{\vec{d} \in \mathcal{D}(\vec{b}, \vec{b}')} \mathrm{e}^{\mathrm{i}\frac{2\pi}{M}(j-1)\sum\limits_{k=1}^{N} (k-1)(d_k - b_k \oplus d_k \oplus b_k')} \left(\frac{t}{M}\right)^{|\vec{d}|} (1-t)^{|\vec{b}|-|\vec{d}|} \\ & \times \sum_{m=d_1}^{|\vec{d}|} \binom{|\vec{d}| - d_1}{m - d_1} \binom{|\vec{b} \oplus \vec{d} \oplus \vec{b}'| - b_1 \oplus d_1 \oplus b_1'}{m - b_1 \oplus d_1 \oplus b_1'}^{*} \\ & \times m!\,(|\vec{d}| - m)!(\cos\theta)^{2m - d_1 - d_1 \oplus b_1 \oplus b_1'} (\sin\theta)^{2(|\vec{d}| - m)}. \end{aligned} \tag{B.17}$$

B.2. Probability of exactly one click

We can now compute the probability p_j of having just one click in detector D_j by simply computing the trace of both sides in (B.17):

$$\begin{aligned} p_j = & \sum_{g(\vec{b})=1}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|} \sum_{g(\vec{d})=1:\ \vec{d} \wedge \vec{b} = \vec{d}}^{2^N-1} \left(\frac{t}{M}\right)^{|\vec{d}|} (1-t)^{|\vec{b}|-|\vec{d}|} \\ & \times \sum_{m=d_1}^{|\vec{d}|} \left[\binom{|\vec{d}| - d_1}{m - d_1}\right]^2 m!\,(|\vec{d}| - m)!(\cos\theta)^{2(m-d_1)} (\sin\theta)^{2(|\vec{d}| - m)}. \end{aligned} \tag{B.18}$$

In order to obtain an easier expression to compute, we distinguish the cases: $b_1 = 0$, $b_1 = 1$ and the special case $\vec{b} = 100 \ldots 0$:

$$\begin{aligned}
p_j = {} & \sum_{\substack{g(\vec{b})=2\\ b_1=0}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|} \sum_{\substack{g(\vec{d})=2:\ \vec{d}\wedge\vec{b}=\vec{d}\\ d_1=0}}^{2^N-1} \left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\\
& \times \sum_{m=0}^{|\vec{d}|}\left[\binom{|\vec{d}|}{m}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2m}(\sin\theta)^{2(|\vec{d}|-m)}\\
& + q^{N-1}(1-q)\left(\frac{t}{M}\right) \qquad \text{(this term comes from: } \vec{b}=100\ldots0,\ \vec{d}=100\ldots0)\\
& + \sum_{\substack{g(\vec{b})=3\\ b_1=1}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\\
& \times \left[\sum_{\substack{g(\vec{d})=1:\ \vec{d}\wedge\vec{b}=\vec{d}\\ d_1=1}}^{2^N-1} \left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\sum_{m=1}^{|\vec{d}|}\left[\binom{|\vec{d}|-1}{m-1}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2(m-1)}(\sin\theta)^{2(|\vec{d}|-m)}\right.\\
& \left. + \sum_{\substack{g(\vec{d})=2:\ \vec{d}\wedge\vec{b}=\vec{d}\\ d_1=0}}^{2^N-1} \left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\sum_{m=0}^{|\vec{d}|}\left[\binom{|\vec{d}|}{m}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2m}(\sin\theta)^{2(|\vec{d}|-m)}\right]. \qquad \text{(B.19)}
\end{aligned}$$

We can now partially sum over the vectors $\vec{d}$ since the terms in the sums only depend on the Hamming weight of these vectors:

$$\begin{aligned}
p_j = {} & \sum_{\substack{g(\vec{b})=2\\ b_1=0}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\sum_{|\vec{d}|=1}^{|\vec{b}|}\binom{|\vec{b}|}{|\vec{d}|}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\\
& \times \sum_{m=0}^{|\vec{d}|}\left[\binom{|\vec{d}|}{m}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2m}(\sin\theta)^{2(|\vec{d}|-m)} + q^{N-1}(1-q)\left(\frac{t}{M}\right)\\
& + \sum_{\substack{g(\vec{b})=3\\ b_1=1}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\\
& \times \left[\sum_{|\vec{d}|=1}^{|\vec{b}|}\binom{|\vec{b}|-1}{|\vec{d}|-1}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\sum_{m=1}^{|\vec{d}|}\left[\binom{|\vec{d}|-1}{m-1}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2(m-1)}(\sin\theta)^{2(|\vec{d}|-m)}\right.\\
& \left. + \sum_{|\vec{d}|=1}^{|\vec{b}|-1}\binom{|\vec{b}|-1}{|\vec{d}|}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\sum_{m=0}^{|\vec{d}|}\left[\binom{|\vec{d}|}{m}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2m}(\sin\theta)^{2(|\vec{d}|-m)}\right].
\end{aligned}$$

(B.20)

By employing the following identity:

$$\begin{aligned}
& \sum_{m=0}^{|\vec{d}|}\left[\binom{|\vec{d}|}{m}\right]^2 m!(|\vec{d}|-m)!(\cos\theta)^{2m}(\sin\theta)^{2(|\vec{d}|-m)} = |\vec{d}|!\sum_{m=0}^{|\vec{d}|}\binom{|\vec{d}|}{m}(\cos\theta)^{2m}(\sin\theta)^{2(|\vec{d}|-m)}\\
& = |\vec{d}|!(\sin^2\theta+\cos^2\theta)^{|\vec{d}|} = |\vec{d}|!, \qquad \text{(B.21)}
\end{aligned}$$

both in the second and last row of (B.20), we get the following expression:

$$\begin{aligned}
p_j = {} & \sum_{\substack{g(\vec{b})=2\\ b_1=0}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\sum_{l=1}^{|\vec{b}|}\binom{|\vec{b}|}{l}\left(\frac{t}{M}\right)^{l}(1-t)^{|\vec{b}|-l}l! + q^{N-1}(1-q)\left(\frac{t}{M}\right) + \sum_{\substack{g(\vec{b})=3\\ b_1=1}}^{2^N-1} q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\\
& \times \left[\sum_{l=0}^{|\vec{b}|-1}\binom{|\vec{b}|-1}{l}\left(\frac{t}{M}\right)^{l+1}(1-t)^{|\vec{b}|-l-1}\sum_{m=0}^{l}\left[\binom{l}{m}\right]^2(m+1)!(l-m)!(\cos\theta)^{2m}(\sin\theta)^{2(l-m)}\right.\\
& \left. + \sum_{l=1}^{|\vec{b}|-1}\binom{|\vec{b}|-1}{l}\left(\frac{t}{M}\right)^{l}(1-t)^{|\vec{b}|-l}l!\right].
\end{aligned}$$

(B.22)

The remaining sum over m can be similarly simplified as follows:

$$\sum_{m=0}^{l}\left[\binom{l}{m}\right]^2 (m+1)!(l-m)!(\cos\theta)^{2m}(\sin\theta)^{2(l-m)} = l!(1+l\cos^2\theta). \tag{B.23}$$

By substituting (B.23) into (B.22) and by partially summing over vectors $\vec{b}$ we obtain the final expression for the probability that only detector D_j clicks:

$$\begin{aligned}p_j = {}& Nq^{N-1}(1-q)\left(\frac{t}{M}\right) + \sum_{r=2}^{N-1}\binom{N-1}{r}q^{N-r}(1-q)^r\sum_{l=1}^{r}\binom{r}{l}\left(\frac{t}{M}\right)^l(1-t)^{r-l}l!\\ &+\sum_{r=2}^{N}\binom{N-1}{r-1}q^{N-r}(1-q)^r\left[\sum_{l=1}^{r}\binom{r-1}{l-1}\left(\frac{t}{M}\right)^l(1-t)^{r-l}(l-1)!(\sin^2\theta+l\cos^2\theta)\right.\\ &\left.+\sum_{l=1}^{r-1}\binom{r-1}{l}\left(\frac{t}{M}\right)^l(1-t)^{r-l}l!\right].\end{aligned} \tag{B.24}$$

We observe that the probability p_j that only detector D_j clicks is independent of the particular detector because of the symmetric action of the multiport beam splitter.

B.3. QBER

Starting from the conditional state (B.17), we can compute the QBER between Alice$_1$ and Alice$_k$'s outcomes when they measure their qubit in the eigenbasis of the operator $O_{XY}(\varphi_1)$ and $O_{XY}(\varphi_k)$, respectively, with $O_{XY}(\varphi) = \cos(\varphi)X + \sin(\varphi)Y$ (X and Y are the Pauli operators). The operator $O_{XY}(\varphi)$ has eigenvalues $\lambda = \pm 1$ and correspondent eigenvectors: $|\lambda\rangle_\varphi = \frac{1}{\sqrt{2}}(|0\rangle + \lambda e^{i\varphi}|1\rangle)$.

To start with, we compute the following quantity:

$$\langle\vec{b}'|P^{A_1}_{|+1\rangle_{\varphi_1}}\otimes P^{A_k}_{|-1\rangle_{\varphi_k}}|\vec{b}\rangle = \frac{1}{4}(e^{b_1'\,i\varphi_1})((-1)^{b_k'}e^{b_k'\,i\varphi_k})(e^{-b_1\,i\varphi_1})((-1)^{b_k}e^{-b_k\,i\varphi_k})\prod_{l\neq 1,k}\delta_{b_l,b_l'} \tag{B.25}$$

and we insert it into the probability that Alice$_1$ measured the outcome $+1$ and Alice$_k$ measured the outcome -1, when D_j clicked:

$$\begin{aligned}\mathrm{Tr}[P^{A_1}_{|+1\rangle_{\varphi_1}}\otimes P^{A_k}_{|-1\rangle_{\varphi_k}}\rho^j_{A_1,\ldots,A_N}] = {}& \frac{1}{p_j}\sum_{g(\vec{b})=1}^{2^N-1}\sum_{\vec{b}'\in\mathcal{Q}(\vec{b})}\frac{(-1)^{b_k+b_k'}}{4}e^{i(b_1'-b_1)(\varphi_1+\phi)}e^{(b_k'-b_k)i\varphi_k}q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\\ &\times\sum_{\vec{d}\in\mathcal{D}(\vec{b},\vec{b}')}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}e^{i\frac{2\pi}{M}(j-1)(k-1)(d_k-b_k\oplus b_k'\oplus d_k)}\\ &\times\sum_{m=d_1}^{|\vec{d}|}\binom{|\vec{d}|-d_1}{m-d_1}\binom{|\vec{b}\oplus\vec{d}\oplus\vec{b}'|-b_1\oplus d_1\oplus b_1'}{m-b_1\oplus d_1\oplus b_1'}^* m!\,(|\vec{d}|-m)!(\cos\theta)^{2m-d_1-d_1\oplus b_1\oplus b_1'}(\sin\theta)^{2(|\vec{d}|-m)},\end{aligned} \tag{B.26}$$

where $\mathcal{Q}(\vec{b})$ is a set of at most 2 binary vectors, defined as: $\mathcal{Q}(\vec{b}) = \{\vec{b}, \overline{b_1}b_2\ldots\overline{b_k}\ldots b_N(\text{iff } b_1\oplus b_k = 1)\}$[6]. This means that the sum over $\vec{b}'$ is reduced to just one term, namely $\vec{b}' = \vec{b}$, plus the possibility of a second term in which $\vec{b}'$ differs from $\vec{b}$ in position 1 and k, as long as the bits of vector $\vec{b}$ differ from each other in those positions. Now we compute the sum over $\vec{b}'$ as follows:

[6] The straight line over a bit indicates its negation.

$$\begin{aligned}
\mathrm{Tr}\,[P^{A_1}_{|+1\rangle_{\varphi_1}} \otimes P^{A_k}_{|-1\rangle_{\varphi_k}}\,\rho^{j}_{A_1,\ldots,A_N}] &= \frac{1}{p_j}\Bigg\{\sum_{g(\vec{b})=1}^{2^N-1}\frac{q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}}{4}\sum_{g(\vec{d})=1:\,\vec{d}\wedge\vec{b}=\vec{d}}^{2^N-1}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\\
&\times\sum_{m=d_1}^{|\vec{d}|}\left[\binom{|\vec{d}|-d_1}{m-d_1}\right]^2 m!\,(|\vec{d}|-m)!(\cos\theta)^{2(m-d_1)}\,(\sin\theta)^{2(|\vec{d}|-m)}\\
&-\sum_{g(\vec{b})=1:\,b_1\oplus b_k=1}^{2^N-1}\frac{q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}}{4}e^{\mathrm{i}(-1)^{b_1}(\varphi_1+\phi)+\mathrm{i}(-1)^{b_k}\varphi_k+\mathrm{i}\frac{2\pi}{M}(j-1)(k-1)(-1)^{b_k\oplus 1}}\\
&\times\sum_{\vec{d}\in\mathcal{D}(\vec{b},\overline{b_1}b_2\ldots\overline{b_k}\ldots b_N)}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\\
&\times\sum_{m=b_1}^{|\vec{d}|}\binom{|\vec{d}|-b_1}{m-b_1}\binom{|\vec{d}|-\overline{b_1}}{m-\overline{b_1}}^{*}m!(|\vec{d}|-m)!(\cos\theta)^{2m-1}\,(\sin\theta)^{2(|\vec{d}|-m)}\Bigg\},
\end{aligned}\tag{B.27}$$

where the set $\mathcal{D}(\vec{b},\,\overline{b_1}b_2\ldots\overline{b_k}\ldots b_N)$ simplifies to: $\mathcal{D}(\vec{b},\,\overline{b_1}b_2\ldots\overline{b_k}\ldots b_N)=\{\vec{d}\in g^{-1}([1,\,2^N-1]):\,\vec{d}\wedge\vec{b}=\vec{d},\ d_1=b_1,\ \ d_k=b_k\}$. We notice that the first addend in (B.27) is proportional to p_j (B.18):

$$\begin{aligned}
&\mathrm{Tr}\,[P^{A_1}_{|+1\rangle_{\varphi_1}} \otimes P^{A_k}_{|-1\rangle_{\varphi_k}}\,\rho^{j}_{A_1,\ldots,A_N}]\\
&=\frac{1}{4}-\frac{1}{4p_j}\sum_{g(\vec{b})=1:\,b_1\oplus b_k=1}^{2^N-1}q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\mathrm{e}^{\mathrm{i}(-1)^{b_1}(\varphi_1+\phi)+\mathrm{i}(-1)^{b_k}\varphi_k+\mathrm{i}\frac{2\pi}{M}(j-1)(k-1)(-1)^{b_k\oplus 1}}\\
&\sum_{\vec{d}\in\mathcal{D}(\vec{b},\overline{b_1}b_2\ldots\overline{b_k}\ldots b_N)}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\sum_{m=b_1}^{|\vec{d}|}\binom{|\vec{d}|-b_1}{m-b_1}\binom{|\vec{d}|-\overline{b_1}}{m-\overline{b_1}}^{*}m!(|\vec{d}|-m)!(\cos\theta)^{2m-1}\,(\sin\theta)^{2(|\vec{d}|-m)}.
\end{aligned}\tag{B.28}$$

Finally, we split the sums over $\vec{b}$ in the two sub-cases: $b_1=1, b_k=0$ and $b_1=0, b_k=1$ and we notice that the two contributions differ only in the exponential term. By summing the two contributions, the exponential factor produces a cosine function and one gets:

$$\begin{aligned}
\mathrm{Tr}\,[P^{A_1}_{|+1\rangle_{\varphi_1}} \otimes P^{A_k}_{|-1\rangle_{\varphi_k}}\,\rho^{j}_{A_1,\ldots,A_N}] &= \frac{1}{4}-\frac{2\cos\left[\left(\varphi_1+\phi-\varphi_k\right)+\frac{2\pi}{M}(j-1)(k-1)\right]}{4p_j}\\
&\times\sum_{|\vec{b}|=1}^{N-1}\binom{N-2}{|\vec{b}|-1}q^{N-|\vec{b}|}(1-q)^{|\vec{b}|}\sum_{|\vec{d}|=1}^{|\vec{b}|}\binom{|\vec{b}|-1}{|\vec{d}|-1}\left(\frac{t}{M}\right)^{|\vec{d}|}(1-t)^{|\vec{b}|-|\vec{d}|}\\
&\times\sum_{m=1}^{|\vec{d}|}\binom{|\vec{d}|}{m}\binom{|\vec{d}|-1}{m-1}m!(|\vec{d}|-m)!(\cos\theta)^{2m-1}\,(\sin\theta)^{2(|\vec{d}|-m)}\\
&=\frac{1}{4}-\frac{\cos\left[\left(\varphi_1+\phi-\varphi_k\right)+\frac{2\pi}{M}(j-1)(k-1)\right]}{2p_j}\\
&\times\sum_{r=0}^{N-2}\binom{N-2}{r}q^{N-r-1}(1-q)^{r+1}\sum_{l=0}^{r}\binom{r}{l}\left(\frac{t}{M}\right)^{l+1}(1-t)^{r-l}(l+1)!\sum_{m=0}^{l}\binom{l}{m}(\cos\theta)^{2m+1}\,(\sin\theta)^{2(l-m)}\\
&=\frac{1}{4}-\frac{1}{2p_j}\cos\left[\left(\varphi_1+\phi-\varphi_k\right)+\frac{2\pi}{M}(j-1)(k-1)\right]\cos\theta\\
&\times\sum_{r=0}^{N-2}\binom{N-2}{r}q^{N-r-1}(1-q)^{r+1}\sum_{l=0}^{r}\binom{r}{l}\left(\frac{t}{M}\right)^{l+1}(1-t)^{r-l}(l+1)!
\end{aligned}\tag{B.29}$$

In a similar fashion, one computes the probability of A_1 measuring the outcome -1 and A_k measuring the outcome $+1$ and obtains an identical expression to (B.29). In conclusion, the QBER conditioned on D_j clicking is given by twice the probability given in (B.29).

By fixing the angles φ_1 and φ_k as mentioned in the protocol's description: $\varphi_1=0$ and $\varphi_k=\arg(U_{kj})=\frac{2\pi}{M}(k-1)(j-1)$ we minimize the QBER and thus increase the secret key rate. This requires Alice$_k$ to adjust her measurement depending on which detector clicked, implying that such measurement does not commute with the operations performed by node C. On the other hand, the QBER is now minimal and reads the same regardless of which couple (A_1, A_k) one considers or which detector D_j clicks:

$$Q_{A_1A_k} = \frac{1}{2} - \frac{1}{p_j}\cos\phi\cos\theta\sum_{r=0}^{N-2}\binom{N-2}{r}q^{N-r-1}(1-q)^{r+1}\sum_{l=0}^{r}\binom{r}{l}(l+1)!\left(\frac{t}{M}\right)^{l+1}(1-t)^{r-l}, \tag{B.30}$$

where p_j is given in (B.24).

B.4. Phase-error rate

Finally we compute the phase-error rate, defined as the probability that the product of the Z-measurement results of all the parties equals $+1$ (i.e. the qubit of an even number of parties collapsed in state $|1\rangle$, which corresponds to the outcome $Z = -1$):

$$Q_Z = \Pr\left[\prod_{k=1}^{N} Z_{A_k} = 1\right] = \mathrm{Tr}\left[\left(\sum_{\substack{g(\vec{f})=3 \\ |\vec{f}|\ \mathrm{even}}}^{2^N-1} P_{|\vec{f}\rangle}\right)\rho^j_{A_1,\ldots,A_N}\right], \tag{B.31}$$

where the quantum state $\rho^j_{A_1,\ldots,A_N}$ conditioned on detector D_j clicking is given in (B.17) and the case $g(\vec{f}) = 0$ is excluded since $|\vec{0}\rangle$ does not appear in (B.17). By following analogous steps to those presented in appendix B.2 we obtain the following expression for the phase-error rate:

$$\begin{aligned} Q_Z = & \frac{1}{p_j}\sum_{r=1}^{\lfloor\frac{N-1}{2}\rfloor}\binom{N-1}{2r}q^{N-2r}(1-q)^{2r}\sum_{l=1}^{2r}\binom{2r}{l}\left(\frac{t}{M}\right)^{l}(1-t)^{2r-l}l! \\ & + \frac{1}{p_j}\sum_{r=1}^{\lfloor\frac{N}{2}\rfloor}\binom{N-1}{2r-1}q^{N-2r}(1-q)^{2r}\left[\sum_{l=1}^{2r-1}\binom{2r-1}{l}\left(\frac{t}{M}\right)^{l}(1-t)^{2r-l}l!\right. \\ & \left. + \sum_{l=1}^{2r}\binom{2r-1}{l-1}\left(\frac{t}{M}\right)^{l}(1-t)^{2r-l}(l-1)!(\sin^2\theta + l\cos^2\theta)\right]. \end{aligned} \tag{B.32}$$

B.5. Dark counts

So far we computed the quantities p_j, $Q_{A_1A_k}$ and Q_Z assuming that every click in the detectors is due to the arrival of one or more photons. By naming Ω_{ph} the event in which one or more photons arrive at detector D_j and no other photon arrives at any other detector, we can formally express the computed quantities as:

$$p_j = \Pr(\Omega_{\mathrm{ph}}), \tag{B.33}$$

$$Q_{A_1A_k} = \Pr(A_1 \neq A_k|\Omega_{\mathrm{ph}}), \tag{B.34}$$

$$Q_Z = \Pr\left(\prod_{k=1}^{N} Z_{A_k} = 1|\Omega_{\mathrm{ph}}\right). \tag{B.35}$$

For the setup presented in section 1 and the channel model described at the beginning of this section, the explicit expressions of (B.33), (B.34) and (B.35) are given in (B.24), (B.30) and (B.32), respectively.

We now assume that every detector is characterized by a probability p_d of clicking conditioned on no photon arriving. We also define Ω_{click} to be the event in which only detector D_j clicks and $\Omega_{\mathrm{no\ ph}}$ to be the event in which no photon arrives at any detector. Then, the error rates $Q^{\mathrm{dc}}_{A_1A_k}$ and Q^{dc}_Z and the probability p^{dc}_j that enter the key rate formula and that model the correspondent observed quantities read as follows:

$$p^{\mathrm{dc}}_j = \Pr(\Omega_{\mathrm{click}}) = p_j(1-p_d)^{M-1} + p_d(1-p_d)^{M-1}\Pr(\Omega_{\mathrm{no\ ph}}) \tag{B.36}$$

$$\begin{aligned} Q^{\mathrm{dc}}_{A_1A_k} &= \Pr(A_1 \neq A_k|\Omega_{\mathrm{click}}) \\ &= \frac{1}{p^{\mathrm{dc}}_j}[\Pr(A_1 \neq A_k|\Omega_{\mathrm{no\ ph}})\Pr(\Omega_{\mathrm{no\ ph}})p_d(1-p_d)^{M-1} + Q_{A_1A_k}\,p_j(1-p_d)^{M-1}] \end{aligned} \tag{B.37}$$

$$\begin{aligned} Q^{\mathrm{dc}}_Z &= \Pr\left(\prod_{k=1}^{N} Z_{A_k} = 1|\Omega_{\mathrm{click}}\right) \\ &= \frac{1}{p^{\mathrm{dc}}_j}\left[\Pr\left(\prod_{k=1}^{N} Z_{A_k} = 1|\Omega_{\mathrm{no\ ph}}\right)\Pr(\Omega_{\mathrm{no\ ph}})p_d(1-p_d)^{M-1} + Q_Z\,p_j(1-p_d)^{M-1}\right], \end{aligned} \tag{B.38}$$

where p_j, $Q_{A_1A_k}$ and Q_Z are defined in (B.33), (B.34) and (B.35), respectively, while the probabilities related to the arrival of no photon read:

$$\Pr(\Omega_{\text{no ph}}) = (q + (1-q)(1-t))^N \tag{B.39}$$

$$\Pr(A_1 \neq A_k|\Omega_{\text{no ph}}) = \frac{1}{2} \tag{B.40}$$

$$\Pr\left(\prod_{k=1}^{N} Z_{A_k} = 1|\Omega_{\text{no ph}}\right) = \frac{1}{\Pr(\Omega_{\text{no ph}})}\sum_{l=0}^{\lfloor \frac{N}{2} \rfloor}\binom{N}{2l} q^{N-2l}(1-q)^{2l}(1-t)^{2l}. \tag{B.41}$$

The probabilities (B.39), (B.40) and (B.41) are obtained by following similar steps to those presented in this section and that led to the final expressions for p_j, $Q_{A_1A_k}$ and Q_Z, respectively. The starting point in this case is the conditional state of the qubits when no photon arrived at any detector:

$$\Pr(\Omega_{\text{no ph}})\rho^{\text{no ph}}_{A_1\ldots A_N} = \mathrm{Tr}_{\substack{\sigma_1,\ldots,\sigma_M\\ l_1,\ldots,l_N}}[\otimes_{i=1}^{M} P_{|0\rangle_{\sigma_i}}|\Phi_4\rangle\langle\Phi_4|\otimes_{i=1}^{M} P_{|0\rangle_{\sigma_i}}]. \tag{B.42}$$

Appendix C. Optimized CKA

Although we have shown in section 4 that a truly multipartite QKD scheme can outperform the iterative use of any bipartite QKD scheme in the direct-transmission scenario (i.e. the central node is removed), this does not necessarily hold when one has at hand the CKA experimental setup and uses it to perform bipartite QKD protocols. In other words, it might be possible to outperform the multipartite CKA by iteratively executing its bipartite version (fix $N = 2$ in equation (3.4)) between one selected party and all the other $N - 1$ users, and then using the established secret keys to encode the final conference key via one-time pad encryption. In this case the asymptotic conference key rate would be $r(2)/(N-1)$ according to the reasoning given at the beginning of section 4, where $r(N)$ is given in (3.4). More generally, it might be advantageous to group the N parties in subsets of equal cardinality, let them perform the CKA within the subset, and then use the secret keys established in each subset to encode the conference key. Since one selected party must belong to every subset in order to distribute the final conference key to the others in a secure way, there are $(N-1)/d$ subsets of $d+1$ users each. In this case the asymptotic conference key rate would read: $d \cdot r(d+1)/(N-1)$. In order to investigate which of these configurations yields the highest asymptotic conference key rate, we optimize the rate with respect to the possible subdivisions of the N parties in groups of equal cardinality (i.e. we maximize it with respect to all the divisors d of $N-1$):

$$r_{\text{opt}}(N) = \max_{d|N-1}\frac{d}{N-1}r(d+1), \tag{C.1}$$

which includes the cases where the parties are iteratively performing bipartite protocols ($d = 1$) and where the N parties are performing the CKA all at once like in figure 2 ($d = N - 1$).

In figure C1(a) we plot the optimized conference key rate for $N = 5$ parties (equation (C.1), solid lines) as a function of the loss in each quantum channel, for different fixed values of the parameter q and a fixed number of input (output) ports of the beam splitter: $M = 5$. We also plot the direct transmission bound (4.1) for the same number of parties. The correspondent optimal number of parties within each subset depends on the loss and on the value of q, and it is given in figure C1(b).

From figure C1(a) we observe that the resulting key rate, although not being optimized over the parameter q, is similar to the $N = 5$ key rate in figure 2 for most losses, since we fixed q to values close to the optimal ones. Furthermore, it performs better than the standard CKA with five parties in the high-loss region. Indeed, as already explained in figure 2, the effect of dark counts becomes greater when more parties are performing the CKA at the same time. Thus, allowing for a lower number of parties within each subset increases the maximum tolerated loss.

In figure C1(b) we observe that at low losses it is optimal for the five parties to perform a truly multipartite scheme rather than iteratively performing bipartite protocols. The reason is that in the ideal scenario of extremely low losses ($t \longrightarrow 1$) and q close to 1, there is only one party successfully sending one photon to the central node to be detected. In this case the post-selected state shared by the parties is the W-class state used for establishing the secret key. Of course, there are more chances that this event is going to happen when more parties are involved, thus a multipartite scheme is advantageous with respect to an iteration of bipartite schemes. One can see this also analytically, by showing that the asymptotic rate (3.4) of the CKA performed by N parties all at once can be approximated as follows (when the above assumptions hold):

$$r(N) \simeq Nq^{N-1}(1-q)t\left[1 - h\left(\frac{1}{2} - \frac{1}{N}\right)\right], \tag{C.2}$$

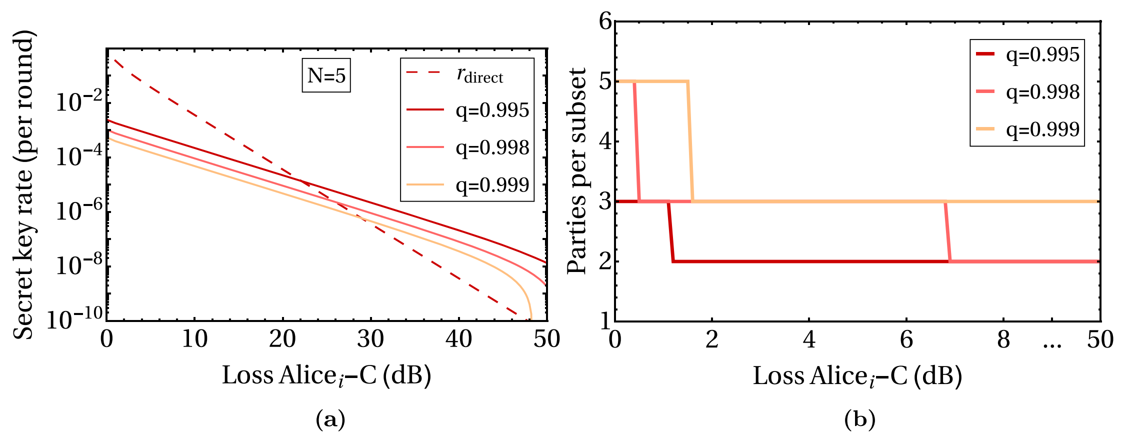

Figure C1. (a) The optimized conference key rate (equation (C.1), solid lines) as a function of the loss in the channel linking one party to the central node, for different fixed values of q: $q = 0.995, 0.998$ and 0.999 (top to bottom). We also plot the direct transmission bound (equation (4.1), dashed line) for five parties. We observe that the optimized key rate outperforms the standard CKA especially at high losses (compare with the case $N = 5$ in figure 2), since having a lower number of parties taking part to the CKA all at once reduces the negative effect of dark counts. (b) The optimal number of parties belonging to the subsets in which the total number of users ($N = 5$) have been subdivided, as a function of the loss in one quantum channel, for different fixed values of q: $q = 0.995, 0.998$ and 0.999 (bottom to top). We observe that performing a truly multipartite scheme could be optimal especially at low losses, i.e. when the parties' shared state is well approximated by a multipartite W state. We optimize the conference key rate achieved by $N = 5$ parties over the cardinality of the subsets of parties performing the CKA all at once. The different keys established within each subgroup (which can be composed of either two, three or five parties each) are then used to encode the final conference key.

while the rate achieved by subdividing the task in $N - 1$ bipartite schemes is:

$$r_{\text{bipartite}}(N) \simeq \frac{2q(1-q)t}{N-1}. \tag{C.3}$$

By numerically comparing (C.2) with (C.3) for sufficiently high values of q, one notices that the former results in a higher key rate. When the value of q decreases, the probability that two or more parties send their photon to the central node increases, reducing the key rate. Being such events more likely when more parties are involved, the iterative execution of bipartite schemes is favored. Similarly, increasing the loss transforms the same events—which are more likely with more parties—from neglected events (if they cause double clicks) to harmful events (when some photons get lost in the transmission), thus favoring the iteration of schemes with a low number of parties.

ORCID iDs

Federico Grasselli https://orcid.org/0000-0003-2966-7813

References

[1] Gisin N and Thew R 2007 *Nat. Photon.* **1** 165–71
[2] Kimble H J 2008 *Nature* **453** 1023
[3] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Scarani V, Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[6] Lo H-K, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595–604
[7] Diamanti E, Lo H-K, Qi B and Yuan Z 2016 *NPJ Quantum Inf.* **2** 16025
[8] Pirandola S *et al* 2019 arXiv:1906.01645
[9] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[10] Abruzzo S, Kampermann H and Bruß D 2014 *Phys. Rev.* A **89** 012301
[11] Panayi C, Razavi M, Ma X and Lütkenhaus N 2014 *New J. Phys.* **16** 043005
[12] Azuma K, Tamaki K and Munro W J 2015 *Nat. Commun.* **6** 10171
[13] Vazirani U and Vidick T 2014 *Phys. Rev. Lett.* **113** 140501
[14] Friedman R A, Dupuis F, Fawzi O, Renner R and Vidick T 2018 *Nat. Commun.* **9** 459
[15] Yin H-L *et al* 2016 *Phys. Rev. Lett.* **117** 190501
[16] Boaron A *et al* 2018 *Phys. Rev. Lett.* **121** 190502
[17] Liao S-K *et al* 2017 *Nature* **549** 43
[18] Takenaka H *et al* 2017 *Nat. Photon.* **11** 502
[19] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[20] Tamaki K, Lo H-K, Wang W and Lucamarini M 2018 arXiv:1805.05511
[21] Ma X, Zeng P and Zhou H 2018 *Phys. Rev.* X **8** 031043

[22] Cui C *et al* 2019 *Phys. Rev. Appl.* **11** 034053
[23] Lin J and Lütkenhaus N 2018 *Phys. Rev.* A **98** 042332
[24] Curty M, Azuma K and Lo H-K 2019 *NPJ Quantum Inf.* **5** 64
[25] Zhou X-Y, Zhang C-H, Zhang C-M and Wang Q 2019 *Phys. Rev.* A **99** 062316
[26] Grasselli F and Curty M 2019 *New J. Phys.* **21** 073001
[27] Grasselli F, Navarrete A and Curty M 2019 *New J. Phys.* **21** 113032
[28] Liu Y *et al* 2019 *Phys. Rev. Lett.* **123** 100505
[29] Minder M, Pittaluga M, Roberts G L, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2019 *Nat. Photon.* **13** 334–8
[30] Zhong X, Hu J, Curty M, Qian L and Lo H-K 2019 *Phys. Rev. Lett.* **123** 100506
[31] Wang S *et al* 2019 *Phys. Rev.* X **9** 021046
[32] Takeoka M, Guha S and Wilde M M 2014 *Nat. Commun.* **5** 5235
[33] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[34] Fu Y, Yin H-L, Chen T-Y and Chen Z-B 2015 *Phys. Rev. Lett.* **114** 090501
[35] Epping M, Kampermann H, Macchiavello C and Bruß D 2017 *New J. Phys.* **19** 093012
[36] Ribeiro J, Murta G and Wehner S 2018 *Phys. Rev.* A **97** 022307
[37] Grasselli F, Kampermann H and Bruß D 2018 *New J. Phys.* **20** 113014
[38] Jo Y and Son W 2019 *OSA Continuum* **2** 814–26
[39] Ottaviani C, Lupo C, Laurenza R and Pirandola S 2019 *Commun. Phys.* **2** 118
[40] Augusiak R and Horodecki P 2009 *Phys. Rev.* A **80** 042307
[41] Bäuml S and Azuma K 2017 *Quantum Sci. Technol.* **2** 024004
[42] Dür W, Vidal G and Cirac J I 2000 *Phys. Rev.* A **62** 062314
[43] Żukowski M, Zeilinger A and Horne M A 1997 *Phys. Rev.* A **55** 2564
[44] Lim Y L and Beige A 2005 *Phys. Rev.* A **71** 062311
[45] Peruzzo A, Laing A, Politi A, Rudolph T and O'Brien J L 2011 *Nat. Commun.* **2** 224
[46] Spagnolo N *et al* 2013 *Nat. Commun.* **4** 1606
[47] Clements W R *et al* 2016 *Optica* **3** 1460–5
[48] Tabia G N M 2012 *Phys. Rev.* A **86** 062107
[49] Bernien H *et al* 2013 *Nature* **497** 86–90
[50] Rozpedek F *et al* 2019 *Phys. Rev.* A **99** 052330
[51] Abobeih M H, Cramer J, Bakker M A, Kalb N, Markham M, Twitchen D J and Taminiau T H 2018 *Nat. Commun.* **9** 2552
[52] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[53] Sheridan L, Le T P and Scarani V 2010 *New J. Phys.* **12** 123019
[54] Tomamichel M, Lim C, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[55] Curty M, Xu F, Cui W, Lim C, Tamaki K and Lo H-K 2014 *Nat. Commun.* **5** 3732
[56] Yin H-L and Chen Z-B 2019 *Sci. Rep.* **9** 17113
[57] Lu F-Y *et al* 2019 arXiv:1901.04264
[58] Tomamichel M and Renner R 2011 *Phys. Rev. Lett.* **106** 110506
[59] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634

F Experimental quantum conference key agreement

Title:	Experimental quantum conference key agreement
Authors:	Massimiliano Proietti, Joseph Ho, Federico Grasselli, Peter Barrow, Mehul Malik and Alessandro Fedrizzi
Journal:	Nature Photonics
Impact factor:	25.86 (2018)
Date of submission:	3 February 2020
Publication status:	Under review
Contribution by FG:	Third author (input approx. 10%)

This publication corresponds to reference [Pro+20]. A summary of its content is presented in chapter 7.

The research project was conceived and developed by my co-authors in their quantum optics laboratory at Heriot-Watt university and consisted in implementing the CKA that I devised in [GKB18]. My initial contribution was to provide the optimal values of some input parameters of the experiment in order to maximize the protocol's key rate. I obtained these values from self-produced numerical simulations of the protocol effectively implemented in the lab. During the course of the project I provided support on the security aspects of its implementation and I contributed to establishing the custom multiparty error correction scheme that was used to correct the parties' raw keys. Finally, I wrote the second section of the Supplementary Information attached to the paper and proofread the whole manuscript.

arXiv:2002.01491v1 [quant-ph] 4 Feb 2020

Experimental quantum conference key agreement

Massimiliano Proietti†,[1] Joseph Ho†,[1] Federico Grasselli,[2] Peter Barrow,[1] Mehul Malik,[1] and Alessandro Fedrizzi[1]

[1] *Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK*

[2] *Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany*

Future quantum networks will enable long-distance quantum key distribution (QKD) by providing on-demand entanglement to arbitrary combinations of users [1–4]. Paradigmatic QKD protocols establish secure keys between pairs of users, however when more than two parties want to communicate, recently introduced quantum conference quantum key agreement (CKA) protocols can drastically outperform 2-party primitives in terms of resource cost [5–11]. Here we implement a four-user quantum CKA protocol using polarisation-encoded Greenberger-Horne-Zeilinger (GHZ) entangled states generated by high-brightness, telecom photon-pair sources. We distribute these states over fibre connections of up to 50km length and implement custom multi-party error correction and privacy amplification on the resulting raw keys. From a finite-key analysis, we establish an information-theoretic secure key of up to 1.15×10^6 bits, which is used to encrypt and securely share an image between the four users. Surpassing the previous maximum distance for GHZ state transmission [12] by more than an order of magnitude, these results demonstrate the viability of network protocols relying on multi-partite entanglement. Future applications beyond quantum CKA include entanglement-assisted remote clock-synchronization [13, 14], quantum secret sharing [15], and GHZ-based repeater protocols [16].

Conference key agreement is a multi-user protocol for sharing a common information-theoretic secure key beyond the two-party paradigm [5]. This key allows group-wide encryption for authenticated users to communicate securely, wherein exclusively members of the group can decrypt messages broadcast by any other member. The canonical approach to distribute a conference key is to iterate two-party QKD (2QKD) primitives to establish secret keys between pairs of users in the group, followed by an additional bitwise XOR operation per pair of users transforming the unique keys into a common secret key [17, 18]. An alternative approach is to share genuine multi-partite GHZ-entangled states [7, 8] between users of the group, enabling the direct extraction of the conference key without requiring this additional step. Remarkably, quantum CKA can outperform 2QKD when N users are arranged within some general network with constrained channel capacity and quantum routers [7–11]. Furthermore, quantum network coding schemes [4] allow the distillation of a shared N-user GHZ state from a single network use, reducing the resource cost—and thus increasing the key rate—achievable in quantum CKA by a factor (N-1) [7] when compared with distilling the required number of 2QKD key pairs.

Here we experimentally demonstrate the salient features of the N-BB84 protocol introduced in [8] with a state-of-the-art photonic platform. An untrusted quantum server prepares and distributes L rounds of the maximally entangled GHZ state, $|GHZ\rangle \equiv (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$, to N participants in the network. In our work we implement a four-party protocol consisting of: Alice (A), Bob 1 (B_1), Bob 2 (B_2), and Bob 3 (B_3), see Fig. 1 (a). Each user performs quantum measurements on their respective photon in either the Z-basis $\{|0\rangle, |1\rangle\}$ constituting type-1 rounds, or the X-basis $\{|+\rangle \doteq (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle \doteq (|0\rangle - |1\rangle)/\sqrt{2}\}$ for type-2 rounds. Type-1 rounds are used to obtain the raw key as these measurements ensure all users in the protocol obtain the same bit value, in the absence of noise, owing to the structure of the GHZ state. Type-2 rounds are carried out randomly with probability p, for a total of $m = L \cdot p$ rounds, and are used to detect the presence of an eavesdropper. Users coordinate the measurement sequence using $L \cdot h(p)$ bits of a pre-shared key. In particular, one user generates the L-bit string indicating the measurement type of each round. The string can be classically compressed, shared, and decompressed by the other parties. Note that the values of p are typically on the order of 0.02, leading to a small value of $h(p)$, i.e., the amount of information to be initially pre-shared is small.

Once the measurements are complete, users proceed to verify the security of their key by performing parameter estimation. All users announce their outcomes for a subset of the type-1 rounds, m in total and randomly chosen, and all m type-2 rounds to determine

† These two authors contributed equally.

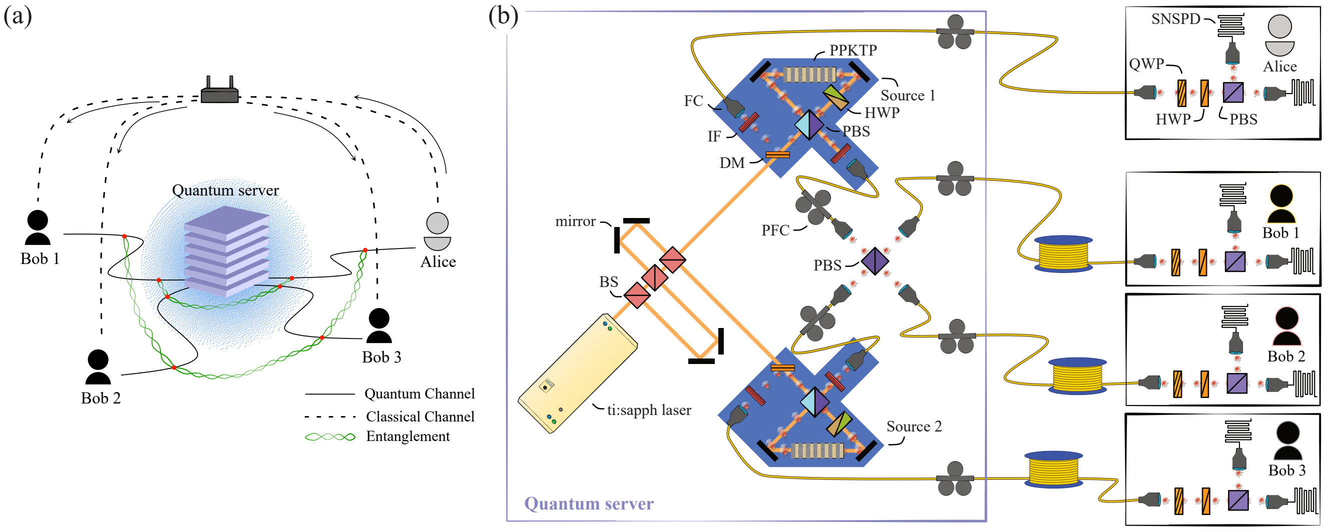

FIG. 1. **(a) Quantum conference key agreement scheme**. A quantum server distributes entangled GHZ states to Alice, who initiates the protocol, and Bobs 1, 2, and 3. They establish a common key from a pre-agreed sequence of Z measurements while checking the security by measuring X. **(b) Experimental setup.** A mode-locked picosecond laser (ti:sapph) multiplexed to 320 MHz repetition rate supplies two entangled photon sources which are based on parametric downconversion in periodically poled KTP crystals (PPKTP), pumped bidirectionally in a Sagnac loop for producing polarisation-entangled Bell pairs [19]. Down-converted photons are separated from the pump with dichroic mirrors (DM) and coupled into fibres (FC). One photon from each source non-classically interfere on a polarising beamsplitter (PBS) creating the four-photon GHZ state, see Methods for details. Each user receives their photon via single-mode fibres and performs projective measurements in the Z(X) basis by using a quarter- (QWP) and half-wave plate (HWP), and a polarising beamsplitter (PBS) before detection with superconducting nanowire single-photon detectors (SNSPD). Detection events are time-tagged and counted in coincidence within a 1 ns time window.

$Q^m_{\mathrm{AB}_i} = \left(1 - \left\langle \sigma_z^{\mathrm{A}} \sigma_z^{\mathrm{B}_i} \right\rangle\right)/2$ for $i = \{1,2,3\}$ and $Q^m_X = \left(1 - \left\langle \sigma_x^{\otimes 4} \right\rangle\right)/2$ respectively. We define the quantum bit error rate (QBER) as $\mathrm{QBER}^m \doteq \max Q^m_{\mathrm{AB}_i}$. All users retain $n = L - 2m$ bits forming the raw conference key, subsequently corrected with an error correction scheme and shortened with privacy amplification to ensure security. Finally, all users remove $L \cdot h\,(p)$ bits from their secret conference key to encode the pre-shared keys for subsequent protocols. Hence, our protocol is a key-growing routine, as in any known QKD scheme.

In our experiment, see Fig. 1(b), we employ two high-brightness, polarisation-entangled photon-pair sources [19] at telecommunication wavelength (1550 nm). We generate four-photon GHZ states by non-classically interfering one photon from each source on a PBS, which has success probability of 1/2 (see for example [20] or Methods for details). We use commercially available superconducting nanowire single-photon detectors (SNSPDs) with typical quantum efficiencies of > 80% at this wavelength.

We establish the upper bound on the performance of our protocol by assuming an infinite number of rounds can be performed, $L \to \infty$. In this asymptotic regime nearly all rounds are used to extract the raw key, $p \to 0$. We evaluate the asymptotic key rate (AKR) as the fraction of secret bits, ℓ, extracted from the total rounds [8]:

$$\mathrm{AKR} = \frac{\ell}{L} = 1 - h(Q_X) - h(\mathrm{QBER})\,, \qquad (1)$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon entropy. From Eq. 1 we note the AKR depends only on the noise parameters Q_X and QBER. We estimate these parameters experimentally using a large sample size of type-1 and type-2 measurements to minimise uncertainties. The results are shown in Fig. 2.

We denote the network topology as $\{d_1, d_2, d_3\}$, where d_i is the fibre length in kilometres between B_i and the server. Alice remains fixed at 2 m from the server in all cases. We implement four scenarios: $\{0,0,0\}$, $\{0,0,20\}$, $\{0,10,20\}$, and $\{20,10,20\}$, corresponding to measured network losses (in dB) of 0, 4.84, 7.57, and 11.77. The observed four-photon generation rates g_R for these scenarios are 40.89 Hz, 12.68 Hz, 6.31 Hz, and 2.03 Hz. In addition, for the finite-key analysis only, we consider a fifth asymmetric scenario $\{5,10,20\}$. The conference key rate is determined as a product of the fractional AKR and the recorded generation rates g_R. In all cases we observe similar noise parameters, and thus AKR, indicating that the entanglement quality is not degraded significantly by the transmission fibres. The experimental AKR is mainly limited by multiple-pair generations at the sources and by spectral impurities of the photons,

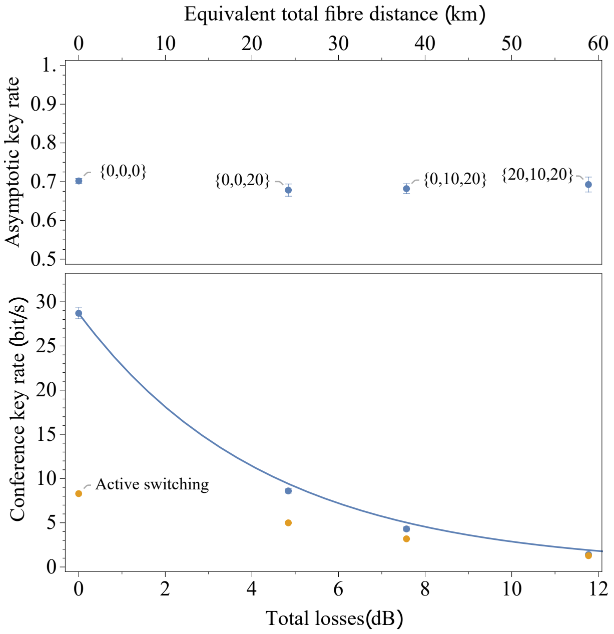

FIG. 2. **Asymptotic key rate results**. (top) We determine the fractional asymptotic key rate (AKR) by measuring Q_X and QBER without performing the full protocol. We evaluate AKR for a range of loss conditions set by the placement of fibre links in the network. (bottom) The conference key rate is plotted as a function of the total fibre length in the network. We include results of the generation rates with measurement-basis switching using our implementation, see Methods for details.

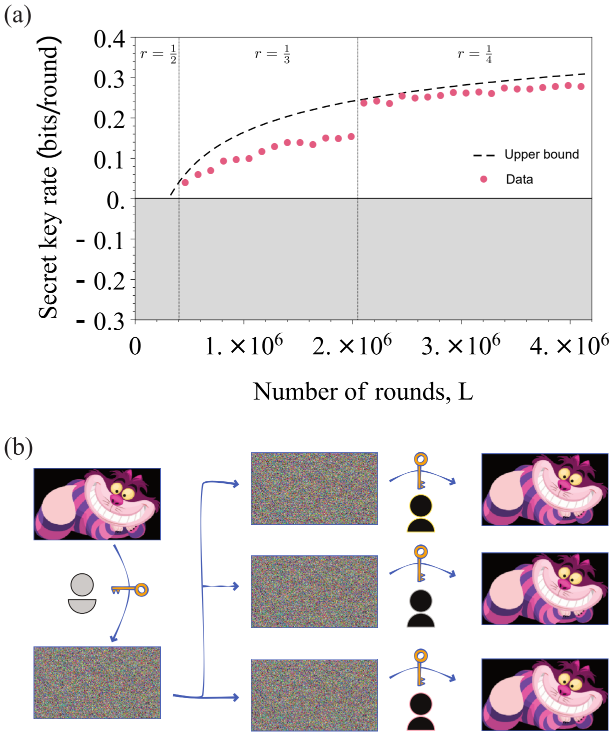

FIG. 3. **(a) Finite key results**. We implement all steps in the N-BB84 protocol for a range of L rounds to retrieve the final key of length ℓ and evaluate the secret key rate, $SKR = \ell/L$. In our experiment we employ LDPC codes with fixed code rates, r, using the estimated QBER in each run. We implement privacy amplification using Toeplitz matrices, then remove a portion of the final key for the pre-shared bits used to encode the measurement rounds. The upper bound given by Eq. 5 is shown compared with the experimental data. **(b) Encryption**. We generate an ϵ_{tot}-secure conference key of 1.15×10^6 bits. Using 1.06×10^6 bits, Alice encrypts an image (8-bit RGB, 280 by 158 pixels) employing a one-time-pad-like scheme. Alice sends the encrypted image over a public channel allowing only Bob 1, Bob 2, and Bob 3, who share the conference key, to decode the image.

see Supplementary Information (SI) for details. To the best of our knowledge, our work demonstrates for the first time the distribution of 1550 nm four-qubit entangled state in long telecom fibres, proving the viability of polarisation-encoded photons to remain highly entangled over long distances.

We also include the adjusted conference key rates when we perform the protocol with actively switched measurement bases. In our experiment, this is accomplished by rotating wave plates with motorised stages that are slow compared to the clock rate of our sources. As such, this leads to a reduced overall rate as shown in Fig. 2 (see Methods for details).

Our N-BB84 implementation operates at low rates and a complete finite-key analysis, where a fractional secret key rate (SKR) is adjusted to take into account finite statistics from parameter estimation, is crucial. For our experiment, we determine the optimal fraction of type-2 measurements to be $p = m/L = 0.012$. With this value of p, the amount of information reserved for the pre-shared key is $h(p) = 0.093$, see Methods for more details. Moreover, we set a total security parameter i.e. the maximal probability that an eavesdropper gains non-zero information about the key to be 1.8×10^{-8}, see SI for details. We implement the protocol in an asymmetric fibre network $\{5, 10, 20\}$ with a measured loss of 9.53 dB in total. We obtain over 4.09×10^6 type-1 rounds and 5.01×10^4 type-2 rounds during 177 hours of continuous measurement. Due to the long measurement time active polarisation feedback was implemented to minimise noise owing to thermal drifts in the laboratory (see Methods for details). Once the raw key is distilled by all users, we implement one-way error correction using low-density parity-check (LDPC) codes complying with the Digital Video Broadcasting (DVB-S2) standard [21]. The code was adapted to our multi-party scenario, simultaneously correcting Bob 1, Bob 2, and Bob 3 keys. This step ensures that all parties share a common key, however it remains partly secret owing to information leaked during error correction, and any potential eavesdropping during the distribution step. In order to reduce the information held by any potential eavesdropper, we implement one round of privacy amplification on the entire raw key, reducing its final length. We use Toeplitz matrices for this purpose, a class of universal-2 hash functions [22] that can be implemented efficiently for our given key size.

We estimate the theoretical performance of our post-processing steps by evaluating the noise parameters $Q_X = 0.05$ and $\text{QBER} = 0.0159$, which we use to calculate the upper bound set by Eq. 5 in the Methods section and plotted in Fig 3(a) (dashed line). When performing the protocol in earnest with a finite data set to estimate these parameters, we replace the Shannon limit for the error correction term $h(\text{QBER}^m + 2\xi_z)$ in Eq. 5 with the fraction of parity bits disclosed by Alice.

Finally, we use the secret conference key to encrypt an image of a Cheshire cat that is shared between the parties in a brief conference call (Fig. 3b).

The security of our protocol is based on the proof in [8] and the assumptions therein. We note that Alice's measurement device is trusted whereas Bobs' measurement devices can be untrusted, as long as the detectors are memoryless. Adapting the quantum conference-key agreement protocol for full (measurement-)device-independence is a work in progress, see for example [23, 24].

Experimental 2QKD key rates are bounded by the the well-known repeaterless bound [25] established for point-to-point rates. We remark that this bound does not apply to our scenario, where four users are connected to a common server according to some network topology. New bounds were recently found if repeaters are introduced in a chain-like network [26] showing that higher key-rates can in principle be achieved. As our scenario omits repeaters these new bounds do not hold either, however we might expect similar improvements in the maximum key rates as opposed to standard end-to-end 2QKD protocols. An accurate model for fundamental bounds in a general network to apply to our scenario is still missing. We study this briefly in the SI, highlighting the non-trivial conference key rate dependence on asymmetric distribution of noise in the network.

Our post-processing, Fig. 3, is currently based on one-way LDPC error correction. The well-known two-way CASCADE protocol [27] outperforms the optimal LDPC approach in two-party QKD for small QBER [28], however, in the multi-user case this improvement will likely be offset by the additional iterations needed to correct uncorrelated errors in $(N-1)$ raw keys. In contrast, LDPC codes disclose a fixed amount of information that depends only on the largest QBER between Alice and any of the Bobs in the network. To the best of our knowledge, no proof exists for the optimal strategy to achieve the minimal bit disclosure rate when implementing error correction in the multi-user QKD scenario, and we leave this as an open question for future work.

Experimentally, future steps will be directed towards GHZ rate increases, the extension to more conference parties, and field tests in established fibre networks [29]. For direct GHZ-state transmission as demonstrated here, quantum CKA scales unfavourably with the number of users due to the exponential reduction in multi-photon detection considering unavoidable transmission losses. However, loss will not be a problem in fully-featured quantum networks where CKA will retain its significant (N-1) rate advantage.

METHODS

Entangled photon source

We produce photon-pairs using Type-II collinear spontaneous parametric down conversion (SPDC) implemented in a 22 mm long periodically-poled KTP (PPKTP) crystal. Both of our sources are optically pumped using a mode-locked laser operating with a nominal repetition rate of 80 MHz, 1.4 ps pulses and its central wavelength at 774.9 nm. A passive pulse interleaver is used to quadruple the 80 MHz pulse train to 320 MHz [30]. The PPKTP crystals are embedded within a polarisation-based Sagnac interferometer [19] and pumped bidirectionally, using a half-wave plate to set diagonally-polarised light, to create polarisation-entangled photons at 1549.8 nm in the approximate state:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|h\rangle|v\rangle - |v\rangle|h\rangle\right), \tag{2}$$

which we can map to any Bell state via local operation on one of the two photons.

With loose bandpass filters of 3 nm bandwidth, we measure an average source brightness of ∼ 4100 pairs/mW/s, with a symmetric heralding efficiency of ∼ 60% [31]. The average heralding efficiency reduces by ∼ 12% with a commensurate decrease of 45% in source brightness at the point of detection of the four users at zero distance. We characterise each photon pair source by performing quantum state tomography, reconstructing density matrices using maximum-likelihood estimation and Monte-Carlo simulations based on Poissonian count statistics to determine errors. For each source we obtain a typical two-photon Bell-state fidelity $F = 95.58 \pm 0.15\%$ and purity $P = 92.07 \pm 0.27\%$, while entanglement is measured by concurrence $\mathcal{C} = 92.38 \pm 0.21\%$.

The four-photon GHZ state is created by interfering one photon from each source on a polarising beamsplitter (PBS), which transmits horizontally and reflects vertically polarised photons. Post-selecting on the case where one photon is emitted in each output, which occurs with a probability of 1/2, we obtain the state

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|hhhh\rangle - |vvvv\rangle\right), \tag{3}$$

where $|h\rangle \equiv |0\rangle$ and $|v\rangle \equiv |1\rangle$ represent horizontal and vertical polarisations respectively. We measure independent two-photon interference visibility of $92.96 \pm 0.95\%$ using 100 mW pump power, and four-qubit state tomography returns a purity and fidelity of $P = 81.39 \pm 0.83\%$ and $F = 87.58 \pm 0.48\%$ respectively.

Active switching

Most QKD protocols require random switching of the measurement basis, either passively or actively, with each clock cycle. The same holds for the N-BB84 protocol, where users switch between the Z/X measurement bases according to a pre-agreed random sequence. Since all users implement the same measurement sequence, passive switching is not an option.

As noted, p is typically small hence switching between bases occurs relatively infrequently. In addition the multi-photon detection rates in our experiment are low, hence the standard method of polarisation switching with electro-optic modulators would be excessive. We therefore implemented active switching using motorised rotation stages with switching speeds on the order of seconds—marginally slower than our average required switching periods, which reduces the maximum possible raw generation rate g_R.

We evaluate the adjusted generation rate g'_R for the finite key scenario for the $\{5, 10, 20\}$ topology, by performing 1000 rounds of the protocol with active basis switching. We set $p = 0.02$, thus 20 type-2 rounds are randomly allocated in the measurement sequence. We measured the reduced key generation rate and found $g'_R/g_R = 0.91$.

This adjustment ratio is rate dependent. We find the lower bound on g'_R by assuming the type-2 rounds are never sequential hence each occurrence requires time to switch. This leads to the general expression,

$$g'_R \geq \frac{1}{\tau_s p + \frac{1-p}{g_R}}, \tag{4}$$

where τ_s is the switching speed. We use this equation to extrapolate the adjusted generation rates obtained in the asymptotic case as shown by orange dots in Fig. 2.

Active polarisation control

The optical fibre links in our experiment are realised by spools of bare SMF28 fibre. Thermal drifts in the laboratory introduces unwanted rotations in polarisation which, if uncorrected, leads to added noise in the protocol. These effects are typically negligible for short fibre lengths, e.g., in our testing we found the 5 km spool added no observable noise greater than with a 2 m fibre link, while the 10 km and 20 km spools showed significant added noise in $Q_{\mathrm{AB}i}$ measurements.

We implement active polarisation control to correct for these effects during key transmission to preserve low-noise operation throughout the protocol. The feedback control loop is implemented by performing single-qubit tomography in each fibre to characterise the unitary transformation on the polarisation qubits. We then use the polarisation optics in the measurement stages to undo the rotations on the qubits and perform measurements in the required basis. In our setup we carry out one-qubit tomography of all four fibre links simultaneously, including post-processing, to obtain an estimate of the unitary operation and implement the corrective action on the motorised waveplates. This takes less than 30 seconds and is performed once every ~ 20 minutes for an optimal tradeoff between maintaining a high duty-cycle while minimising bit error rates.

Error correction using LDPC codes

The use of LDPC codes allows one party to initialise the routine by encoding a block of k raw bits into a j-bit codeword using a $H_{(j-k)\times j}$ parity check matrix, where the ratio $r = k/j$ defines the code rate which in principle can be any number from 0 to 1. The DVB-S2 standard provides H matrices already computed for a set of different code rates specified for a codeword size of $j = 64'800$ bits. In our experiment, we set the code rate according to the estimated QBER using m samples with appropriate ξ_Z correction. From the provided set of code rates we used $1/2$, $1/3$ and $1/4$ for small, mid and large values of L as shown in Fig. 3(a). Alice uses the parity matrix to calculate the parity check bits, then sends to all parties the parity check bits and the H matrix through an authenticated classical channel. Each Bob implements a decoding algorithm consisting of simple addition, comparison and table look-up operations. The codes used here have been modified from MatLAB communication packages based on the DVB-S2 standards [21]. The number of parity bits communicated during EC is discarded to ensure security of the final conference key.

Finite-key conference rate

When using a finite number of rounds, the estimated parameters Q_X^m and QBER from the m type-2 and type-1 rounds, are affected by statistical error which must be taken into account in the final key rate. The fractional key rate is given by,

$$\begin{aligned}\frac{\ell}{L} = {} & \frac{n}{L}[1 - h(Q_X^m + 2\xi_X) \\ & - h(\mathrm{QBER}^m + 2\xi_Z)] - \log_2 \left[\frac{2(N-1)}{\epsilon_{EC}}\right]^{\frac{1}{L}} \\ & - 2\log_2 \left[\frac{1 - 2(N-1)\epsilon_{PE}}{2\epsilon_{PA}}\right]^{\frac{1}{L}} - h(p)\,,\end{aligned} \tag{5}$$

where N is number of users in the protocol, (ξ_X, ξ_Z) are finite-key correction terms and $(\epsilon_{EC}, \epsilon_{PE}, \epsilon_{PA})$ set the security parameters of our protocol, see SI for further details. The final term in Eq. 5 is the portion of the final key removed after PA, to account for the preshared key used in marking the type-2 rounds.

Author contributions

AF and MM conceived the project. MP, JH and PB performed the experiment and collected the data. JH and MP analysed the data. FG, MP and JH developed the theory results. All authors contributed to writing the manuscript.

Acknowledgements

This work was supported by the UK Engineering and Physical Sciences Research Council (grant number EP/N002962/1, EP/T001011/1). FG acknowledges financial support from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662. MM acknowledges funding from the QuantERA ERA-NET Cofund (FWF Project I3773-N36) and the UK EPSRC (EP/P024114/1).

SUPPLEMENTARY INFORMATION

Experimental Noise

As outlined in the main text, for the state employed in the protocol as in Eq. (3), we expect $Q_X = 0$ and QBER $= 0$. However, in the experimental implementation, the values observed are always non-zero. In our setup as in Fig. 1, the dominant sources of noise come from high-order generations in the PDC process and imperfect mode-matching at the PBS. A comprehensive model to account the effects of the noise on the expected value of Q_X and QBER, is non-trivial and goes beyond the scope of this work. However, we provide some qualitative remarks and suggestions for improvements.

Due to the probabilistic nature of the PDC process, there is always a non-zero probability that more than a single pair is generated within the crystal embedded in the Sagnac interferometer. This effect can be quantitatively accounted for by the so-called signal-to-noise ratio (SNR), defined as the ratio of single-pair events over the multiple-pair events. Note that increasing the pump power decreases the SNR. As shown in Fig. S1, both Q_X and QBER depend indeed from the pump power. The dependence is well fit by a linear trend, at least within the power range we considered. Note that for the data shown represents the setup initially, which was later optimised for our experiments hence the values shown here are slightly greater than those reported in the main text at 100 mW. Importantly, whereas the QBER tends to 0 in the limit of power → 0, the Q_X does not. Qualitatively, this can be understood from the fact that the QBER only depends on the polarisation of the photons in the state in Eq. (3), and not on their coherence. On the other hand, the value of Q_X is directly affected by the amount of coherence in the GHZ state considered for the protocol. In turn, the state's coherence is influenced by all the degrees of freedom, i.e.: polarisation, photon-number, time and spectrum. Decreasing the power – therefore increasing the SNR– only affects the purity in the photon-number degree of freedom but cannot affect the other degrees of freedom. In particular, although our photons are spectrally filtered at the source, they retain some spectral mixture intrinsic to the PDC process. This leads to non-ideal interference at the PBS, and therefore to a non-zero lower bound for the measurable Q_X. Such lower bound can be linked to the experimentally measured visibility as following. Assuming that the photons at the PBS successfully interfere with some probability t, we can write the state ρ_o after the interference as:

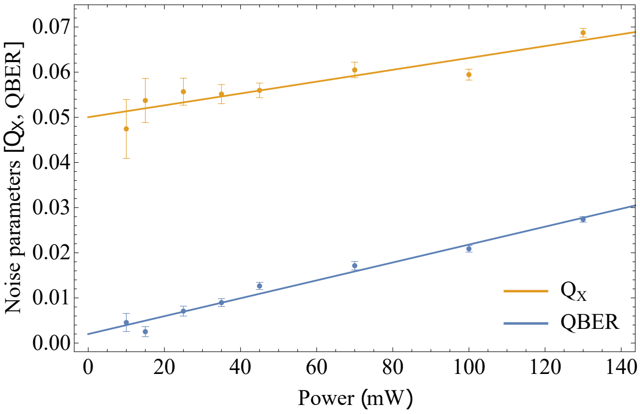

FIG. S1. Q_X and QBER as a function of power. Within the range of power considered, the trend is linear although the slope for the QBER is greater than the slope for Q_X. Moreover, Q_X is lower-bounded by the value of 0.05 at zero-power.

$$\rho_o = t\rho_s + (1-t)\rho_f. \tag{S1}$$

Where ρ_s is the density matrix of the state in case of success, given by $\rho_s = |GHZ\rangle\langle GHZ|$, and ρ_f is the density matrix in case of failure given by $(|hhhh\rangle\langle hhhh| + |vvvv\rangle\langle vvvv|)/2$. The expected Q_X for this state is

$$Q_X = \frac{1 - \mathrm{Tr}[\rho_o \otimes X^{\otimes 4}]}{2} = \frac{1-t}{2} \tag{S2}$$

Note that for $t = 1$, $Q_X = 0$, and for $t = 0$, $Q_X = 1/2$. Similarly, given the experimentally measured visibility V_{exp} we expect $Q_X = 0$ and $Q_X = 1/2$ for $V_{\mathrm{exp}} = 1$ and $V_{\mathrm{exp}} = 0$ respectively. We can thus, at least for these two extreme cases, interpret t as V_{exp}. Assuming that $t \approx V_{\mathrm{exp}}$ in general, we have that for $V_{\mathrm{exp}} = 0.9$, $Q_X = 0.05$ in accordance with our results (see main text). It should be noted however, that the interference at the PBS is a coherent process, which might not be fully characterised by the simple model just presented. Hence, in general, we can conclude that $Q_X \gtrsim (1 - V_{\mathrm{exp}})/2$.

Security parameters in NBB84

As stated in the main text, Eq. (5) represents the achievable secret key rate of the NBB84 protocol when the parties perform a finite number of rounds L. In other words, Alice needs to set the length of the PA output to Eq. (5) in order to ensure that the established key is secure with security parameter ϵ_{tot}. The security parameter ϵ_{tot} represents the maximal probability that a potential eavesdropper gains at least some information about the established key. It is related to the failure probabilities of the different stages of the protocol as follows: $\epsilon_{tot} = \epsilon_{EC} + \epsilon_{PA} + 2\epsilon_{PE}$, where ϵ_{EC} is the maximal failure probability of the EC procedure and ϵ_{PA} represents the same in the case of PA, while the last term is related to the failure probability of the PE step. In particular, the observed values $Q^m_{AB_i}$ and Q^m_X in the $2m$ rounds devoted to PE might differ from the correspondent values $Q^n_{AB_i}$ and Q^n_X characterizing the remaining $n = L - 2m$

rounds which are used to extract the secret key. The deviation of $Q^n_{AB_i}$ and Q^n_X is quantified by the theory of random sampling without replacement [32] and must be accounted for in the secret key rate Eq. (5), by taking the worst-case in order to preserve security. As shown in Ref. [8], the distance $|Q^n_{AB_i} - Q^m_{AB_i}|$ ($|Q^n_X - Q^m_X|$) between the pairwise bit discordance (the parameter Q^n_X) and its observed value is not larger than $2\xi_Z$ ($2\xi_X$) with probability at least $1-\epsilon_Z$ ($1-\epsilon_X$), where:

$$\xi_{Z,X} = \sqrt{\frac{(n+m)(m+1)}{8nm^2}\ln\left(\frac{1}{\epsilon_{Z,X}}\right)} \ . \tag{S3}$$

By combining the above statements one can deduce that:

$$\Pr\left[Q^n_X \leq Q^m_X + 2\xi_X \ \wedge \ Q^n_{AB_i} \leq Q^m_{AB_i} + 2\xi_Z \ \forall i\right] \geq 1 - \epsilon^2_{PE} \ , \tag{S4}$$

where we defined the total PE failure probability $\epsilon^2_{\rm PE}$ as follows:

$$\epsilon^2_{PE} \equiv (N-1)\epsilon_Z + \epsilon_X \ . \tag{S5}$$

Note that the probabilities ϵ_Z and ϵ_X, and hence ϵ^2_{PE}, can be chosen freely as to maximize the resulting secret key rate, with the only constraint that: $\epsilon_{PE} \leq \epsilon_{tot}$. Indeed, in our experiment we maximize the key rate in Eq. (5) over the failure probabilities $\epsilon_Z, \epsilon_X, \epsilon_{EC}$ and ϵ_{PA} and over the fraction of type-2 rounds p, having fixed the security parameter to $\epsilon_{tot} = 1.8 \times 10^{-8}$ and using preliminary estimations for QBER and Q_X. We obtain optimal values: $p = 0.012$, $\epsilon_{EC} \sim 10^{-13}$ and $\epsilon_{PA} \sim 10^{-10}$. The optimal value for p is then used to establish the fraction of type-2 measurements that need to be performed during data collection. We remark that since ϵ_{EC} and ϵ_{PA} possess an operational meaning as described above, one needs to verify that the actual procedures implemented for EC and PA fail at most with probabilities 10^{-13} and 10^{-10}, respectively. Due to the lack of a quantitative estimation of the failure probability characterizing the procedures adopted for EC and PA in our experiment, we could not verify that they are below the stated values. Nevertheless, we confirm that both procedures never failed in all the instances where they were used.

For further details, we refer the reader to Ref. [8].

Topology dependence in a conference key scenario

Conversely from the standard Alice-Bob scenario, conference key protocols are performed over a network where different users are connected according to some topology, and each link might be some noisy quantum channel. Therefore, in general, the conference key rates might depend on the noise distribution in the network opening a new problem absent in 2QKD.

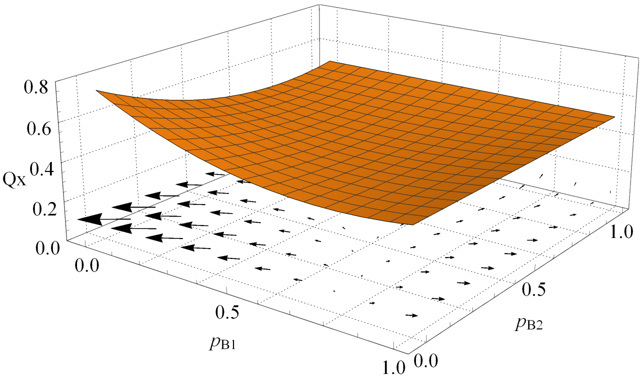

FIG. S2. Plot of Q_X as a function of the noise parameters p_{B1} and p_{B2} characterising the depolarising channels (Eq. S7) of Bob 1 and Bob 2, respectively. The noise parameter of Bob 3 is fixed to: $p_{B3} = 1.5 - p_{B1} - p_{B2}$. We also insert the vector field of the gradient of Q_X with respect to p_{B1} and p_{B2}.

Here, we study the 4-party network considered in the main text i.e. four users connected to one common server, with the noise affecting each link modeled as a depolarising channel

$$\mathcal{D}(\rho) = (1 - \frac{3p}{4})\mathcal{I} + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z) \tag{S6}$$

Therefore, in general we can assume the channels of Alice, Bob 1, Bob 2 and Bob 3 to have noise parameters $p_{\rm A}$, $p_{\rm B1}$, $p_{\rm B2}$, and $p_{\rm B3}$, respectively. For simplicity, we consider the case where Alice's channel is noiseless $p_{\rm A} = 0$ as the results are qualitatively the same. In this case, the expressions of Q_X and Q_{ABi}, for a depolarised 4-qubit GHZ state with noise parameters $p_{\rm B1}$, $p_{\rm B2}$ and $p_{\rm B3}$, are

$$Q_X(p_{\rm B1}, p_{\rm B2}, p_{\rm B3}) = \frac{[(p_{\rm B1}-1)(p_{\rm B2}-1)(p_{\rm B3}-1)+1]}{2}$$
$$Q_{ABi}(p_{\rm Bi}) = \frac{p_{\rm Bi}}{2} \tag{S7}$$

Q_X depends on the noise parameters of all the channels, whereas Q_{ABi} only depends locally on the noise parameter affecting the link connecting Alice and B_i. Of course, both functions have a global minimum in ($p_{\rm B1}$, $p_{\rm B2}$, $p_{\rm B3}$) $= (0,0,0)$, that is when all the channels are noiseless.

What is interesting to study is whether both the functions have a minimum with the constraint $p_{\rm B1} + p_{\rm B2} + p_{\rm B3} = c$ where c is a constant in the interval $c \in [0,3]$. In practice, this corresponds to fix some total amount of noise strength c on the network and finding which solution gives the highest key rate i.e. the lowest Q_X and Q_{ABi}. It is straightforward to see that the minimum of $\max_i Q_{ABi}$ is given by $p_{\rm B1} = p_{\rm B2} = p_{\rm B3} = c/3$. To find the minimum of Q_X, we compute the gradient of

$$f(p_{\rm B1},p_{\rm B2}) = Q_X(p_{\rm B1},p_{\rm B2},c-p_{\rm B1}-p_{\rm B2})$$

$$\frac{\partial f(p_{\rm B1},p_{\rm B2})}{\partial p_{\rm B1}} = \frac{1}{2}(p_{\rm B2}-1)(c-2p_{\rm B1}-p_{\rm B2})) \qquad \text{(S8)}$$

$$\frac{\partial f(p_{\rm B1},p_{\rm B2})}{\partial p_{\rm B2}} = \frac{1}{2}(p_{\rm B1}-1)(c-p_{\rm B1}-2p_{\rm B2})) \qquad \text{(S9)}$$

The plot in Fig. S2 shows the function $f(p_{\rm B1},p_{\rm B2})$ for $c = 1.5$ with at the bottom the vector field of the gradient as given by ∇f. One can verify that the minimum of the function is in $p_{\rm B1} = p_{\rm B2} = p_{\rm B3} = c/3$, therefore we conclude that the maximum conference key rate is achievable when the noise is symmetrically spread over the network. This result intuitively reflects the symmetry of the GHZ state, however in practice we can never assume the same amount of noise in all the channels. Nevertheless, it is important to note that the function is quite flat around the minimum. It follows that for small deviations from the symmetric configuration the effect on the key rate could be neglected. We leave open for investigation similar studies that account for different noise models.

[1] A. Pirker, J. Wallnöfer, and W. Dür, "Modular architectures for quantum networks," New Journal of Physics **20** (2018).

[2] F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation," npj Quantum Information **5**, 1–9 (2019).

[3] Michael Epping, Hermann Kampermann, and Dagmar Bruß, "Large-scale quantum networks based on graphs," New Journal of Physics **18** (2016).

[4] Michael Epping, Hermann Kampermann, and Dagmar Bruß, "Robust entanglement distribution via quantum network coding," New Journal of Physics **18** (2016).

[5] Kai Chen and Hoi-Kwong Lo, "Conference key agreement and quantum sharing of classical secrets with noisy ghz states," Proceedings of International Symposium on Information Theory , 1607–1611 (2005).

[6] Yao Fu, Hua-Lei Yin, Teng-Yun Chen, and Zeng-Bing Chen, "Long-distance measurement-device-independent multiparty quantum communication," Phys. Rev. Lett. **114**, 090501 (2015).

[7] Michael Epping, Hermann Kampermann, Dagmar Bruß, et al., "Multi-partite entanglement can speed up quantum key distribution in networks," New Journal of Physics **19**, 093012 (2017).

[8] Federico Grasselli, Hermann Kampermann, and Dagmar Bruß, "Finite-key effects in multipartite quantum key distribution protocols," New Journal of Physics **20**, 113014 (2018).

[9] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner, "Fully device-independent conference key agreement," Physical Review A **97**, 022307 (2018).

[10] Matej Pivoluska, Marcus Huber, and Mehul Malik, "Layered quantum key distribution," Phys. Rev. A **97**, 032312 (2018).

[11] Yonggi Jo and Wonmin Son, "Semi-device-independent multiparty quantum key distribution in the asymptotic limit," OSA Continuum **2**, 814–826 (2019).

[12] C Erven, E Meyer-Scott, K Fisher, J Lavoie, BL Higgins, Z Yan, CJ Pugh, J-P Bourgoin, R Prevedel, LK Shalm, et al., "Experimental three-photon quantum nonlocality under strict locality conditions," Nature photonics **8**, 292–296 (2014).

[13] Changliang Ren and Holger F. Hofmann, "Clock synchronization using maximal multipartite entanglement," Physical Review A **86**, 1–4 (2012).

[14] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," Nature Physics **10**, 582–587 (2014).

[15] Li Xiao, Gui Lu Long, Fu-Guo Deng, and Jian-Wei Pan, "Efficient multiparty quantum-secret-sharing schemes," Physical Review A **69**, 052307 (2004).

[16] VV Kuzmin, DV Vasilyev, N Sangouard, W Dür, and CA Muschik, "Scalable repeater architectures for multiparty states," npj Quantum Information **5**, 1–6 (2019).

[17] Momtchil Peev, Andreas Poppe, Oliver Maurhart, Thomas Lorünser, Thomas Länger, and Christoph Pacher, "The SECOQC quantum key distribution network in Vienna," European Conference on Optical Communication, ECOC (2009).

[18] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, and Rupert Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," Nature **564**, 225–228 (2018).

[19] Alessandro Fedrizzi, Thomas Herbst, Andreas Poppe, Thomas Jennewein, and Anton Zeilinger, "A wavelength-tunable fiber-coupled source of narrowband entangled photons," Opt. Express **15**, 15377–15386 (2007).

[20] Massimiliano Proietti, Martin Ringbauer, Francesco Graffitti, Peter Barrow, Alexander Pickston, Dmytro Kundys, Daniel Cavalcanti, Leandro Aolita, Rafael Chaves, and Alessandro Fedrizzi, "Enhanced multiqubit phase estimation in noisy environments by local encoding," Phys. Rev. Lett. **123**, 180503 (2019).

[21] Alberto Morello and Vittoria Mignone, "Dvb-s2: The second generation standard for satellite broad-band services," Proceedings of the IEEE **94**, 210–227 (2006).

[22] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," IEEE Transactions on Information Theory **57**, 3989–4001 (2011).

[23] Timo Holz, Daniel Miller, Hermann Kampermann, and Dagmar Bruß, "Comment on "fully device-independent conference key agreement"," Physical Review A **100**, 026301 (2019).

[24] Jérémy Ribeiro, Gláucia Murta, and Stephanie Wehner, "Reply to "comment on 'fully device-independent conference key agreement'"," Physical Review A **100**, 026302 (2019).

[25] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, "Fundamental limits of repeaterless quantum communications," Nature communications **8**, 15043 (2017).

[26] Stefano Pirandola, "End-to-end capacities of a quantum communication network," Commun. Phys **2**, 51 (2019).

[27] Gilles Brassard and Louis Salvail, "Secret-key reconciliation by public discussion," Workshop on the Theory and Application of of Cryptographic Techniques , 410–423 (1993).

[28] David Elkouss, Anthony Leverrier, Romain Alléaume, and Joseph J Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," 2009 IEEE International Symposium on Information Theory , 1879–1883 (2009).

[29] JF Dynes, Adrian Wonfor, WW-S Tam, AW Sharpe, R Takahashi, M Lucamarini, A Plews, ZL Yuan, AR Dixon, J Cho, et al., "Cambridge quantum network," npj Quantum Information **5**, 1–8 (2019).

[30] Matthew A Broome, Marcelo P Almeida, Alessandro Fedrizzi, and Andrew G White, "Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing," Optics express **19**, 22698–22708 (2011).

[31] Francesco Graffitti, Jérémy Kelly-Massicotte, Alessandro Fedrizzi, and Agata M Brańczyk, "Design considerations for high-purity heralded single-photon sources," Physical Review A **98**, 053811 (2018).

[32] Niek J Bouman and Serge Fehr, "Sampling in a quantum population, and applications," in Annual Cryptology Conference (Springer, 2010) pp. 724–741.

G

Quantum Conference Key Agreement: A Review

Title:	Quantum Conference Key Agreement: A Review
Authors:	Gláucia Murta, Federico Grasselli, Hermann Kampermann and Dagmar Bruß
Journal:	Advanced Quantum Technologies (QUTE)
Impact factor:	N/A
Date of submission:	20 February 2020
Publication status:	Under review
Contribution by FG:	Second author (input approx. 35%)

This publication corresponds to reference [Mur+20]. A summary of its content is presented in chapter 7.

The goal of the review and its general structure were jointly established by all authors at the beginning of the project. I personally wrote section III.B, section IV, part of section VII and all the figure captions in the manuscript. I also produced all the plots by using custom code written by me. I regularly discussed the contents of the paper with GM and provided further help on other parts of the paper. Finally, I contributed to proofreading the whole manuscript together with my co-authors.

arXiv:2003.10186v1 [quant-ph] 23 Mar 2020

Quantum Conference Key Agreement: A Review

Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf,
Universitätsstraße 1, D-40225 Düsseldorf, Germany

Conference key agreement (CKA), or multipartite key distribution, is a cryptographic task where more than two parties wish to establish a common secret key. A composition of bipartite quantum key distribution protocols can accomplish this task. However, the existence of multipartite quantum correlations allows for new and potentially more efficient protocols, to be applied in future quantum networks. Here, we review the existing quantum CKA protocols based on multipartite entanglement, both in the device-dependent and the device-independent scenario.

I. INTRODUCTION

Quantum mechanics can bring unprecedented advantages to the realization of information processing tasks. A remarkable example is quantum key distribution (QKD)[1, 2], arguably the most mature quantum technology. QKD allows two parties, Alice and Bob, to securely communicate by establishing a secret key that is information theoretically secure. Security proofs are given for different levels of assumptions. In the scenario where the devices and/or quantum states are characterized, robust security is proven for realistic parameters [3, 4] (see also [5]) with implementations achieving long distances [6, 7]. Also for the device-independent scenario, i.e. no assumptions on the quantum states and on the working behavior of the devices, a security proof in the fully adversarial scenario is well established [8]. The required experimental parameters are characterized [9] for protocols based on the simplest Bell inequality [10].

The extensive development of quantum technological applications allow near future applications which are based on genuine multipartite quantum protocols using shared multipartite entangled states in network structures [11–17]. Applications range from distributed quantum computing to genuine multipartite quantum communication protocols which may lead to the quantum internet [18, 19].

Here we focus on conference key agreement (CKA), or multiparty key distribution, which is a generalization of the task of key distribution to the scenario in which N users wish to establish a common secret key. This allows the users to broadcast secure messages in a network. CKA can e.g. be achieved by, first establishing bipartite keys between the users, followed by securely distributing a common key to all other users via the bipartite keys. This solution has been discussed to be inefficient in the classical scenario, and several classical protocols allowing the parties to establish a common key were proposed (see e.g. [20, 21] and [22, 23]). In the quantum scenario, that is, when the parties can use quantum resources, a secure conference key can also be established by using several bipartite QKD links. Bipartite quantum links are already being implemented in small quantum networks over metropolitan distances [24–29] and in larger networks spanning entire countries [30–32]. The long-term vision of a general quantum network, however, goes beyond mere bipartite links and includes network nodes that process quantum information, thus enabling the distribution of multipartite entangled states across the network [33]. In a quantum network, quantum communication with genuine multipartite entangled states may offer advantages over the bipartite case [34], and allow secure interactions between an arbitrary subset of the participating partners.

The rich structure of multipartite entangled quantum states opens the possibility for a wide variety of new key distribution protocols. While protocols for CKA based merely on bipartite QKD do not bring much novelty in terms of the necessary quantum technologies or the theoretical tools required for the security analysis, this changes when protocols explore multipartite entanglement. Here, quantum correlations can be exploited to devise truly multipartite schemes. This is the focus of this paper, namely we will review the proposals and developments regarding the use of multipartite quantum entanglement for the establishment of a conference key.

II. PRELIMINARIES

A. Multipartite entangled resources

Multipartite quantum states have a more convoluted structure than the bipartite ones [35–38]. Different classes of states can be defined according to their entanglement properties, and concepts such as k-separability and genuine multipartite entanglement arise (for a precise definition of these concepts, see [35, 36, 38]). For multipartite systems, there exist different entanglement classes that are not equivalent under stochastic local operations and classical communication (SLOCC) [38–40]. In particular, in the tripartite case [39], two nonequivalent classes of genuinely multipartite entangled states can be defined: the GHZ-class represented by the Greenberger–Horne–Zeilinger (GHZ) state [41]

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right), \tag{1}$$

and the W-class represented by the W state [39]

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}\left(|001\rangle + |010\rangle + |100\rangle\right). \tag{2}$$

These classes of states also exhibit different physical properties. The GHZ-state is a direct generalization of Bell states to the multipartite case and maximally violates the well-studied family of N-party Bell inequalities called MABK [42–44]. However, the entanglement present in the GHZ-state is not robust to particle losses, while the W-state still exhibits bipartite entanglement when one particle is lost.

The 3-party GHZ and W states in Eqs. (1) and (2) can be generalized in a straightforward way to N parties. They constitute the resources for quantum CKA protocols discussed in the following sections.

B. Security

1. Security definition

We consider N users, Alice, Bob_1, Bob_2, $\ldots$, Bob_{N-1}. The users wish to establish a common string of bits that is unknown to any other party, in particular to any potential eavesdropper.

The security of a quantum conference key agreement protocol is based on two conditions: correctness and secrecy.

Definition 1 (Correctness)**.** *A CKA protocol is ϵ_{corr}-correct if*

$$p(K_A = K_{B_1} = \ldots = K_{B_{N-1}}) \geq 1 - \epsilon_{corr}, \tag{3}$$

where K_A, K_{B_i} are the final keys held by Alice and Bob_i and $p(K_A = K_{B_1} = \ldots = K_{B_{N-1}})$ is the probability that all final keys are identical.

Definition 2 (Secrecy)**.** *A CKA protocol is ϵ_{sec}-secret if, for Ω being the event that the protocol does not abort,*

$$p(\Omega)\frac{1}{2}\|\rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_E\| \leq \epsilon_{sec}, \tag{4}$$

where $p(\Omega)$ is the probability of the event Ω, $\tau_{K_A} = \frac{1}{|S|}\sum_{s_i \in S} |s_i\rangle\langle s_i|$ is the maximally mixed state over all possible values that the key K_A can assume, and $S = \{0,1\}^{\times \ell}$, where ℓ is the length of the key K_A.

Correctness implies that, at the end of the protocol, Alice and the Bobs share the same string of bits except for probability at most ϵ_{corr}. The secrecy requirement states that Alice's key is randomly chosen among the set of possible strings and the eavesdropper has no information about the key, except for probability at most ϵ_{sec}. If a CKA protocol is ϵ_{corr}-correct and ϵ_{sec}-secret, then it is said to be ϵ_s-correct-and-secret for all $\epsilon_s \geq \epsilon_{corr} + \epsilon_{sec}$.

Additionally, a useful CKA protocol should have a robust honest implementation. This is captured by the concept of completeness.

Definition 3 (Completeness)**.** *A quantum CKA protocol is ϵ_c-complete if there exists an honest implementation of the protocol, such that the probability of not aborting is greater than $1 - \epsilon_c$.*

Finally, the security of a quantum CKA protocol can be summarized as [45]:

Definition 4 (Security of a quantum CKA protocol)**.** *A quantum CKA protocol is (ϵ_s, ϵ_c)-secure if*

(I) (Soundness) For any implementation of the protocol, it is ϵ_s-correct-and-secret.

(II) (Completeness) There exists an honest implementation of the protocol, such that the probability of not aborting is greater than $1 - \epsilon_c$.

Definition 4 implies composable security [45–47]. This means that the conference key generated by a protocol satisfying the conditions stated in Definition 4 is composable secure and therefore can be used as a building block for further protocols (this, however, cannot always be inferred in the device-independent scenario, see Remark 1 in Section V).

The quantum left-over hashing lemma [48, 49] establishes that a secret conference key can be obtained if the key length ℓ is slightly shorter than

$$\ell \lesssim H^{\epsilon}_{\min}(A_1^n|E) \tag{5}$$

where $H^{\epsilon}_{\min}(A_1^n|E)$ is the conditional smooth min-entropy [50] evaluated for the classical-quantum (cq) state $\rho_{A_1^n E}$ composed of Alice's raw key of size n and the quantum side information of a potential eavesdropper.

The conditional smooth min-entropy of a cq-state ρ_{AE} is defined as

$$H^{\epsilon}_{\min}(A|E) = \sup_{\tilde{\rho}_{AE} \in \mathcal{B}^{\epsilon}(\rho_{AE})} H_{\min}(A|E), \tag{6}$$

where $\epsilon \in [0,1)$, and the supremum is taken over positive sub-normalized operators that are ϵ-close to ρ_{AE} in the purifying distance [50]. And the conditional min-entropy, $H_{\min}(A|E)$, of a classical variable A conditioned on the quantum side information E is closely related to the optimal probability of the eavesdropper guessing the value of A, $p_{guess}(A|E)$, [51]

$$H_{\min}(A|E) = -\log p_{guess}(A|E). \tag{7}$$

For a precise definition and properties of entropic quantities we refer the reader to [50].

The main task in the security proof of a conference key agreement protocol is to estimate $H^{\epsilon}_{\min}(A_1^n|E)$. Note that this is very similar to the bipartite case of quantum key distribution. In fact, the secrecy condition only depends on the correlations between the eavesdropper and Alice's string. However, in the multipartite scenario the parties need to ensure that all of the Bobs correct their raw key so that the correctness requirement is satisfied.

2. Security model

In the scenario where N parties wish to securely communicate, the adversary is an external party, Eve, who can eavesdrop on all the exchanged public communication. Moreover, Eve might try to tamper with the quantum channels and explore correlations with the generated conference key.

Similar to the bipartite case, we can also classify the attacks performed by the eavesdropper into three categories:

1. Individual attacks: the eavesdropper can only attack individually each round of the protocol. In this case she is assumed to have no quantum memory, and therefore her best strategy is to perform a measurement on her quantum side information at each round.

2. Collective attacks: Eve is assumed to perform the same attack for each round of the protocol, that is, her quantum side information is identically and independently distributed (IID) with respect to different rounds. Differently from individual attacks, Eve is now assumed to have a quantum memory. Therefore, she can store her quantum side information at each round and perform a global operation on it at the end of the execution of the protocol.

3. Coherent attacks: This is the most general type of attack where there are no assumptions on the capabilities of the eavesdropper, except that she is bounded by the laws of quantum mechanics. In this case the states shared by the parties at each round may have arbitrary correlations with previous and future rounds.

C. Generic Protocols

The goal of quantum conference key agreement is that the N users make use of their shared quantum resources together with local operations and public communication in order to establish a secure conference key.

In the following section we will present the proposed quantum protocols that perform the task of CKA, making use of multipartite entanglement. The protocols we will discuss consist of the following main steps:

1. **Preparation and distribution:** A source distributes a multipartite entangled state to the N parties. This step is repeated n times.

2. **Measurements:** Upon receiving the systems, the parties perform local measurements and record the classical outcome. The measurements are randomly chosen according to the specifications of the protocol. One of the possible measurement settings is used with higher probability and is called the key generation measurement. The other measurements are used for test rounds, which only occasionally occur.

3. **Parameter estimation:** The parties announce the inputs and outputs of their test rounds and of some randomly chosen key generation rounds which are used to estimate their correlation and the potential influence of an eavesdropper. At the end of this step each party is left with a string of $n_{raw} < n$ bits, which constitute their raw key.

4. **Information reconciliation (error correction):** The parties publicly exchange classical information in order for the Bobs to correct their string of bits to match Alice's string. In the multipartite case, the information reconciliation protocol needs to account for the correction of the strings of all the Bobs.

5. **Privacy amplification:** Alice randomly picks a hash function, chosen among a two-universal family of hash functions (see [48]), and communicates it to the Bobs. Every party applies the hash function to turn her/his partially secure string of n_{raw} bits into a secure key of $\ell < n_{raw}$ bits.

The key rate of a protocol is given by

$$r = \tau \frac{\ell}{n} \tag{8}$$

where τ is the repetition rate of the setup, i.e. the inverse of the time it takes to implement one round of preparation and measurement of the quantum systems. In the following sections we will typically take $\tau = 1$ as we will not be focused on any specific experimental implementation. The key rate in the limit of infinitely many rounds, $n \to \infty$, is called the asymptotic key rate and denoted r_∞.

III. PROTOCOLS FOR MULTY-QUBIT STATES

A. GHZ state protocols

The first proposals of quantum conference key agreement protocols explore the multipartite correlations exhibited by the N-party GHZ state:

$$|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}} \left(|00\ldots0\rangle + |11\ldots1\rangle \right), \tag{9}$$

where $\{|0\rangle, |1\rangle\}$ is the Z-basis, composed by the eigenstates of the Pauli operator σ_z. The GHZ state satisfies all the desired conditions for a conference key agreement protocol: the outcomes of measurements in the Z-basis are perfectly correlated, random and uniformly distributed. Interestingly, for $N \geq 3$ this perfect correlation can only be achieved if all the parties measure in the Z-basis. As shown in [34], even bipartite perfect correlation cannot be obtained if the parties choose a different basis. This represents a drastic difference from the bipartite case ($N = 2$). Indeed, if Alice and Bob share the maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, for each choice of local basis for Alice, there exists a local basis for Bob such that their outcomes exhibit perfect correlation. This property is exploited in the bipartite six-state [52] and BB84 [1] protocols for QKD.

Early proposals of protocols that employ the GHZ state to establish a conference key between three parties were presented in [53]. Security is proved, against individual attacks, for the ideal case where Alice can prepare and distribute perfect GHZ states. Robustness to noise is not considered. In Ref. [54], Chen and Lo proved the security of quantum conference key agreement based on the distillation of GHZ states [55, 56]. They derive distillation rates for a protocol based on a improved version of the multi-party hashing method [55]. These rates correspond to conference key rates, due to the fact that the multi-party hashing distillation protocol [55] can be implemented by classical post-processing of the raw key. Ref. [54] also considers distillation rates when recurrence protocols are applied before the multi-party hashing. Recurrence protocols are based on CSS codes [57, 58] and, if certain conditions are met, they can also be translated to a classical post-processing of the generated raw keys, in a similar fashion to the bipartite case [59]. Ref. [54] modifies the recurrence protocol introduced in [56], using ideas of [59], to design a protocol that can be converted to classical post-processing of the raw key. This type of classical post-processing of the raw key requires two-way communication and was denoted advantage distillation [60–62].

In the following subsections, we present specific protocols with GHZ states that can be regarded as the generalization of the six-state and the BB84 protocols to the multipartite case.

1. *Multiparty six-state protocol*

The quantum conference key agreement protocol introduced in [34] can be seen as a generalization of the six-state QKD protocol [52] to the multipartite case. Indeed, in Ref. [34] the parties perform measurements in the three bases $\{X, Y, Z\}$. Measurements in the Z-basis are used with higher frequency, and they constitute the key generation rounds. The X-basis and Y-basis are instead used in fewer rounds, specifically in the test rounds, in order to estimate the information available to a potential eavesdropper.

From the parameter estimation rounds, the statistics of the Z-measurements is used to estimate the qubit error rates (QBERs) and thus to determine the information that needs to be communicated by Alice for information reconciliation. The bipartite QBERs, Q_{AB_i}, for $1 \leq i \leq N-1$, are the probabilities that the outcome of a Z-measurement by Bob$_i$ disagrees with Alice's Z-measurement outcome. In the multipartite scenario we can also define the total QBER Q_Z as the probability that at least one Bob obtains an outcome different than Alice. If the N parties share a state ρ, the QBER Q_Z is given by

$$Q_Z = 1 - \mathrm{tr}\left(\rho\left(|0\rangle\langle 0|^{\otimes N} + |1\rangle\langle 1|^{\otimes N}\right)\right). \qquad (10)$$

With the statistics of the test rounds, the parties want to estimate the expected value of the operator $X^{\otimes N}$. Since the multipartite GHZ state does not exhibit perfect correlation in more than one basis [34], the QBER Q_X is defined as the probability that the $X^{\otimes N}$-measurement gives a result that differs from the ideal case:

$$Q_X = \frac{1 - \langle X^{\otimes N}\rangle}{2}. \qquad (11)$$

Note that if the parties share the GHZ state (9), then the corresponding Q_X is zero.

A crucial step in the security analysis of the protocol presented in Ref. [34] is a reduction to depolarized states. An N-qubit depolarized state is a state of the form:

$$\begin{aligned}\rho_{\mathrm{dep}} = \lambda_{0,\vec{0}}|\Psi_{0,\vec{0}}\rangle\langle\Psi_{0,\vec{0}}| + \lambda_{1,\vec{0}}|\Psi_{1,\vec{0}}\rangle\langle\Psi_{1,\vec{0}}| \\ + \sum_{\sigma,\vec{u}\neq\vec{0}} \lambda_{\vec{u}}|\Psi_{\sigma,\vec{u}}\rangle\langle\Psi_{\sigma,\vec{u}}|,\end{aligned} \qquad (12)$$

where

$$|\psi_{\sigma,\vec{u}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|\vec{u}\rangle + (-1)^{\sigma}|1\rangle|\bar{\vec{u}}\rangle\right) \qquad (13)$$

for $\vec{u} \in \{0,1\}^{\times(N-1)}$, $\bar{\vec{u}} = \vec{u} \oplus \vec{1}$, and $\sigma \in \{0,1\}$. The states $\{|\psi_{\sigma,\vec{u}}\rangle\}_{\sigma,\vec{u}}$ form a basis, denoted as the GHZ basis. The depolarized GHZ state is then diagonal in the GHZ basis and such that $\lambda_{0,\vec{u}} = \lambda_{1,\vec{u}} \equiv \lambda_{\vec{u}}$ for $\vec{u} \neq \vec{0}$.

For a state of the form (12), one finds that

$$Q_Z(\rho_{\mathrm{dep}}) = 1 - (\lambda_{0,\vec{0}} + \lambda_{1,\vec{0}}), \qquad (14)$$

and

$$Q_X(\rho_{\mathrm{dep}}) = \frac{1 - (\lambda_{0,\vec{0}} - \lambda_{1,\vec{0}})}{2}. \qquad (15)$$

Finally, the asymptotic key rate for the depolarized state (12) is given as a function of Q_X, Q_Z and the bipartite QBERs Q_{AB_i} [34]:

$$\begin{aligned} r_\infty =& (1 - Q_Z)\left(1 - \log(1 - Q_Z)\right) \\ &+ \left(1 - \frac{Q_Z}{2} - Q_X\right)\log\left(1 - \frac{Q_Z}{2} - Q_X\right) \\ &+ \left(Q_X - \frac{Q_Z}{2}\right)\log\left(Q_X - \frac{Q_Z}{2}\right) \\ &- \max_{1\leq i\leq N-1} h\left(Q_{AB_i}\right)\end{aligned}. \qquad (16)$$

For the generality of the security analysis of [34], it remains to argue that the reduction to depolarized states, (12), is not restrictive. Any N-qubit state can be brought to the form (12) by successive application of the following set of local operations [63, 64]

$$\begin{aligned}\mathcal{D} = \left\{X^{\otimes N}\right\} \cup \left\{Z_{AB_j} | 1 \leq j \leq N-1\right\} \\ \cup \left\{R_k | 1 \leq k \leq N-1\right\}\end{aligned}, \tag{17}$$

where the operations Z_{AB_j} and R_k are defined as

$$Z_{AB_j} = Z_A \otimes Z_{B_j} \otimes I_{B_{[N-1]\setminus j}} \tag{18}$$

and

$$R_k = \mathrm{diag}(1, i)_A \otimes \mathrm{diag}(1, -i)_{B_k} \otimes I_{B_{[N-1]\setminus k}}. \tag{19}$$

Indeed, the application of the map

$$\rho \mapsto \tilde{\rho} = \circ_{i=1}^{2N-1} \mathcal{D}_i[\rho] \tag{20}$$

where

$$\mathcal{D}_i[\rho] = \frac{1}{2}\rho + \frac{1}{2} D_i \rho D_i^\dagger \; ; \; D_i \in \mathcal{D}, \tag{21}$$

brings any N-qubit state to the form (12).

A crucial observation is that the map (20) can be implemented in the protocol by flipping the outcomes of some of the measurements and adding additional measurements in the Y-basis [34].

Consider first the set of operations $\left\{X^{\otimes N}\right\} \cup \left\{Z_{AB_j} | 1 \leq j \leq N-1\right\}$. Successive application of these operations brings any N-qubit state to the GHZ-diagonal form

$$\tilde{\rho} = \sum_{\sigma, \vec{u}} \lambda_{\sigma, \vec{u}} |\psi_{\sigma, \vec{u}}\rangle\langle\psi_{\sigma, \vec{u}}|. \tag{22}$$

For the key generation rounds, in which Alice and the Bobs measure in the Z-basis, the application of Z_{AB_j} does not have any effect on the final outcomes and the operation $X^{\otimes N}$ can be equivalently applied by Alice and the Bobs by flipping their Z-measurement outcomes. For the estimation of $X^{\otimes N}$ in the test rounds, the operations $\left\{X^{\otimes N}\right\} \cup \left\{Z_{AB_j} | 1 \leq j \leq N-1\right\}$ have no effect, as can be seen by the fact that they commute with $X^{\otimes N}$.

The application of the operations $\{R_k\}$ is what finally brings the state to the depolarized form (12). They have no effect on the key generation rounds as they do not change the outcome of the Z-measurements. For the test rounds, the action of R_k is more subtle. As shown in [34], the action of R_k followed by a measurement in the X-basis is equivalently implemented by Bob$_k$ performing a Y-basis measurement. Therefore the action of the operators $\{R_k\}$, which are essential to simplify the security analysis of the protocol introduced [34], can be implemented in the protocol by adding Y-basis measurements to the test rounds.

In Ref. [34] the authors show that in a quantum network with quantum routers, for a bottleneck configuration with constrained channel capacity, the multipartite six-state protocol based on the GHZ state leads to higher rates as compared to several implementations of bipartite QKD, when the gate quality is above certain threshold value.

A security analysis of the multiparty six-state protocol against coherent attacks taking into account finite size effects was presented in [65].

2. Multiparty BB84 protocol

In Ref. [65], also a multipartite version of the BB84 protocol was introduced: here, the parties only need to perform measurements in two bases, the Z-basis and the X-basis. The security analysis is based on the uncertainty relation for smooth entropies [66]. This technique has previously been used in the bipartite case [3, 5] for the security proof of the BB84 protocol in the finite regime for parameters that are compatible with current technology. The uncertainty relation establishes that for a pure state $|\psi_{A\vec{B}E}\rangle$, if Alice can perform measurements in two bases, say the X-basis and the Z-basis, then the following relation is satisfied:

$$H_{\min}^{\epsilon}(Z_1^m|E) \leq q - H_{\max}^{\epsilon}(X_1^m|B_1 \dots B_{N-1}) \tag{23}$$

where the conditional smooth min-entropy on the l.h.s. is evaluated for the cq-state shared by Alice and Eve when Alice measures her systems in the Z-basis, and the conditional smooth max-entropy on the r.h.s. is evaluated for the cq-state shared by Alice and the Bobs when Alice measures her systems in the X-basis. For a precise definition of $H_{\max}^{\epsilon}$ we refer the reader to [50]. The term q quantifies the incompatibility of the two measurements used by Alice, and for the case where Alice can measure X or Z the quality factor q for the m rounds will be equal to m.

The quantity $H_{\max}^{\epsilon}(X_1^m|B_1 \dots B_{N-1})$ can be estimated by using the X-measurements performed by the Bobs (11). Indeed, the data processing inequality guarantees that

$$H_{\max}^{\epsilon}(X_1^m|B_1 \dots B_{N-1}) \leq H_{\max}^{\epsilon}(X_1^m|\vec{X}_1^n), \tag{24}$$

where $\vec{X}_1^m$ contains the X-outcomes of every Bob, had the Bobs measured in the X-basis in the m rounds. Clearly the entropy on the r.h.s. of Eq. (24), that is the entropy of Alice's X-outcome string given the X-outcome strings of the Bobs, can be estimated via the X-basis error defined in Eq. (11).

Finally Ref. [65] establishes the asymptotic secret key rate of the multiparty BB84 protocol

$$r_\infty = 1 - h(Q_X) - \max_{1 \leq i \leq N-1} h(Q_{AB_i}). \tag{25}$$

3. Comparison of multiparty six-state and BB84 protocols

For any specific implementation, the asymptotic key rates obtained by the multiparty six-state protocol [34]

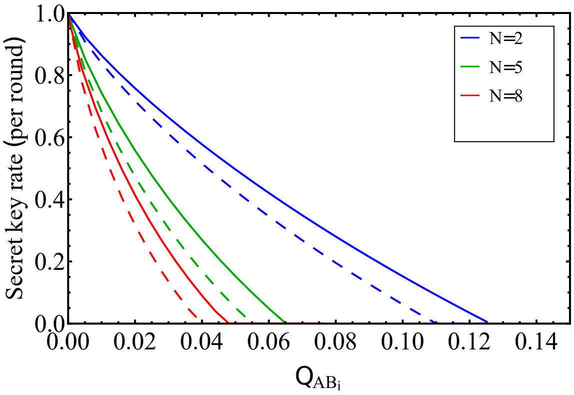

Figure 1. Asymptotic secret key rates of the multipartite six-state (solid) [34] and BB84 (dashed) [65] protocols as a function of the bipartite QBER between Alice and any Bob, for a local depolarizing noise model. The rates are plotted for different numbers of parties ($N = 2, 5, 8$, right to left). The plot shows that the multipartite six-state protocol asymptotically outperforms the multipartite BB84 protocol.

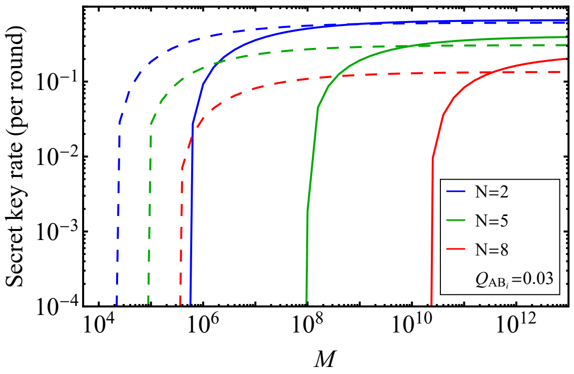

Figure 2. Secret key rates of the multipartite six-state (solid) [34] and BB84 (dashed) [65] protocols as a function of the total number of rounds M, for different number of parties ($N = 2, 5$ and 8, left to right) and fixed bipartite QBER ($Q_{AB_i} = 0.03$). The noise model employed is the local depolarizing channel given in Eqs.(26) and (27). A non-null conference key can be obtained for fewer rounds with the multipartite BB84 protocol, compared to the multipartite six-state protocol, and the advantage of the former protocol increases with the number of parties.

are higher than those obtained by the multiparty BB84 [65]. This is because more structure can be ensured about the underlying state in the protocol presented in [34]. For instance, consider the implementation where Alice prepares a GHZ state and distributes it to each of the Bobs using a qubit depolarizing channel. The state shared by the parties is thus

$$\rho_{A\vec{B}} = \mathcal{D}_2^{\otimes(N-1)}|\mathrm{GHZ}_N\rangle\langle\mathrm{GHZ}_N|, \tag{26}$$

where

$$\mathcal{D}_2(\rho) = (1-\nu)\rho + \nu\frac{\mathbb{1}}{2}. \tag{27}$$

Fig. 1 shows the comparison of the asymptotic key rates achieved by the two multiparty protocols ($N = 2, 5, 8$) in the specific implementation given by the noise model in Eq. (26). The key rates are plotted as a function of the bipartite QBER between Alice and any Bob, which turns out to be a simple function of the noise parameter characterizing the depolarizing channel: $Q_{AB_i} = \nu/2$. The figure confirms that, asymptotically, the multipartite six-state protocol [34] overcomes the multipartite BB84 [65] in terms of performance.

Ref. [65] also performs a complete security analysis in the finite-key regime for the multiparty six-state and multiparty BB84 protocol. Regarding the rates in the finite-key regime, it was shown that, even though the six-state protocol can tolerate higher noise, for the low-noise regime a non-zero conference key rate can be proven for the multiparty BB84 protocol using a significantly smaller number of rounds. This is confirmed by Fig. 2, where the secret key rates of both protocols are plotted as a function of the total number of protocol rounds, having fixed the bipartite QBER. The noise model employed is the same used for Fig. 1, i.e. the local depolarizing channel given in Eq. (27). It is important to remark that the lower threshold on the minimum number of signals for a non-zero key by the multiparty BB84 protocol, may be simply due to the techniques used to compute the key rates. The finite-key rates of the multipartite six-state are derived using the post-selection technique [67] in combination with the finite version of the asymptotic equipartition property [68] (see also [48]). These techniques might lead to higher overhead terms in the finite-key regime and therefore to a less tight estimate than what can be obtained using the uncertainty relation for smooth entropies [66]. However, due to the fact that in the multiparty six-state protocol the parties are required to perform three distinct measurements, the uncertainty relation is not applicable.

4. Prepare-and-measure implementation

Even though entanglement plays an essential role for the security of bipartite QKD, it is known that some QKD protocols have a corresponding prepare-and-measure implementation that does not require any entanglement. The BB84 protocol, for example, can be implemented with Alice transmitting single qubit states to Bob.

Similarly, in the multipartite case we can also talk about a corresponding prepare-and-measure implementation. However, now this reduction will require the preparation of some $(N-1)$-entangled states [34].

Indeed for the key generation rounds, in which the parties are performing measurements in the Z-basis, Alice could instead randomly choose her bit and prepare

$(N-1)$ copies of the corresponding single qubit state to send to the Bobs, $|0\rangle^{\otimes(N-1)}$ or $|1\rangle^{\otimes(N-1)}$. Although entanglement is not required to reproduce the statistics of the key generation rounds, the corresponding state shared by the Bobs when Alice performs a measurement in the X-basis or Y-basis is entangled. Therefore, for the test rounds, Alice is required to prepare an $(N-1)$-entangled state.

For example, when Alice performs an X-measurement, given that she obtains the outcome a, the corresponding state that she has to distribute to the Bobs is the $(N-1)$-entangled state:

$$|\psi_a\rangle_{B_1\ldots B_{N-1}} = \frac{1}{\sqrt{2}}\left(|00\ldots0\rangle + (-1)^a|11\ldots1\rangle\right). \quad (28)$$

The prepare-and-measure equivalence significantly reduces the resources required for the implementation of the protocols [34, 65], as Alice needs to control $(N-1)$-partite entanglement instead of N-partite entanglement. This can have significant practical implications especially in the noisy intermediate scale (NISQ) era [69]. Moreover, it is important to remark that, for most of the rounds, the key generation rounds, Alice can in fact prepare product states, and entanglement is only required in a small fraction of the rounds for the purpose of parameter estimation.

A prepare-and-measure protocol in which Alice only needs to send separable states was proved secure for the case $N = 3$ in [70]. However, when extending the protocol to an arbitrary number of parties N the states distributed by Alice would become increasingly distinguishable as N increases, which would allow an eavesdropper to retrieve more information about the key, while causing less disturbance. Thus, the secret key rate would decrease with increasing N, even for a perfect implementation.

B. W state protocol

Quantum conference key agreement does not necessarily need to rely on the correlations provided by multipartite GHZ states. Indeed, the protocol devised in [71] exploits the multipartite entanglement of a W-class state in order to establish a conference key. The W state of N parties is defined as

$$|\mathrm{W}_N\rangle = \frac{1}{\sqrt{N}}\left(|0\ldots01\rangle + |0\ldots10\rangle + \ldots + |1\ldots00\rangle\right), \quad (29)$$

whereas a W-class state has a similar form to (29) but presents arbitrary phases on each term.

In the conference key agreement protocol of Ref. [71], the state is post-selected thanks to single-photon interference occurring in a central untrusted node, extending the founding idea of twin-field QKD [72, 73] to the multipartite scenario.

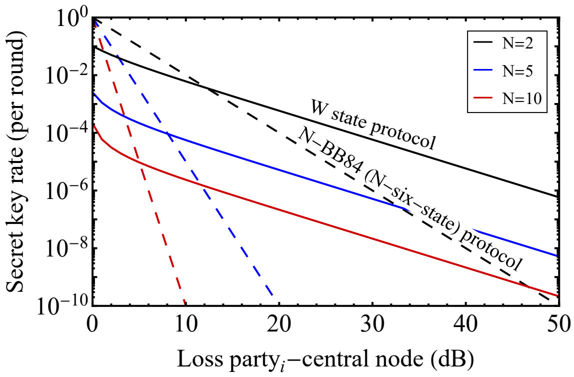

Figure 3. Comparison of the asymptotic conference key rate achieved by the W state protocol [71] (solid) and by the N-BB84 protocol [65] (dashed, the N-six-state protocol rate is identical in this ideal scenario) as a function of the loss in the channel linking each party to the central entanglement distributor, for different number of parties ($N = 2, 5$ and 10). We assume ideal implementations where the only source of error is photon loss and where the GHZ state of the N-BB84 (N-six-state) protocol is encoded in orthogonal polarizations of a photon.

In particular, each round of the protocol starts with party$_i$ ($i = 1, 2, \ldots, N$) preparing the following entangled state between an optical pulse a_i and a qubit A_i:

$$|\phi\rangle_{A_i a_i} = \sqrt{q}|0\rangle_{A_i}|0\rangle_{a_i} + \sqrt{1-q}|1\rangle_{A_i}|1\rangle_{a_i}, \quad (30)$$

where $|0\rangle_{a_i}$ is the vacuum state, $|1\rangle_{a_i}$ is the single-photon state, and $\{|0\rangle_{A_i}, |1\rangle_{A_i}\}$ is the computational basis of the qubit. The state is strongly unbalanced towards the vacuum: $q \approx 1$. Every party sends his/her optical pulse to a central untrusted node through a lossy optical channel. Here, the pulses are combined in a balanced multiport beam splitter [74] featuring a threshold detector at every output port. The central node announces whether each detector clicked or not and the parties only keep the rounds where exactly one detector clicked. These events are likely to be caused by the arrival and detection of just one photon, due to the unbalance towards the vacuum of the prepared state (30). Because of the balanced superposition generated by the multiport beam splitter, the detected photon could be sent by any party with equal probability. Thus, the main contribution to the N-qubit state shared by the parties conditioned on the single detection is a coherent superposition of states in which one qubit is in state $|1\rangle$ and all the others are in state $|0\rangle$, that is the mentioned W-class state. The qubits' relative coefficients have all equal weights but contain complex phases introduced by the multiport beam splitter.

It has been proven that the only multiqubit state yielding perfectly correlated and random outcomes upon performing local measurements is the GHZ state [34]. Nevertheless, the post-selected W-class state can still be used to distil a conference key. More specifically, the parties obtain the key bits by measuring their qubit in a specific direction in the X-Y plane of the Bloch sphere. The direction is the one that minimizes the bipartite QBER and depends on which detector clicked. For this reason, the protocol cannot be recast as a prepare-and-measure scheme, unlike its bipartite counterpart [73]. Finally, the parties estimate the eavesdropper's knowledge by computing the expectation value of the $Z^{\otimes N}$ operator and by checking when it differs from the ideal case. Note that if the parties are actually sharing a W-class state, then $\langle Z^{\otimes N}\rangle = -1$.

In [71] the security of the protocol is proved in the finite-key regime and under coherent attacks performed by the eavesdropper.

The W-class N-qubit state on which the protocol is based is post-selected thanks to single-photon interference at the central node. Hence, the resulting key rate scales linearly with the transmittance t of one of the quantum channels linking each party to the central node (if the channels are all symmetric). This contrasts with the honest implementations of the protocols [34, 65] presented in subsection III A, which are based on the distribution of N-qubit GHZ states. If these states are encoded, e.g., in the orthogonal polarizations of a photon, their key rate cannot scale better than t^N, where t is the transmittance of the link between one party and the central distributor of the N-partite entangled state. This makes the protocol based on the W state much more suited to high-loss scenarios than the protocols of subsection III A. This is clear from Fig. 3, where we plot the asymptotic conference key rates of protocols [71] (solid lines) and [34, 65] (dashed lines) as a function of the loss in the quantum channel linking one party to the central node ($-10\log_{10} t$). We assume ideal implementations where photon loss is the only source of error. We observe the existence of a loss threshold above which the protocol based on the W state [71] outperforms the protocols based on the distribution of GHZ states [34, 65]. Moreover, the required loss for which the protocol [71] outperforms the protocols [34, 65] decreases as the number of parties involved increases.

IV. CONTINUOUS VARIABLE CONFERENCE KEY AGREEMENT

Quantum conference keys may also be established by means of continuous variable (CV) quantum systems. Following the first of such protocols [75], which enables quantum conferencing among three parties without trusting the measurement devices, more general and refined protocols [76, 77] have been devised. The latter allow an arbitrary number of users to establish conference keys when linked to a central untrusted relay in a star network. These schemes would allow high-rate intra-city secure conferencing among several users.

Both protocols [76, 77] rely on the correlations generated by an N-mode CV GHZ state [78]:

$$|\mathrm{CVGHZ}\rangle_N = \frac{1}{\sqrt{\pi}}\int_{-\infty}^{\infty} dx |x\rangle^{\otimes N} \;, \qquad (31)$$

where $\{|x\rangle\}_x$ are the eigenstates of the $\hat{X}$ quadrature. However, while in [77] the central relay is required to generate such multipartite entangled state, in [76] the state is post-selected thanks to a multipartite CV Bell detection at the central relay. In particular, in [76] every user prepares a Gaussian-modulated coherent state $|\alpha_k\rangle$ ($k = 1, \dots N$) and sends it to the central relay. Here, a suitable cascade of beam splitters followed by homodyne detections of either quadrature $\hat{X}$ or quadrature $\hat{P}$ implement the multipartite Bell detection, whose outcome is made public. The Bell detection projects the incoming coherent states onto the CV GHZ state (31) up to displacements of the N modes. By employing the public data of the Bell detection, the parties post-process the variables $\{\alpha_k\}_{k=1}^N$ describing the prepared coherent states and neutralize the effect of the displacements. They are thus left with variables whose correlations reproduce those of the original CV GHZ state (31) and hence can be used to distil a conference key. This procedure closely resembles the seminal work on measurement-device-independent (MDI) QKD with discrete variables [79] and its CV counterpart [80], now applied to a multipartite scenario. Indeed, the fact that the measurements are only performed by the untrusted relay, makes the protocol in [76] an MDI multipartite QKD protocol. Nevertheless, its performance does not decrease exponentially with the number of users since the CV Bell detection is a deterministic process, unlike its discrete-variable counterpart [79].

Note that, unlike the discrete-variable scenario, here the correlated variables $\{\alpha_k\}_{k=1}^N$ used to distil a binary key are complex numbers. Nevertheless, one can still express the resulting key rate in terms of their mutual information $I(\alpha_k, \alpha_{k'})$ with the well-known Devetak-Winter formula [81], which is assumed to hold also for CV-QKD [82].

Compared to [76], the protocol in [77] is not MDI since the multipartite GHZ state generated in the untrusted relay is then distributed to the parties who perform trusted measurements. Moreover, from a practical point of view, this scheme is harder to implement, as it involves the preparation of several optical modes in squeezed states and their subsequent entanglement in a specific target state. Nevertheless, in principle, the scheme in [77] could achieve slightly higher performances than the more practical protocol in [76].

In terms of security, both protocols [76, 77] have been proved to be secure against collective Gaussian attacks. Furthermore, the protocol in [76] has been analyzed in the framework of finite-key composable security and proven to be secure against coherent attacks through a Gaussian de Finetti reduction [83].

V. DEVICE-INDEPENDENT CONFERENCE KEY AGREEMENT

In the device-independent scenario, Alice and the Bobs do not want to assume any knowledge about the distributed system and internal working of their devices. It is even considered that the shared states as well as the measurement devices can be manufactured by the adversary [84]. The parties' goal is to ensure security using only the observed statistics of inputs and outputs. In a device-independent protocol security is certified by the violation of a Bell inequality.

Note that in a device-independent conference key agreement (DICKA) protocol, an analysis against coherent attacks also needs to account for the fact that the eavesdropper might program the devices to behave in different ways at each round of the protocol. In particular the measurement devices could have memory and behave in correlation with the outcomes of previous rounds. This makes the security analysis in the fully device-independent adversarial scenario significantly more intricate.

A recently developed technique [8, 85], the entropy accumulation theorem (EAT), provides the tools to perform the security analysis of device-independent protocols in the fully adversarial scenario maintaining some noise robustness. The EAT [8, 85] extends the de Finnetti theorems [67, 86] to the device-independent setting, allowing to reduce the analysis to collective attacks.

Remark 1. *(Composability in the device-independent scenario) The security definition, Definition 4, implies universal composability of conference key agreement in the trusted device scenario. However, for the device-independent scenario, attacks proposed in Ref. [87] show that composability cannot be guaranteed if the same devices are re-used in a subsequent protocol. Indeed, in Ref. [87] the authors describe attacks in which information about a previously generated key may be leaked through the public communication of a subsequent run of the protocol, if the devices are re-used. The attacks described in Ref. [87] can be avoided if the parties have sufficient control of the internal memory of their devices and are able to re-set it after one execution of the protocol.*

Based on the EAT, a DICKA protocol was proposed in [88, 89]. The protocol of Ref. [88] initially considers the multipartite Mermin-Ardehali-Belinskii-Klyshko (MABK) inequalities [42–44]. However, as shown in [90], the MABK inequalities are not suitable for establishing a conference key, as an overhead amount of information is required for information reconciliation. In Ref. [89], a new multiparty inequality is introduced and positive conference key can be established in the device-independent scenario. Fig. 4 shows the asymptotic key rates for the device-independent protocol of Ref. [89] for $N = 3, 5, 8$, for an implementation in which all the qubits are submitted to a depolarizing channel.

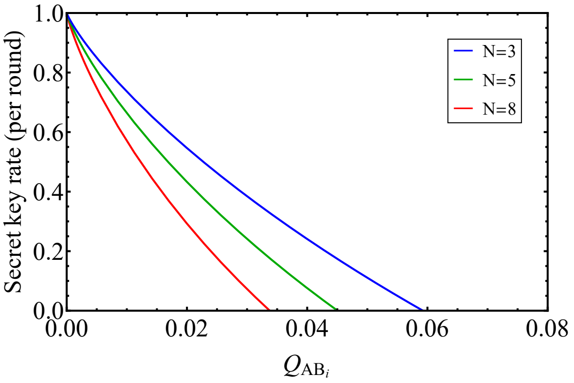

Figure 4. Asymptotic secret key rate for the DICKA protocol of Ref. [89] as a function of the QBER and for fixed number of parties ($N = 3, 5, 8$). We assumed an implementation where the N-party GHZ state is submitted to the depolarizing channel $\mathcal{D}_2^{\otimes N}(|\mathrm{GHZ}_N\rangle\langle\mathrm{GHZ}_N|)$.

The key rates derived in [89] are based on an analytical lower bound to von Neumann entropy of Alice's outcome conditioned on the information available to the eavesdropper, $H(A|E)$, as a function of the violation of the Bell inequality under consideration. The bound employs a relation between the considered multipartite inequality and the bipartite Clauser-Horne-Shimony-Holt (CHSH) inequality [10].

In general, it is not possible to compute directly $H(A|E)$ as a function of the violation for an arbitrary Bell inequality. This is due to the lack of knowledge about the underlying system. A lower bound can be obtained using the relation $H(A|E) \geq H_{\min}(A|E)$, where $H_{\min}(A|E)$ is the conditional min-entropy defined in (7). Due to the relation with the guessing probability, (7), the conditional min-entropy, $H_{\min}(A|E)$, can be estimated in the device-independent scenario [91] using the hierarchy of semi-definite approximations to the quantum set [92, 93]. This method is, however, computationally costly and may lead to non-tight bounds.

Bell inequalities tailored to DICKA protocols were further investigated in [94], where the authors introduced a family of multipartite Bell inequalities (containing the inequality of [89] as a special case) that are maximally violated by the GHZ state, with the Z-basis being one of the optimal measurements for Alice. These are essential features to build a device-independent conference key agreement protocol.

It is interesting to remark that the MABK inequalities were previously explored in other multiparty communication protocols. Refs. [95, 96] consider a secret sharing scenario in which Alice distributes the key in such a way that the $N-1$ Bobs need to collaborate to retrieve its value. The authors establish that, if the eavesdropper is restricted to individual attacks, then the violation of a MABK inequality can guarantee security, even if some of the Bobs collaborate with Eve. Even though this scenario was initially denoted N-party QKD [95, 96], it should be distiguished from the scenario we consider in this review: in which the goal is that all the Bobs can retrieve the key independently.

VI. MULTIPARTITE PRIVATE STATES

Most of the quantum conference key agreement protocols presented in the previous sections exploit the correlations of the multipartite GHZ state (9). Therefore, GHZ distillation protocols are in close connection with distillation of secret conference keys. Indeed, if the parties share several copies of a resource state that can be turned into a smaller number of GHZ states, then they could perform a distillation protocol followed by measurements to generate a secret key. The connection of entanglement distillation and conference key agreement protocols is discussed in [54]. Ref. [97], has recently investigated the limits on the performance of GHZ state distribution in a network, with and without quantum repeaters, and its consequence for CKA protocols based on the GHZ state.

However, it is not only through distillation of GHZ states that one can obtain a secret key. Indeed, as shown in [98], an ϵ-secure conference key can also be obtained from bound entangled states. This result generalizes an analogous one derived in the bipartite case [99].

The concept of private states [100] was generalized to the multipartite case in Ref. [98, 101]. Similar to the bipartite case, a multipartite private state can be seen as a twisted GHZ state tensored with an extra density matrix (the shield)

$$\Gamma^{(d)}_{A\vec{B}A'} = U_t(|\mathrm{GHZ}^d_N\rangle\langle\mathrm{GHZ}^d_N| \otimes \rho_{A'})U_t^\dagger, \tag{32}$$

where $|\mathrm{GHZ}^d_N\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\dots i\rangle$ is the N-party GHZ state of dimension d and the multipartite twisting is a unitary operation of the form

$$U_t = \sum_{i_1,\dots,i_N=0}^{d-1} |i_1\dots i_N\rangle\langle i_1\dots i_N| \otimes U_{i_1,\dots,i_N} \tag{33}$$

for arbitrary unitaries $U_{i_1,\dots,i_N}$ acting on A'.

Ref. [98] establishes that if from a resource state Alice and the Bobs can distill an ϵ-secret conference key, then there exists an LOCC protocol that can distill a state close to a private state (32) and vice-versa. They also exhibit examples of multipartite bound entangled states, that are states from which a GHZ state cannot be distilled, which are ϵ-close to private states. This establishes that distillation of GHZ states is not necessary for quantum conference key agreement and more general classes of protocols are possible.

In the framework of quantum channels and private state distillation, converse bounds on the rate at which a secret key can be distilled using multiplex channels were recently provided in [102]. Ref. [102] establishes that genuine multipartite entanglement is necessary for single shot key distillation. This implies that, if key can be distilled from n copies of a multipartite state ρ, then $\rho^{\otimes n}$ needs to be genuine multipartite entangled. However, this does not require that genuine multipartite entanglement is present at the single round level ρ. Indeed, a study of the entanglement properties required for a resource state to enable a conference key was recently performed in [103]. Results of Ref. [103] show that a conference key can be established even if the parties share a biseparable state in every round.

VII. OUTLOOK

We reviewed the state-of-the-art quantum CKA schemes based on multipartite entanglement. We discussed proposed protocols and their security proofs under different levels of assumptions for the characterisation of the devices, and for several types of implementations.

From an experimental point of view, the implementation of quantum CKA is increasingly accessible, due to key developments of its fundamental ingredients. Multipartite entanglement has been generated in a variety of physical systems, such as e.g. ion traps [104–106], photonic systems [107–111], superconducting circuits [112–114] and nuclear spin qubits in diamond [115]. Also, entanglement among several particles is naturally generated in atomic ensembles [116, 117], and methods to quantify and manipulate this entanglement are being developed [118–122]. A thermalised interacting photon gas [123] may also prove to be a suitable source of genuine multipartite entanglement. Recently, the first quantum CKA protocol has been implemented [124] among four parties. The experiment is based on the multiparty BB84 protocol [65] discussed in Section III A. It relies on the generation of polarization-encoded four-party GHZ states at telecom wavelength by a central quantum server. The states are then distributed to the four parties over up to 50 km of optical fibers, generating a secure conference key according to Definition 4.

While experimental progress is still necessary to scale implementations of quantum CKA to many users, improvements from the theory side are crucial to reduce the experimental demands. To this aim, the development of new protocols and new techniques to prove security will contribute to make quantum CKA a feasible technology.

Novel protocols exploring different resource states and network architectures can lead to improved performance and noise robustness. In the bi-partite case, QKD protocols for d-dimensional systems achieve higher rates and better noise tolerance [125] than the qubit-based protocols. In order to explore this possibility in the multipartite case, quantum CKA protocols for d-dimensional systems need to be developed. Such a generalization can also find applications in the layered protocol presented in [126]. In Ref. [126], asymmetric high-dimensional multipartite entangled states are used to design a layered protocol that establishes a secret key simultaneously between different subsets of users in a network.

Similarly, new tools to improve security proofs can lead to better rates and noise tolerance, especially for DICKA protocols. A family of Bell inequalities suitable for conference key agreement protocols has been introduced in [94]. However, only non-tight numerical lower bounds to the key rates are currently available for DICKA protocols based on these inequalities. The introduction of tighter analytical bounds addressing their security proofs could lead to higher key rates in DICKA protocols.

ACKNOWLEDGEMENTS

We thank Giacomo Carrara, Timo Holz, Carlo Ottaviani, Stefano Pirandola, Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki for helpful discussions. This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 - 390534769, by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662, and by the Federal Ministry of Education and Research BMBF (Project Q.Link.X and HQS).

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175 – 179, 1984.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, pp. 661–663, 1991.

[3] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nature Communications, vol. 3, p. 634, 2012.

[4] M. Hayashi and T. Tsurumaru, "Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths," New Journal of Physics, vol. 14, p. 093014, sep 2012.

[5] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum, vol. 1, p. 14, 2017.

[6] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, "Long-distance quantum key distribution in optical fibre," New Journal of Physics, vol. 8, pp. 193–193, sep 2006.

[7] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nature Photonics, vol. 9, pp. 163 – 168, mar 2015.

[8] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," Nature Communications, vol. 9, p. 459, 2018.

[9] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, "Towards a realization of device-independent quantum key distribution," Quantum Science and Technology, vol. 4, p. 035011, jul 2019.

[10] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," Phys. Rev. Lett., vol. 23, pp. 880–884, Oct 1969.

[11] M. Epping, H. Kampermann, and D. Bruß, "Large-scale quantum networks based on graphs," New Journal of Physics, vol. 18, p. 053036, may 2016.

[12] M. Epping, H. Kampermann, and D. Bruß, "Robust entanglement distribution via quantum network coding," New Journal of Physics, vol. 18, p. 103052, oct 2016.

[13] F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation," npj Quantum Information, vol. 5, no. 1, p. 76, 2019.

[14] A. Pirker, J. Wallnöfer, and W. Dür, "Modular architectures for quantum networks," New Journal of Physics, vol. 20, p. 053054, may 2018.

[15] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, "Light-matter entanglement over 50 km of optical fibre," npj Quantum Information, vol. 5, no. 1, p. 72, 2019.

[16] A. Tchebotareva, S. L. N. Hermans, P. C. Humphreys, D. Voigt, P. J. Harmsma, L. K. Cheng, A. L. Verlaan, N. Dijkhuizen, W. de Jong, A. Dréau, and R. Hanson, "Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength," Phys. Rev. Lett., vol. 123, p. 063601, Aug 2019.

[17] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett., vol. 120, p. 030501, Jan 2018.

[18] H. J. Kimble, "The quantum internet," Nature, vol. 453, no. 7198, pp. 1023–1030, 2008.

[19] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science, vol. 362, no. 6412, 2018.

[20] W.-G. Tzeng, "A practical and secure fault-tolerant conference-key agreement protocol," in Public Key Cryptography. PKC 2000. Lecture Notes in Computer Science. (Z. Y. Imai H., ed.), (Berlin, Heidelberg), pp. 1–13, Springer Berlin Heidelberg, 2000.

[21] Y.-M. Tseng, "An improved conference-key agreement protocol with forward secrecy," Informatica, vol. 16, p. 275, Jan 2005.

[22] S. Berkovits, "How to broadcast a secret," in Advances in Cryptology — EUROCRYPT '91 (D. W. Davies, ed.), (Berlin, Heidelberg), pp. 535–541, Springer Berlin Heidelberg, 1991.

[23] Guang-Huei Chiou and Wen-Tsuen Chen, "Secure broadcasting using the secure lock," IEEE Transactions on Software Engineering, vol. 15, pp. 929–934, Aug 1989.

[24] C. Elliott, "Building the quantum network," New Journal of Physics, vol. 4, pp. 46–46, jul 2002.

[25] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in Quantum Information and Computation III (E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds.), vol. 5815, pp. 138 – 149, International Society for Optics and Photonics, SPIE, 2005.

[26] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in vienna," New Journal of Physics, vol. 11, p. 075001, jul 2009.

[27] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," Chinese Science Bulletin, vol. 54, pp. 2991–2997, Sep 2009.

[28] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," New Journal of Physics, vol. 13, p. 123001, dec 2011.

[29] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo qkd network," Opt. Express, vol. 19, pp. 10387–10409, May 2011.

[30] R. Courtland, "China's 2,000-km quantum link is almost complete [news]," IEEE Spectrum, vol. 53, pp. 11–12, November 2016.

[31] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature, vol. 549, pp. 43 – 47, sep 2017.

[32] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett., vol. 120, p. 030501, Jan 2018.

[33] M. Epping, H. Kampermann, and D. Bruß, "Large-scale quantum networks based on graphs," New Journal of Physics, vol. 18, p. 053036, 2016.

[34] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, "Multi-partite entanglement can speed up quantum key distribution in networks," New Journal of Physics, vol. 19, p. 093012, sep 2017.

[35] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Rev. Mod. Phys., vol. 81, p. 865, June 2009.

[36] O. Gühne and G. Tóth, "Entanglement detection," Physics Reports, vol. 474, no. 1, pp. 1 – 75, 2009.

[37] C. Eltschka and J. Siewert, "Quantifying entanglement resources," Journal of Physics A: Mathematical and Theoretical, vol. 47, p. 424005, oct 2014.

[38] I. Bengtsson and K. Zyczkowski, "A brief introduction to multipartite entanglement," 2016. arXiv:quant-ph/1612.07747.

[39] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," Phys. Rev. A, vol. 62, p. 062314, Nov 2000.

[40] J. I. de Vicente, C. Spee, and B. Kraus, "Maximally entangled set of multipartite quantum states," Phys. Rev. Lett., vol. 111, p. 110502, Sep 2013.

[41] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," 2007. arXiv:quant-ph/0712.0921.

[42] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states," Phys. Rev. Lett., vol. 65, pp. 1838–1840, Oct 1990.

[43] M. Ardehali, "Bell inequalities with a magnitude of violation that grows exponentially with the number of particles," Phys. Rev. A, vol. 46, pp. 5375–5378, Nov 1992.

[44] A. V. Belinskiĭ and D. N. Klyshko, "Interference of light and Bell's theorem," Physics-Uspekhi, vol. 36, pp. 653–693, aug 1993.

[45] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," 2014. arXiv:quant-ph/1409.3525.

[46] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in Proceedings 42nd IEEE Symposium on Foundations of Computer Science, pp. 136–145, Oct 2001.

[47] M. Ben-Or and D. Mayers, "General security definition and composability for quantum & classical protocols," 2004. quant-ph/0409062.

[48] R. Renner, "Security of quantum key distribution," International Journal of Quantum Information, vol. 06, no. 01, pp. 1–127, 2008.

[49] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," IEEE Transactions on Information Theory, vol. 57,

pp. 5524–5535, Aug 2011.

[50] M. Tomamichel, "Quantum information processing with finite resources," SpringerBriefs in Mathematical Physics, 2016.

[51] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Transactions on Information Theory, vol. 55, pp. 4337–4347, Sep. 2009.

[52] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett., vol. 81, pp. 3018–3021, Oct 1998.

[53] A. Cabello, "Multiparty key distribution and secret sharing based on entanglement swapping," 2000. arXiv:quant-ph/0009025.

[54] K. Chen and H. Lo, "Multi-partite quantum cryptographic protocols with noisy GHZ states," Quantum Information & Computation, vol. 7, no. 8, pp. 689–715, 2007.

[55] E. N. Maneva and J. A. Smolin, "Improved two-party and multi-party purification protocols," in Quantum computation and information (Washington, DC, 2000), vol. 305 of Contemp. Math., pp. 203–212, Amer. Math. Soc., Providence, RI, 2002.

[56] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, "Multiparticle entanglement purification protocols," Phys. Rev. A, vol. 57, pp. R4075–R4078, Jun 1998.

[57] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol. 54, pp. 1098–1105, Aug 1996.

[58] A. Steane, "Multiple-particle interference and quantum error correction," Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, vol. 452, no. 1954, pp. 2551–2577, 1996.

[59] D. Gottesman and Hoi-Kwong Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Transactions on Information Theory, vol. 49, pp. 457–475, Feb 2003.

[60] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Transactions on Information Theory, vol. 39, pp. 733–742, May 1993.

[61] J. Bae and A. Acín, "Key distillation from quantum channels using two-way communication protocols," Phys. Rev. A, vol. 75, p. 012334, Jan 2007.

[62] B. Kraus, C. Branciard, and R. Renner, "Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses," Phys. Rev. A, vol. 75, p. 012316, Jan 2007.

[63] W. Dür, J. I. Cirac, and R. Tarrach, "Separability and distillability of multiparticle quantum systems," Phys. Rev. Lett., vol. 83, pp. 3562–3565, Oct 1999.

[64] W. Dür and J. I. Cirac, "Classification of multiqubit mixed states: Separability and distillability properties," Phys. Rev. A, vol. 61, p. 042314, Mar 2000.

[65] F. Grasselli, H. Kampermann, and D. Bruß, "Finite-key effects in multipartite quantum key distribution protocols," New Journal of Physics, vol. 20, p. 113014, nov 2018.

[66] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," Phys. Rev. Lett., vol. 106, p. 110506, Mar 2011.

[67] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," Phys. Rev. Lett., vol. 102, p. 020504, Jan 2009.

[68] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," IEEE Transactions on Information Theory, vol. 55, no. 12, pp. 5840–5847, 2009.

[69] J. Preskill, "Quantum Computing in the NISQ era and beyond," Quantum, vol. 2, p. 79, 2018.

[70] R. Matsumoto, "Multiparty quantum-key-distribution protocol without use of entanglement," Phys. Rev. A, vol. 76, p. 062316, Dec 2007.

[71] F. Grasselli, H. Kampermann, and D. Bruß, "Conference key agreement with single-photon interference," New Journal of Physics, vol. 21, p. 123002, dec 2019.

[72] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, no. 7705, pp. 400–403, 2018.

[73] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," npj Quantum Information, vol. 5, no. 1, p. 64, 2019.

[74] M. Zukowski, A. Zeilinger, and M. A. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters," Phys. Rev. A, vol. 55, pp. 2564–2579, Apr 1997.

[75] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication," Phys. Rev. A, vol. 93, p. 022325, Feb 2016.

[76] R. L. C. Ottaviani, C. Lupo and S. Pirandola, "Modular network for high-rate quantum conferencing," Communications Physics, vol. 2, no. 118, 2019.

[77] Z. Zhang, R. Shi, and Y. Guo, "Multipartite continuous variable quantum conferencing network with entanglement in the middle," Applied Sciences, vol. 8, no. 8, 2018.

[78] P. van Loock and A. Furusawa, "Detecting genuine multipartite continuous-variable entanglement," Phys. Rev. A, vol. 67, p. 052315, May 2003.

[79] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett., vol. 108, p. 130503, 2012.

[80] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," Nature Photonics, vol. 9, no. 6, pp. 397–402, 2015.

[81] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A, vol. 461, January 2005.

[82] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," Entropy, vol. 17, no. 9, pp. 6072–6092, 2015.

[83] A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de Finetti reduction," Phys. Rev. Lett., vol. 118, p. 200501, 2017.

[84] Some assumptions are still present in the device-independent scenario, such as isolated labs and trusted random number generators (see [9] for a discussion).

[85] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation," 2016. arXiv:quant-ph/1607.01796.

[86] R. König and R. Renner, "A de Finetti representation for finite symmetric quantum states," Journal of Mathematical Physics, vol. 46, no. 12, p. 122108, 2005.

[87] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," Phys. Rev. Lett., vol. 110, p. 010503, Jan 2013.

[88] J. Ribeiro, G. Murta, and S. Wehner, "Fully device-independent conference key agreement," Phys. Rev. A, vol. 97, p. 022307, Feb 2018.

[89] J. Ribeiro, G. Murta, and S. Wehner, "Reply to "comment on 'fully device-independent conference key agreement' "," Phys. Rev. A, vol. 100, p. 026302, Aug 2019.

[90] T. Holz, D. Miller, H. Kampermann, and D. Bruß, "Comment on "fully device-independent conference key agreement"," Phys. Rev. A, vol. 100, p. 026301, Aug 2019.

[91] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," Nature Communications, vol. 2, p. 238, jul 2008.

[92] M. Navascues, S. Pironio, and A. Acin, "Bounding the set of quantum correlations," Phys. Rev. Lett., vol. 98, p. 010401, Jan 2007.

[93] M. Navascues, S. Pironio, and A. Acin, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," New Journal of Physics, vol. 10, p. 073013, jul 2008.

[94] T. Holz, H. Kampermann, and D. Bruß, "A genuine multipartite bell inequality for device-independent conference key agreement," 2019. arXiv:quant-ph/1910.11360.

[95] V. Scarani and N. Gisin, "Quantum communication between n partners and Bell's inequalities," Phys. Rev. Lett., vol. 87, p. 117901, Aug 2001.

[96] V. Scarani and N. Gisin, "Quantum key distribution between n partners: Optimal eavesdropping and bell's inequalities," Phys. Rev. A, vol. 65, p. 012311, Dec 2001.

[97] M. Takeoka, E. Kaur, W. Roga, and M. M. Wilde, "Multipartite entanglement and secret key distribution in quantum networks," 2019. arXiv:1912.10658.

[98] R. Augusiak and P. Horodecki, "Multipartite secret key distillation and bound entanglement," Phys. Rev. A, vol. 80, p. 042307, Oct 2009.

[99] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," Phys. Rev. Lett., vol. 94, p. 160502, Apr 2005.

[100] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "General paradigm for distilling classical key from quantum states," IEEE Transactions on Information Theory, vol. 55, pp. 1898–1929, April 2009.

[101] P. Horodecki and R. Augusiak, "Quantum states representing perfectly secure bits are always distillable," Phys. Rev. A, vol. 74, p. 010302, Jul 2006.

[102] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, "Universal limitations on quantum key distribution over a network," 2019. arXiv:1912.03646.

[103] G. Carrara, H. Kampermann, D. Bruß, and G. Murta, "In preparation," 2020.

[104] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland, "Creation of a six-atom 'schrödinger cat' state," Nature, vol. 438, no. 7068, pp. 639–642, 2005.

[105] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, "Scalable multiparticle entanglement of trapped ions," Nature, vol. 438, no. 7068, pp. 643–646, 2005.

[106] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Haensel, M. Hennrich, and R. Blatt, "14-qubit entanglement: creation and coherence," Phys. Rev. Lett., vol. 106, p. 130506, 2011.

[107] J.-W. P. et al., "Multiphoton entanglement and interferometry," Rev. Mod. Phys., vol. 84, p. 777, 2012.

[108] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, "Observation of eight-photon entanglement," Nature Photonics, vol. 6, no. 4, pp. 225–228, 2012.

[109] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan, "Experimental ten-photon entanglement," Phys. Rev. Lett., vol. 117, p. 210502, Nov 2016.

[110] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, H. Li, L. Zhang, Z. Wang, L. You, X.-L. Wang, X. Jiang, L. Li, Y.-A. Chen, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion," Phys. Rev. Lett., vol. 121, p. 250505, Dec 2018.

[111] M. Malik, M. Erhard, M. Huber, M. Krenn, R. Fickler, and A. Zeilinger, "Multi-photon entanglement in high dimensions," Nature Photonics, vol. 10, no. 4, pp. 248–252, 2016.

[112] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, "Superconducting quantum circuits at the surface code threshold for fault tolerance," Nature, vol. 508, no. 7497, pp. 500–503, 2014.

[113] C. Song, K. Xu, W. Liu, C.-p. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y.-A. Chen, C.-Y. Lu, S. Han, and J.-W. Pan, "10-qubit entanglement and parallel logic operations with a superconducting circuit," Phys. Rev. Lett., vol. 119, p. 180511, Nov 2017.

[114] M. G. et al, "Genuine 12-qubit entanglement on a superconducting quantum processor," Phys. Rev. Lett., vol. 122, p. 110501, 2019.

[115] S. B. van Dam, J. Cramer, T. H. Taminiau, and R. Hanson, "Multipartite entanglement generation and contextuality tests using non-destructive three-qubit parity measurements," Phys. Rev. Lett., vol. 123, p. 050401, 2019.

[116] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein, "Quantum metrology with nonclassical states of atomic ensembles," Rev. Mod. Phys., vol. 90, p. 035005, Sep 2018.

[117] J. Ma, X. Wang, C. Sun, and F. Nori, "Quantum spin squeezing," Physics Reports, vol. 509, no. 2, pp. 89 – 165, 2011.

[118] B. Lücke, J. Peise, G. Vitagliano, J. Arlt, L. Santos, G. Tóth, and C. Klempt, "Detecting multiparticle en-

tanglement of dicke states," Phys. Rev. Lett., vol. 112, p. 155304, Apr 2014.

[119] M. F. Riedel, P. Böhi, Y. Li, T. W. Hänsch, A. Sinatra, and P. Treutlein, "Atom-chip-based generation of entanglement for quantum metrology," Nature, vol. 464, no. 7292, pp. 1170–1173, 2010.

[120] P. Kunkel, M. Prüfer, H. Strobel, D. Linnemann, A. Frölian, T. Gasenzer, M. Gärttner, and M. K. Oberthaler, "Spatially distributed multipartite entanglement enables epr steering of atomic clouds," Science, vol. 360, no. 6387, pp. 413–416, 2018.

[121] M. Fadel, T. Zibold, B. Décamps, and P. Treutlein, "Spatial entanglement patterns and Einstein-Podolsky-Rosen steering in Bose-Einstein condensates," Science, vol. 360, no. 6387, pp. 409–413, 2018.

[122] K. Lange, J. Peise, B. Lücke, I. Kruse, G. Vitagliano, I. Apellaniz, M. Kleinmann, G. Tóth, and C. Klempt, "Entanglement between two spatially separated atomic modes," Science, vol. 360, no. 6387, pp. 416–418, 2018.

[123] D. Dung, C. Kurtscheid, T. Damm, J. Schmitt, F. Vewinger, M. Weitz, and J. Klaers, "Variable potentials for thermalized light and coupled condensates," Nature Photonics, vol. 11, p. 565, 2017.

[124] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, "Experimental quantum conference key agreement," 2020. arXiv:quantum-ph/2002.01491.

[125] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," Phys. Rev. A, vol. 82, p. 030301, Sep 2010.

[126] M. Pivoluska, M. Huber, and M. Malik, "Layered quantum key distribution," Phys. Rev. A, vol. 97, p. 032312, Mar 2018.

H Analytical entropic bounds for multiparty device-independent cryptography

Title:	Analytical entropic bounds for multiparty device-independent cryptography
Authors:	Federico Grasselli, Gláucia Murta, Hermann Kampermann and Dagmar Bruß
Journal:	npj Quantum Information
Impact factor:	9.206 (2017)
Date of submission:	15 May 2020
Publication status:	Under review
Contribution by FG:	First author (input approx. 75%)

This publication corresponds to reference [Gra+20]. A summary of its content is presented in chapter 7.

HK, GM and DB triggered the consideration of this research project. I developed the project while having regular discussions with GM and HK on our intermediate results and on the direction of the project. I derived most of the proofs of the results presented in the manuscript and performed the analytical calculations of the conditional entropies. In particular, I proved the two main theorems of the paper (Theorem 1 and 2) and provided the proofs of the statements in sections II and III of the Supplementary Information attached to the manuscript. I also contributed in proving the statements in sections I, V and VI of the same attachment. I wrote the whole manuscript except for section I and parts of sections V and VI of the Supplementary Information, which were written by GM and HK. I performed all the numerical simulations which played a decisive role in revealing the optimal states minimizing the considered conditional entropies. The plots included in the manuscript were also obtained by me. All the authors contributed to the discussion of the results and to reviewing the manuscript.

arXiv:2004.14263v2 [quant-ph] 15 May 2020

Analytical entropic bounds for multiparty device-independent cryptography

Federico Grasselli,[1,*] Gláucia Murta,[1,†] Hermann Kampermann,[1] and Dagmar Bruß[1]
[1] *Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany*

We consider a device-independent (DI) scenario where N parties test a generic full-correlator Bell inequality with two inputs and two outcomes per party. By exploiting the inequality's symmetries, we drastically simplify the general form of the quantum state that can be considered, without loss of generality. We then focus on the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality and derive an upper bound on the maximal violation of the MABK inequality by an arbitrary N-qubit state, as a function of the state's parameters. The two results enable us to derive analytical bounds on the von Neumann entropy of the parties' outcomes, conditioned on the eavesdropper's information. These quantities are crucial for the security of most cryptographic protocols and better bounds significantly impact the protocols' performance. In particular, we bound the conditional entropy of a single party's outcome and the joint conditional entropy of two parties' outcomes, as a function of the MABK violation observed by three parties. We extend the former bound to N parties and prove its tightness, while we observe that the latter bound significantly improves previous results.

INTRODUCTION

Stimulated by data security concerns and by commercial opportunities, several companies and governments are increasingly investing resources in quantum cryptography technologies [1, 2]. Those include, most prominently, quantum key distribution (QKD) [3–10] and quantum random number generation [11, 12]. The former enables two parties to establish an information-theoretically secure shared key, while the latter is considered the only source of genuine randomness. In the context of emerging quantum networks [13–20], the task of QKD can be generalized to quantum conference key agreement (CKA) [21–27]. Here, N parties establish a common secret key to securely broadcast messages within their network, as proved recently in the first CKA experiment [28]. However, it is challenging to ensure that the assumptions on the implementation of these cryptographic tasks are met in practice, hence jeopardizing their security.

This led to the development of device-independent (DI) cryptographic protocols, whose security holds independently of the actual functioning of the quantum devices and is based on the observation of a Bell inequality violation [29]. Such protocols include DIQKD [30–38] and DICKA [39–42] schemes, where a secret key is shared by two or more parties, respectively. Otherwise, with DI randomness generation (DIRG) protocols [43–53] one can generate intrinsic randomness which is guaranteed to be private thanks to a Bell violation.

A crucial aspect of any DI protocol is the ability to carefully estimate, from the observed Bell violation, the minimum amount of uncertainty that a potential eavesdropper, Eve, could have about the protocol's outputs. Indeed, this quantity determines the length of the secret random bitstring that can be distilled from the protocol's outputs. Eve's uncertainty is often quantified by an appropriate conditional von Neumann entropy [6, 32, 33, 37], relative to the effective state shared by the parties in a generic round of the protocol. The goal is to minimize the entropy over all the possible states yielding the observed Bell inequality violation.

This task can be carried out numerically, however the available techniques [54–57] focus on minimizing a lower bound on the von Neumann entropy, namely the min-entropy [6], thus producing sub-optimal results. Here we follow an analytical approach that reduces the degrees of freedom of the generic state shared by the parties without loss of generality, by exploiting the symmetries of the considered Bell inequality. The resulting state depends on a small number of parameters, allowing a direct minimization of the conditional von Neumann entropy. This can result in a tight bound of the eavesdropper's uncertainty, which directly translates to an increased performance of the protocols. To the best of our knowledge, such an analytical procedure has only been developed by Pironio et al. [33] in the case of two parties testing the Clauser-Horne-Shimony-Holt (CHSH) inequality [58].

In this work we develop a similar analytical procedure, applicable to a broad class of DI scenarios. Specifically, we consider N parties, each equipped with two measurement settings with binary outcomes, testing a generic full-correlator Bell inequality –i.e. an inequality where each correlator involves every party [59]. Without loss of generality, we reduce the density matrix of the generic state shared by the N parties to a $2^N \times 2^N$ diagonal matrix, except for $2^{N-1} - N$ purely imaginary off-diagonal terms. This means, for instance, that three parties share a state completely determined by only eight independent parameters (one is removed due to normalization). Notably, we recover the result of Pironio et al. when $N = 2$.

We then focus on the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequality [60–62] and derive an analytical bound on the maximal violation of the MABK inequality obtained by performing rank-one projective measurements on an arbitrary N-qubit state, as a func-

[*] corresponding author: federico.grasselli@hhu.de
[†] corresponding author: glaucia.murta@hhu.de

tion of the state's parameters. This is a result of independent interest, which generalizes the bound for the bipartite case of [63] and constitutes, to our knowledge, the first of this kind valid for an arbitrary N-qubit state.

By combining the results on the state reduction and on the MABK violation upper bound, we obtain analytical bounds on relevant conditional von Neumann entropies when three parties, Alice, Bob and Charlie, test the MABK inequality. Specifically, we obtain a tight lower bound on the von Neumann entropy of Alice's outcome conditioned on the eavesdropper's information. We extend the bound to N parties by showing that it coincides with one derived previously [64] on completely different grounds and with no allegation of tightness. The bound can find potential application in DIRG based on multipartite nonlocality. We also provide a heuristic argument for which full-correlator Bell inequalities, such as the MABK inequality, are unlikely to be employed in any DICKA protocol.

In the same tripartite context, we derive a lower bound on the joint conditional von Neumann entropy of Alice and Bob's outcomes, which substantially improves the result derived in [49], where the authors bound the corresponding min-entropy. The derived bound can be employed in proving the security of DI global randomness generation schemes.

RESULTS

Reduction of the N-party quantum state

Consider a DI scenario with N parties, denoted Alice$_1$, ..., Alice$_N$. The parties test a generic full-correlator Bell inequality [59] where each of them can choose among two measurement settings with binary outcomes. We identify this as the $(N, 2, 2)$ DI scenario. We assume the setup to be characterized by an eavesdropper, Eve, distributing an unknown quantum state to the parties, and by unknown dichotomic observables $A_x^{(i)}$ representing the possible measurements settings ($x = 0, 1$) for each party ($i = 1, \ldots, N$). Then, the considered Bell inequality is a linear combination of full-correlators of the form:

$$\left\langle A_{x_1}^{(1)} \cdots A_{x_N}^{(N)} \right\rangle . \tag{1}$$

From the observed Bell violation, the parties could quantify Eve's uncertainty on some of their outcomes by computing an appropriate conditional von Neumann entropy. With this result, they could enhance their outcomes' privacy (privacy amplification [6]) and use them for various cryptographic tasks (e.g. DICKA or DIRG).

Here we present a fundamental result which enables a direct computation of the conditional von Neumann entropy of interest.

We first define the GHZ basis [21] for the Hilbert space of N qubits as follows.

Definition 1. *The GHZ basis for the set of N-qubit states is composed of the following 2^N states:*

$$|\psi_{\sigma,\vec{u}}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle |\vec{u}\rangle + (-1)^{\sigma} |1\rangle |\bar{\vec{u}}\rangle \right), \tag{2}$$

where $\sigma \in \{0,1\}$ while $\vec{u} \in \{0,1\}^{N-1}$ and $\bar{\vec{u}} = \vec{1} \oplus \vec{u}$ are $(N-1)$-bit strings. In particular, for a three-qubit state, the GHZ basis reads:

$$|\psi_{i,j,k}\rangle = \frac{1}{\sqrt{2}} \left(|0, j, k\rangle + (-1)^{i} |1, \bar{j}, \bar{k}\rangle \right) \quad i, j, k \in \{0, 1\}, \tag{3}$$

where the bar over a bit indicates its negation.

We can now state the first major result of this work, the proof of which is reported in the Methods section.

Theorem 1. *Let N parties test an $(N, 2, 2)$ full-correlator Bell inequality. It is not restrictive to assume that, in each round, Eve distributes a mixture $\sum_\alpha p_\alpha \rho_\alpha$ of N-qubit states ρ_α, together with a flag $|\alpha\rangle$ (known to her) which determines the measurements performed on ρ_α given the parties' inputs. Without loss of generality, the measurements performed by each device on ρ_α are rank-one binary projective measurements in the (x, y)-plane of the Bloch sphere. Moreover, each state ρ_α is diagonal in the GHZ basis, except for some purely imaginary off-diagonal terms:*

$$\begin{aligned}\rho_\alpha = \sum_{\vec{u} \in \{0,1\}^{N-1}} & [\lambda_{0\vec{u}}^{\alpha} |\psi_{0,\vec{u}}\rangle\langle\psi_{0,\vec{u}}| + \lambda_{1\vec{u}}^{\alpha} |\psi_{1,\vec{u}}\rangle\langle\psi_{1,\vec{u}}| \\ & + \mathbb{i} s_{\vec{u}}^{\alpha} \left(|\psi_{0,\vec{u}}\rangle\langle\psi_{1,\vec{u}}| - |\psi_{1,\vec{u}}\rangle\langle\psi_{0,\vec{u}}| \right)],\end{aligned} \tag{4}$$

Finally, N arbitrary off-diagonal terms $s_{\vec{u}}^{\alpha}$ can be assumed to be zero. Independently, N pairs of the form $(\lambda_{0\vec{u}}^{\alpha}, \lambda_{1\vec{u}}^{\alpha})$ can be arbitrarily ordered (e.g. $\lambda_{0\vec{u}}^{\alpha} \geq \lambda_{1\vec{u}}^{\alpha}$).

In the following we focus our analysis on a given state ρ_α. Hence, for ease of notation we drop the symbol α in the parameters related to the state ρ_α (e.g. $\lambda_{0,\vec{u}}^{\alpha}$ and $s_{\vec{u}}^{\alpha}$) when there is no ambiguity.

Note that, for $N = 2$, we recover the result of [33]. By applying Theorem 1 to the case of $N = 3$ parties, it is not restrictive to assume that they share a mixture of states ρ_α, with the following matrix representation in the GHZ basis:

$$\rho_\alpha = \begin{bmatrix} \lambda_{000} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_{100} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{001} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{101} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_{010} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_{110} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{011} & \mathbb{i}s \\ 0 & 0 & 0 & 0 & 0 & 0 & -\mathbb{i}s & \lambda_{111} \end{bmatrix} . \tag{5}$$

The eigenvalues of (5) are given by:

$$\begin{aligned} \rho_{ijk} &= \lambda_{ijk} \quad (j,k) \neq (1,1) \\ \rho_{i11} &= \frac{\lambda_{011} + \lambda_{111} + (-1)^i \sqrt{(\lambda_{011} - \lambda_{111})^2 + 4s^2}}{2} . \end{aligned} \tag{6}$$

Upper bound on MABK violation

The MABK inequality [60–62] is one possible generalization of the CHSH inequality [58] and is derived on the following MABK operator.

Definition 2. *The MABK operator M_N is defined by recursion [64, 65]:*

$$\begin{aligned} M_2 &= G_{\mathrm{CHSH}}(A_0^{(1)}, A_1^{(1)}, A_0^{(2)}, A_1^{(2)}) \\ &\equiv A_0^{(1)} \otimes A_0^{(2)} + A_0^{(1)} \otimes A_1^{(2)} + A_1^{(1)} \otimes A_0^{(2)} \\ &\quad - A_1^{(1)} \otimes A_1^{(2)} \\ M_N &= \frac{1}{2} G_{\mathrm{CHSH}}(M_{N-1}, \overline{M_{N-1}}, A_0^{(N)}, A_1^{(N)}), \end{aligned} \tag{7}$$

where $A_{x_i}^{(i)}$ for $x_i = 0, 1$ are the binary observables of Alice$_i$ $((A_{x_i}^{(i)})^\dagger = A_{x_i}^{(i)}$ *and* $(A_{x_i}^{(i)})^2 \leq \mathrm{id})$ *and where $\overline{M_l}$ is the operator obtained from M_l by replacing every observable $A_{x_i}^{(i)}$ with $A_{1-x_i}^{(i)}$. For $N = 3$, the MABK operator reads:*

$$\begin{aligned} M_3 =& A_0 \otimes B_0 \otimes C_1 + A_0 \otimes B_1 \otimes C_0 \\ &+ A_1 \otimes B_0 \otimes C_0 - A_1 \otimes B_1 \otimes C_1 \end{aligned} \tag{8}$$

where A_x, B_y and C_z are Alice's, Bob's and Charlie's observables, respectively.

Then the N-partite MABK inequality reads as follows:

$$\langle M_N \rangle = \mathrm{Tr}[M_N \rho] \leq \begin{cases} 2, & \text{classical bound} \\ 2^{N/2}, & \text{GME threshold} \\ 2^{(N+1)/2} & \text{quantum bound} \end{cases} \tag{9}$$

where M_N is the MABK operator and a violation of the GME threshold implies that the parties share a genuine multipartite entangled (GME) state.

The second major result is an upper bound on the maximal MABK violation obtained when N parties share an N-qubit state and perform rank-one projective measurements on the respective qubits. The bound is state-dependent and tight on certain classes of states (proof and tightness conditions in Methods). This is, to the best of our knowledge, the first bound of such kind for an N-partite Bell inequality. Recently, the authors in [66] derived a similar bound in the $N = 3$ case. Our bound is tight on a larger set of states (discussion in Methods) and is valid for general N.

Theorem 2. *The maximum violation $\mathcal{M}_\rho$ of the N-partite MABK inequality* (9)*, attained with rank-one projective measurements on an N-qubit state ρ, satisfies*

$$\mathcal{M}_\rho \leq 2\sqrt{t_0 + t_1} \tag{10}$$

where t_0 and t_1 are the largest and second-to-the-largest eigenvalues of the matrix $T_\rho T_\rho^T$, where T_ρ is the correlation matrix of ρ.

We define the correlation matrix of an N-qubit state as follows.

Definition 3. *The correlation matrix of an N-qubit state ρ, T_ρ, is a square or rectangular matrix defined by the elements $[T_\rho]_{ij} = \mathrm{Tr}[\rho \sigma_{\nu_1} \otimes \ldots \otimes \sigma_{\nu_N}]$ such that:*

$$\begin{aligned} i &= 1 + \sum_{k=1}^{\lceil N/2 \rceil} 3^{\lceil N/2 \rceil - k} (\nu_k - 1) \\ j &= 1 + \sum_{k=\lceil N/2 \rceil + 1}^{N} 3^{N-k} (\nu_k - 1) \end{aligned} \tag{11}$$

where $\nu_1, \ldots, \nu_N \in \{1, 2, 3\}$, σ_{ν_i} are the Pauli operators and $\lceil x \rceil$ returns the smallest integer greater or equal to x.

Remark. *We remark that the most general measurements to be considered in computing the maximal MABK violation are projective measurements defined by observables $(A_{x_i}^{(i)})^2 = \mathrm{id}$* [59]*, since POVMs never provide higher violations* [67, 68]*. Such measurements on qubits reduce to either* (i) *rank-one projective measurements given by $A_{x_i}^{(i)} = \vec{a}_{x_i}^i \cdot \vec{\sigma}$ with unit vectors $\vec{a}_{x_i}^i \in \mathbb{R}^3$ and where $\vec{\sigma} = (X, Y, Z)^T$ is the vector of Pauli operators, or* (ii) *rank-two projective measurements given by the identity $A_{x_i}^{(i)} = \pm\mathrm{id}$, i.e. measurements with a fixed outcome. While for $N = 2$ parties the identity does not lead to any violation* [63] *and the optimal measurements are described by case* (i)*, in a multipartite scenario case* (ii) *cannot be ignored.*

For instance, if $N = 3$ parties share the state $\mathrm{id}/2 \otimes |\psi_{00}\rangle\langle\psi_{00}|$ (with $|\psi_{00}\rangle$ given in Definition 1), an MABK violation of $2\sqrt{2}$ is achieved if the first party measures $A_0^{(1)} = A_1^{(1)} = \mathrm{id}$, whereas no violation is obtained if her measurements are restricted to $A_{x_i}^{(i)} = \vec{a}_{x_i}^i \cdot \vec{\sigma}$.

We point out that previous works [66, 69–71] addressing the violation of multipartite Bell inequalities achieved by a given multi-qubit state have neglected case (ii) and only considered case (i). By applying the above example, we stress that the results of [66, 69–71] characterizing Bell violations yielded by multi-qubit states are, in fact, less general than claimed.

Nevertheless, for states whose maximal violation is above the GME threshold, the bound we provide in Theorem 2 is general and holds independently of the parties' measurements. Indeed, measuring the identity cannot lead to violations above the GME threshold and thus case (i) is already the most general.

By applying Theorem 2 to the state ρ_α in (5), we obtain an upper bound on the maximal MABK violation $\mathcal{M}_\alpha$ achievable on ρ_α with rank-one projective measurements.

Corollary 1. *For a tripartite state ρ_α of the form given in* (5)*, the maximal violation $\mathcal{M}_\alpha$ of the MABK inequal-*

ity achieved with rank-one projective measurements satisfies:

$$\mathcal{M}_\alpha \leq \mathcal{M}_\alpha^\uparrow = 4\sqrt{\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk})^2}, \tag{12}$$

where $\{\rho_{ijk}\}$ *are the eigenvalues of the state* ρ_α*, as specified in* (6)*.*

In the Methods section, we provide the tightness conditions (75) for which the upper bound in (12) is achieved.

Tight conditional entropy bound

Consider the $(3, 2, 2)$ DI scenario where Alice, Bob and Charlie test the tripartite MABK inequality in order to quantify Eve's uncertainty on Alice's outcome X, by computing the conditional von Neumann entropy $H(X|E)$. We emphasize that, in a DIRG protocol, the entropy $H(X|E)$ determines the asymptotic rate of secret random bits extracted by applying privacy amplification [6] on Alice's X outcomes [72, 73]. Similarly, in DICKA the secret key rate is determined by $H(X|E)$ decreased by the amount of classical information disclosed by the parties in the other steps of the protocol [41, 64, 72].

We derive a tight analytical lower bound on $H(X|E)$ as a function of the observed MABK violation. Theorem 1 guarantees that we can restrict the computation of the conditional entropy $H(X|E_{\text{tot}})$ over a mixture of states ρ_α of the form (5) and to rank-one projective measurements performed by the parties. We emphasize that the total information $E_{\text{tot}} = E\Xi$ available to Eve includes the knowledge of the flag Ξ which carries the value of α (see Methods). The goal is to lower bound the conditional entropy with a function F of the observed MABK violation m. The bound is tight if, for any given MABK violation m, there exist a quantum state and a set of measurements that achieve that violation and whose conditional entropy is exactly given by $F(m)$.

Thanks to Theorem 1, we can be express the conditional entropy $H(X|E_{\text{tot}})$ as follows:

$$\begin{aligned} H(X|E_{\text{tot}}) &= \sum_\alpha p_\alpha H(X|E\Xi = \alpha) \\ &= \sum_\alpha p_\alpha H(X|E)_{\rho_\alpha}, \end{aligned} \tag{13}$$

as a matter of fact the state on which $H(X|E_{\text{tot}})$ is computed is a classical-quantum state (see Eq. (38) in Methods). At the same time, the observed violation m can be expressed as:

$$m = \sum_\alpha p_\alpha m_\alpha. \tag{14}$$

In (13), the entropy $H(X|E)_{\rho_\alpha}$ is the conditional entropy of Alice's outcome given that Eve distributed the state ρ_α, while p_α is the probability distribution of the mixture prepared by Eve. In (14), m_α is the violation that the parties would observe had they shared the state ρ_α in every round of the protocol and performed the corresponding rank-one projective measurements.

We then aim at lower bounding $H(X|E)_{\rho_\alpha}$ with a convex function F of the MABK violation m_α:

$$H(X|E)_{\rho_\alpha} \geq F(m_\alpha). \tag{15}$$

By combining (13), (14), (15) and the convexity of F, one can obtain the desired lower bound on $H(X|E_{\text{tot}})$ as a function of the observed violation m:

$$H(X|E_{\text{tot}}) \geq F(m). \tag{16}$$

In the following we show in detail how to obtain the function F. In particular, we minimize the conditional entropy $H(X|E)_{\rho_\alpha}$ over all the states ρ_α of the form (5), whose MABK violation m_α achieved with rank-one projective measurements is upper bounded by (12).

The eigenvectors of the state ρ_α, correspondent to the eigenvalues in (6), read:

$$\begin{aligned} &|\rho_{ijk}\rangle = |\psi_{i,j,k}\rangle \quad (j,k) \neq (1,1) \\ &|\rho_{011}\rangle = \cos(\arctan q)\,|\psi_{0,1,1}\rangle - \mathbb{i}\sin(\arctan q)\,|\psi_{1,1,1}\rangle \\ &|\rho_{111}\rangle = \cos(\arctan q)\,|\psi_{1,1,1}\rangle - \mathbb{i}\sin(\arctan q)\,|\psi_{0,1,1}\rangle\,, \end{aligned} \tag{17}$$

where the parameter q is defined as:

$$q = \frac{2s}{\lambda_{011} - \lambda_{111} + \sqrt{(\lambda_{011} - \lambda_{111})^2 + 4s^2}}. \tag{18}$$

By combining the freedom in ordering the diagonal elements λ_{ijk} of ρ_α (c.f. Theorem 1) with the definition of the eigenvalues ρ_{ijk} in (6), one can impose the following constraints on the eigenvalues:

$$\rho_{0jk} \geq \rho_{1jk} \quad \forall j, k. \tag{19}$$

The entropy $H(X|E)_{\rho_\alpha}$ is computed on the classical-quantum state:

$$\rho_{XE}^\alpha = (\mathcal{E}_X \otimes \mathrm{id}_E)\,\mathrm{Tr}_{BC}[|\phi_{ABCE}^\alpha\rangle\langle\phi_{ABCE}^\alpha|], \tag{20}$$

where $|\phi_{ABCE}^\alpha\rangle$ is a purification of ρ_α (Eve holds the purifying system E), while $\mathcal{E}_X$ represents Alice's projective measurement defined by the following projectors:

$$|a\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a e^{\mathbb{i}\varphi}\,|1\rangle) \quad a \in \{0,1\}, \tag{21}$$

where $\varphi \in [0, 2\pi]$ identifies the measurement direction in the (x, y)-plane of the Bloch sphere. The entropy minimization is greatly simplified if, instead of minimizing over the matrix elements $\{\lambda_{ijk}\}$ and s of ρ_α, one minimizes over its eigenvalues $\{\rho_{ijk}\}$ and over q. Indeed, there exists a bijective map linking the two sets of parameters, defined by the relations (6) and (18). The remarkable

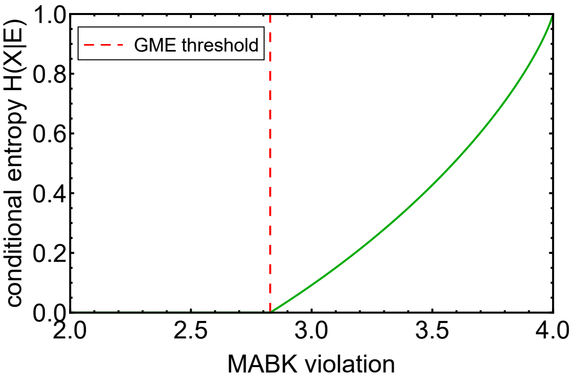

Figure 1. Tight analytical lower bound on the conditional entropy $H(X|E_{\text{tot}})$ as a function of the MABK inequality violation (Eq. (28)) observed by three parties. We notice that Eve has no uncertainty on Alice's outcome X for violations below the genuine multipartite entanglement (GME) threshold.

advantage of adopting the new variables $\{\rho_{ijk}\}$ and q, in the minimization of $H(X|E)_{\rho_\alpha}$, is that the MABK violation upper bound $\mathcal{M}_\alpha^\uparrow$ in (12) only depends on $\{\rho_{ijk}\}$. This allows us to first minimize the entropy over q and φ without affecting the MABK violation. In particular, one can easily verify that the entropy is minimized for $q = \varphi = 0$, by using the constraints (19). In other words, it is optimal for Eve to distribute a mixture of GHZ-diagonal states ($q = 0$ implies $s = 0$), similarly to the bipartite scenario studied in [33]. The resulting conditional entropy reads:

$$H(X|E)_{\rho_\alpha} = 1 - H(\{\rho_{ijk}\}) + H(\{\rho_{ijk} + \rho_{i\bar{j}\bar{k}}\}), \quad (22)$$

where the Shannon entropy of a probability distribution $\{p_i\}_i$ is defined as $H(\{p_i\}) = \sum_i -p_i \log_2 p_i$.

The final step consists in minimizing the entropy in (22) over $\{\rho_{ijk}\}$ and for a given violation m_α, with the constraint given by the MABK violation upper bound (12):

$$m_\alpha \leq \mathcal{M}_\alpha^\uparrow. \quad (23)$$

We perform this optimization analytically and provide the complete proof in section V of the Supplementary Information.

Importantly, we show that the minimal entropy is attained when equality holds in (23) and by the following family of states for every value of the violation m_α:

$$\tau(\nu_m) = \nu_m |\psi_{0,0,0}\rangle\langle\psi_{0,0,0}| + (1 - \nu_m)|\psi_{0,1,1}\rangle\langle\psi_{0,1,1}|. \quad (24)$$

The parameter ν_m is fixed by the violation m_α via (23) evaluated with the equals sign:

$$m_\alpha = \mathcal{M}_\tau^\uparrow(\nu_m) = 4\sqrt{2\nu_m^2 - 2\nu_m + 1}, \quad (25)$$

where we used (12) to compute the upper bound on the violation. The lower bound on the conditional entropy $H(X|E)_{\rho_\alpha}$ is thus given by the entropy of the states in (24):

$$H(X|E)_{\rho_\alpha} \geq F(m_\alpha) := H(X|E)_{\tau(\nu_m)} \quad (26)$$

The entropy of the states in (24) is easily computed from (22) and can be expressed in terms of the violation m_α by reverting (25). We obtain:

$$F(m_\alpha) = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{m_\alpha^2}{8} - 1}\right), \quad (27)$$

where $h(p) = -p \log_2 p - (1 - p)\log_2(1 - p)$ is the binary entropy. Finally, the lower bound (27) is a convex function, hence we can employ it in (16) and obtain the desired lower bound on $H(X|E_{\text{tot}})$ as a function of the observed MABK violation:

$$H(X|E_{\text{tot}}) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{m^2}{8} - 1}\right). \quad (28)$$

In figure 1, we plot the lower bound on the conditional entropy derived in (28), as a function of the observed violation of the MABK inequality. We notice that the minimized conditional entropy is zero for violations below the GME threshold of $2\sqrt{2}$. This means that GME is a necessary feature to guarantee private randomness of Alice's outcome in a tripartite MABK scenario.

Moreover, the lower bound on the conditional entropy in (28) is tight for any given observed violation. Indeed for every violation m, there exists a state $\tau(\nu_m)$ whose entropy coincides with the lower bound and that attains an MABK violation equal to m. As a matter of fact, the tightness conditions (75) of the MABK violation upper bound (12) (see Methods) are satisfied by the states $\tau(\nu_m)$, implying that $\mathcal{M}_\tau^\uparrow = \mathcal{M}_\tau$.

A lower bound on $H(X|E_{\text{tot}})$ as a function of the MABK inequality violation is also derived in [64], for the general N-party scenario. However, we emphasize that the bound in [64] is based on a completely different approach and with no allegation of optimality. The conditional entropy bound obtained in [64] reads:

$$H(X|E_{\text{tot}}) \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{m^2}{2^N} - 1}\right), \quad (29)$$

where m is the observed violation of the N-partite MABK inequality (9).

Surprisingly, the lower bound (29) for $N = 3$ coincides with the tight bound (28) obtained in this work. This observation proves the tightness of the bound (29) in the $N = 3$ case. We further verify that the bound (29) is actually tight for every number of parties N. In order to do so, we show that the bound (29) is attained by the following family of states that generalizes (24) to N-parties:

$$\tau(\nu) = \nu|\psi_{0,\vec{0}}\rangle\langle\psi_{0,\vec{0}}| + (1 - \nu)|\psi_{0,\vec{1}}\rangle\langle\psi_{0,\vec{1}}|. \quad (30)$$

In particular, by combining the conditional entropy and the maximal MABK violation of (30), similarly to what is done in the $N = 3$ case, we derive exactly the bound in (29). Note that the family of states (30) saturates (10), as they satisfy the tightness conditions of Theorem 2 given in Eqs. (IV.75) and (IV.80) of the Supplementary Information. In this way we prove that also (29) is a tight bound.

Finally, we remark that the tight entropy bound (29) is only defined for $m \geq 2^{N/2}$, that is only for violations above the GME threshold. Since private randomness of a party's outcome is a prerequisite of any DICKA protocol, it is an open question whether GME is a necessary ingredient for DICKA. Besides, in the next section we argue on the apparent incompatibility of full-correlator Bell inequalities and DICKA protocols.

Full-correlator Bell inequalities and DICKA

We provide an heuristic argument on why full-correlator Bell inequalities with two dichotomic observables per party, such as the MABK inequality, seem to be useless for DICKA protocols. We hope that this fundamental question can spark the interest of the community towards more conclusive results.

Any DICKA protocol is characterized by two essential ingredients: a violation of a multipartite Bell inequality to ensure secrecy of Alice's outcomes and correlated outcomes among all the parties yielding the conference key. Since a part of Alice's outcomes form the secret key, one of the measurements she uses to assess the violation of the inequality must be the same used for key generation [33, 42, 74]. Note that, unlike Alice, the other parties are equipped with an additional measurement option solely used for key generation.

It is known that every full-correlator Bell inequality with two dichotomic observables per party is maximally violated by the GHZ state [59]. Moreover, the only multiqubit state leading to perfectly correlated and random outcomes among all the parties is the GHZ state, when the parties measure in the Z basis [21].

However, a GHZ state maximally violates a full-correlator Bell inequality when the measurements are chosen such that the resulting inequality (modulo rearrangements) is only composed of expectation values of GHZ stabilizers, which acquire the extremal value 1. Moreover, the stabilizers appearing in the inequality do not act trivially on any qubit –i.e. do not contain the identity– due to the full-correlator structure of the inequality. We call such stabilizers "full-stabilizers" for ease of comprehension.

The problem is that none of the N-partite GHZ state full-stabilizers, for N odd, contains the Z operator [75]. This implies that, in order to maximally violate the inequality, Alice's measurement directions are orthogonal to Z. Since one of these measurements is also used to generate her raw key, she would obtain totally uncorrelated outcomes with the rest of the parties (perfect correlations are only obtained with a GHZ state when measuring Z). This causes the unwanted situation of having maximal violation and perfect correlations among the parties' key bits as mutually exclusive conditions. Since both conditions are required in a DICKA protocol, the above argument constitutes an initial evidence that full-correlator Bell inequalities are not suited for DICKA protocols.

A similar argument holds when the number of parties N is even ($N > 2$). As a matter of fact, in this case there exists only one GHZ full-stabilizer which contains the Z operator, namely: $Z^{\otimes N}$. If $\langle Z^{\otimes N}\rangle$ were to appear in the rearranged inequality expression, there should be at least another correlator containing at least one Z operator. Indeed, if each observable in a correlator never appears again in any other term of the inequality, that correlator is useless since Eve could assign to it any value (Eve is supposed to know the inequality being tested). The lack of any other full-stabilizer containing the Z operator prevents having a second correlator containing Z, thus excluding the term $\langle Z^{\otimes N}\rangle$ in the first place. Therefore, also in the N-even case Alice's measurements leading to maximal violation are orthogonal to Z, yielding uncorrelated raw key bits. We remark that the $N = 2$ case is peculiar since the low number of parties allows $\langle ZZ\rangle$ (obtained from the term $\langle A_1(B_0 - B_1)\rangle$ in the inequality) to appear just once in the CHSH inequality [58].

It is worth mentioning that in Ref. [74] the apparent incompatibility of the MABK inequality with a DICKA protocol was already discussed. In particular, it is shown in the tripartite case that there exists no honest implementation such that the parties' outcomes are perfectly correlated and at the same time the MABK inequality is violated above the GME threshold, which is a necessary condition as we pointed out above.

Despite the concerns on the use of MABK inequalities in DICKA protocols, the results of this paper are still of fundamental interest for DIRG [43–53] based on multiparty nonlocality. As a further application, in the following we improve the bound on Eve's uncertainty of Alice and Bob's outcomes derived in [49].

Joint conditional entropy bound

Consider the same DI scenario introduced in section "Tight conditional entropy bound", and suppose that Eve wishes to jointly guess the measurement outcomes X and Y of Alice and Bob, respectively. This scenario may occur in DIRG protocols where the parties are assumed to be co-located and collaborate to generate global secret randomness [49, 72]. We estimate Eve's uncertainty by providing a lower bound on the conditional von Neumann entropy $H(XY|E)_{\rho_\alpha}$, as a function of the MABK violation m_α. The entropy is computed on the following quantum state:

$$\rho^\alpha_{XYE} = (\mathcal{E}_X \otimes \mathcal{E}_Y \otimes \mathrm{id}_E)\,\mathrm{Tr}_C[|\phi^\alpha_{ABCE}\rangle\langle\phi^\alpha_{ABCE}|], \quad (31)$$

where the maps $\mathcal{E}_X$ and $\mathcal{E}_Y$ represent Alice's and Bob's measurements, respectively, defined by the following rank-one projectors:

$$|a\rangle_X = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a e^{\mathrm{i}\varphi_A}|1\rangle) \quad a \in \{0,1\}$$
$$|b\rangle_Y = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b e^{\mathrm{i}\varphi_B}|1\rangle) \quad b \in \{0,1\}. \tag{32}$$

The lower bound on $H(XY|E)_{\rho_\alpha}$ is derived by minimizing the entropy over the eigenvalues $\{\rho_{ijk}\}$ of ρ_α and over q given in (18), having upper bounded the observed MABK violation with (12), by employing the same arguments used for $H(X|E)_{\rho_\alpha}$.

We perform a fully-analytical optimization which is reported in section VI of the Supplementary Information. Notably, in analogy with the case of $H(X|E)_{\rho_\alpha}$, we verify that the entropy is minimized when $q = \varphi_A = \varphi_B = 0$, i.e. when ρ_α is a GHZ-diagonal state and both Alice and Bob measure in the X basis.

The analytical lower bound on $H(XY|E)_{\rho_\alpha}$ reads:

$$H(XY|E)_{\rho_\alpha} \geq G(m_\alpha), \tag{33}$$

where:

$$G(m_\alpha) := 2 - H\left(\{1-3f(m_\alpha), f(m_\alpha), f(m_\alpha), f(m_\alpha)\}\right), \tag{34}$$

and where the function f is defined as:

$$f(m_\alpha) = \frac{1}{4} - \frac{\sqrt{3}}{24}\sqrt{m_\alpha^2 - 4}. \tag{35}$$

Similarly to the case of $H(X|E)_{\rho_\alpha}$, we can exploit the convexity of the function in (34) to lower bound the conditional entropy of the global state prepared by Eve:

$$H(XY|E_{\mathrm{tot}}) \geq G(m), \tag{36}$$

where m is the violation observed by Alice, Bob and Charlie and $G(m)$ is the function defined in (34).

The bound in (36) is plotted in figure 2 (green line), together with the tight lower bound on the correspondent min-entropy obtained in [49] (magenta line).

We point out the dramatic improvement in certifying device-independently the privacy of Alice and Bob's outcomes with our lower bound on the conditional von Neumann entropy $H(XY|E_{\mathrm{tot}})$, as opposed to bounding the conditional min-entropy $H_{\min}(XY|E_{\mathrm{tot}})$.

The min-entropy is often used to lower bound the von-Neumann entropy in DI protocols, since it can be directly estimated using the statistics of the measurement outcomes [54–57]. In general it holds that $H \geq H_{\min}$ [76]. However, bounding the von Neumann entropy with the min-entropy can be far from optimal, as in the case analyzed here (see figure 2).

From figure 2, we also observe that the conditional entropy of the outcomes X and Y is nonzero for violations below the GME threshold unlike the entropy of Alice's outcome X (c.f. figure 1).

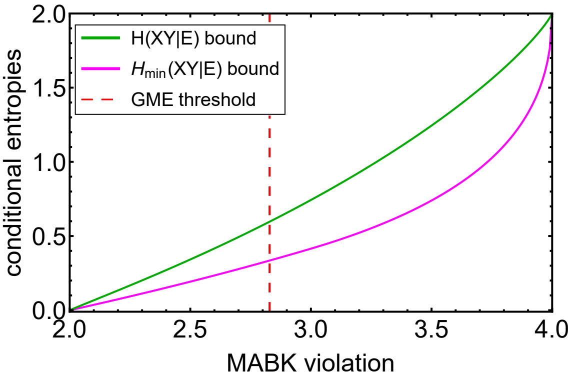

Figure 2. Analytical lower bound on the conditional von Neumann entropy $H(XY|E_{\mathrm{tot}})$ (green line, Eq. (36)) as a function of the MABK violation observed by three parties. We compare it to the lower bound on the conditional min-entropy $H_{\min}(XY|E_{\mathrm{tot}})$ derived in [49] (magenta line). Our bound dramatically improves the one in [49] since it directly bounds the von Neumann entropy. Unlike the case of $H(X|E_{\mathrm{tot}})$ in figure 1, Eve's uncertainty on Alice and Bob's outcomes is nonzero even for violations below the GME threshold.

Finally we remark that, differently from the bound on $H(X|E_{\mathrm{tot}})$ given in (28), we cannot infer the tightness of our analytical bound on $H(XY|E_{\mathrm{tot}})$. This is discussed in detail in section VI of the Supplementary Information.

DISCUSSION

The security of device-independent (DI) cryptographic protocols is based on the ability to bound the entropy of the protocols' outcomes, conditioned on the eavesdropper's knowledge, by a Bell inequality violation. To this aim, we considered a DI scenario where N parties test a generic full-correlator Bell inequality, with two measurement settings and two outcomes per party. We proved, in this context, that it is not restrictive to reduce the most general quantum state tested by the parties to a mixture of simple N-qubit states. Our result reduces to the only other one of this kind [33] when $N = 2$.

In order to obtain the entropic bounds, we proved an analytical upper bound on the maximal violation of the MABK inequality achieved by a given N-qubit state when the parties perform rank-one projective measurements. The bound is tight on certain classes of states and has general validity (i.e. independent of the parties' measurements) for states whose maximal violation is above the GME threshold. Our bound generalizes the known result [63] valid for the CHSH inequality to an arbitrary number of parties. To the best of our knowledge, this is the first bound on the maximal violation of a N-partite Bell inequality achievable by a given state, expressed in terms of the state's parameters.

These results enabled us to derive a tight analytical lower bound on the conditional von Neumann entropy of Alice's outcome, when Alice, Bob and Charlie test the tripartite MABK inequality. We also derived an analytical lower bound on the joint conditional von Neumann entropy of Alice and Bob's outcomes, which dramatically improves a similar estimation made in [49] in terms of the corresponding min-entropy. The improvement gained by directly bounding the von Neumann entropy has direct implications for randomness generation protocols, inasmuch as it increases the fraction of random bits guaranteed to be private.

Surprisingly, our tight lower bound on the conditional entropy of Alice's outcome coincides with an analogous one [64] inferred with a completely different methodology, namely exploiting a correspondence between the CHSH and the MABK inequality, and with no allegation of tightness. Moreover, we showed that the N-partite version of the bound in [64] is actually tight for arbitrary N.

We deduced that genuine multipartite entanglement (GME) is necessary to guarantee the privacy of Alice's random outcome in any device-independent scenario based on the MABK inequality. It is an open question whether GME is a fundamental requirement for DI conference key agreement (DICKA). In this regard, we heuristically argued that full-correlator Bell inequalities with two binary observables per party, such as the MABK inequality, are unlikely to be employed in any DICKA protocol. We envision further and more conclusive results in this direction from the scientific community interested in this topic.

The bounds on the conditional entropies derived in this work can find potential application in DI randomness generation based on multipartite nonlocality. Depending on the application, such protocols would generate local randomness for one party or global randomness for two or more parties. In all cases, the privacy of the generated random data would be ensured by entropic bounds like the ones we derived.

Furthermore, the techniques developed in proving Theorem 1 can inspire analogous analytical reductions of the quantum state for other Bell inequalities. Indeed, of particular interest are the Bell inequalities employed in the existing DICKA protocols [41, 42], for which a result like Theorem 1 would be the first step towards a tight security analysis, which is still lacking.

METHODS

Here we present the proofs of Theorem 1 and Theorem 2.

Proof of Theorem 1

The proof of Theorem 1 is based on three main ingredients: (i) the fact that each party has only two inputs with two outputs allows to reduce the analysis to qubits and rank-one projective measurements; (ii) the symmetries of the MABK inequality allow us to set all the marginals to zero, without changing the MABK violation or the information available to the eavesdropper; (iii) the freedom in the definition of the local axes is used to further reduce the number of free parameters. Our proof is inspired by a similar proof given in [33]. However, our result is valid for an arbitrary number of parties N in the generic $(N, 2, 2)$ DI scenario described in the main text. Notably, for $N = 2$ we recover the result of [33].

In order to prove Theorem 1, we make use of the following Lemma 1 which is a consequence of a result given in [77] and whose proof is reported in section I of the Supplementary Information.

Lemma 1. *Let $\{P_0, P_1\}$ and $\{Q_0, Q_1\}$ be two projective measurements acting on a Hilbert space $\mathcal{H}$, such that P_0, P_1, Q_0 and Q_1 are projectors and $P_0 + P_1 = \text{id}$ and $Q_0 + Q_1 = \text{id}$. There exists an orthonormal basis in an enlarged Hilbert space $\mathcal{H}^*$ such that the four projectors are simultaneously block diagonal, in blocks of size 2×2. Moreover, within a 2×2 block, each projector has rank one.*

Proof of Theorem 1. The first step consists in reducing the state distributed by Eve to a convex combination of N-qubit states. To start with, every generalized measurement (positive-operator valued measure) can be viewed as a projective measurement in a larger Hilbert space. Since we did not fix the Hilbert space to which the shared quantum state belongs, we can assume without loss of generality that the parties' measurements are binary projective measurements on a given Hilbert space $\mathcal{H}$. In particular, the projectors $P_0^{(i)}$ and $P_1^{(i)}$ ($Q_0^{(i)}$ and $Q_1^{(i)}$) correspond to Alice$_i$'s binary observable $A_0^{(i)}$ ($A_1^{(i)}$) relative to input $x_i = 0$ ($x_i = 1$).

Now we can apply Lemma 1 to the projective measurements of Alice$_i$ for $i = 1, \ldots, N$ and state that, at every round of the protocol, the Hilbert space on which e.g. Alice$_1$'s measurements are acting is decomposed as:

$$\mathcal{H}^* = \oplus_\alpha \mathcal{H}_\alpha^2 \ , \tag{37}$$

where every subspace $\mathcal{H}_\alpha^2$ is two-dimensional and both Alice$_1$'s measurements act within $\mathcal{H}_\alpha^2$ as rank-one projective measurements. From Alice$_1$'s point of view, the measurement process consists of a projection in one of the two-dimensional subspaces followed by a projective measurement in that subspace (selected according to Alice$_1$'s input). Therefore, Eve is effectively distributing to Alice$_1$ a direct sum of qubits at every round. Alice$_1$'s measurement then selects one of the qubit subspaces and performs a projective measurement within that subspace. Of course, since Eve fabricates the measurement device, the projective measurements occurring in every subspace can be predefined by Eve. Since this argument holds for every party, Eve is effectively distributing a direct sum of N-qubit states in each round.

Certainly, it cannot be worse for Eve to learn the flag α of the subspace selected in a particular round before sending the direct sum of N-qubit states to the parties. For this reason, we can reformulate the state preparation and measurement in a generic round of the protocol as Eve preparing a mixture

$$\rho_{A_1 \ldots A_N \Xi} = \textstyle\sum_\alpha p_\alpha \rho_\alpha \bigotimes_{i=1}^N |\alpha\rangle\langle\alpha|_{\xi_i} \tag{38}$$

of N-qubit states ρ_α, together with a set of ancillae $\Xi := \{\xi_i\}_{i=1}^N$ (known to her) which fixes the rank-one projective measurements that each party can select on ρ_α.

Let us now focus on one specific occurrence defined by a given α, i.e. on one of the N-qubit states ρ_α. For ease of notation, in the following we omit the symbol α.

We define the plane individuated by the two rank-one projective measurements of each party to be the (x, y)-plane of the Bloch sphere. Now, we assume without loss of generality that the statistics observed by the parties is such that every marginal is random:

$$\left\langle \prod_{i\in P} A^{(i)} \right\rangle = 0, \tag{39}$$

where $A^{(i)}$ is any dichotomic observable of Alice$_i$ and P is any non-empty strict subset of all the parties: $P \subsetneq \{1, \dots, N\}$. Indeed, if this is not the case, the parties can perform the following classical procedure on their outcomes which enforces the requirement in Eq. (39): "Alice$_1$ and Alice$_i$ flip their outcome with probability $1/2$", repeated for every $i = 2, \dots, N$. This procedure does not change the observed Bell violation since an even number of flips occurs at every time, thus leaving the correlators (1) composing the Bell inequality unchanged. Moreover, it requires classical communication between the parties which we assume to be known by Eve.

Since the observed statistics always satisfies (39), we can imagine that it is Eve herself who performs the classical flipping on the outputs in place of the parties. To this aim, Eve could apply the following map to the state ρ she prepared, before distributing it:

$$\rho \mapsto \bar\rho = \circ_{i=2}^{N} \mathcal{D}_i(\rho), \tag{40}$$

where the composition operator in (40) represents the successive application of the following operations

$$\mathcal{D}_i(\rho) = \frac{1}{2}\rho + \frac{1}{2} Z_1 Z_i \rho Z_1^\dagger Z_i^\dagger, \tag{41}$$

with Z_i representing the third Pauli operator applied on Alice$_i$'s qubit. Note that the application of Z prior to measurement flips the outcome of a measurement in the (x, y)-plane. Thus, by applying the map in (40), Eve is distributing a state which automatically satisfies the condition (39). We can safely assume that Eve implements the map in (40) since this is not disadvantageous to her. As a matter of fact, her uncertainty on the parties' outcomes, quantified by the conditional von Neumann entropy, does not increase when she sends the state $\bar\rho$ instead of ρ. We provide a detailed proof of this fact in section II of the Supplementary Information. Therefore, it is not restrictive to assume that the parties receive the state (40) from Eve, which can be recast as:

$$\bar\rho = \frac{1}{2^{N-1}} \sum_{n=0}^{\lfloor \frac{N}{2} \rfloor} \sum_{\mathbf{x}\in I(n)} Z^{\mathbf{x}} \rho Z^{\mathbf{x}}, \tag{42}$$

with

$$I(n) = \{\mathbf{x} \in \{0,1\}^N \, : \, \omega(\mathbf{x}) = 2n\}, \tag{43}$$

$$Z^{\mathbf{x}} = \bigotimes_{j=1}^{N} Z_j^{x_j}, \tag{44}$$

where the Hamming weight $\omega(\mathbf{x})$ of a bit string $\mathbf{x}$ returns the total number of bits that are equal to one and $\lfloor y \rfloor$ returns the greatest integer smaller or equal to y.

By expressing the initial generic state ρ in the GHZ basis:

$$\rho = \sum_{\vec u, \vec v \in \{0,1\}^{N-1}} \sum_{\sigma,\tau=0}^{1} \rho_{(\sigma\vec u)(\tau \vec v)} \left|\psi_{\sigma,\vec u}\right\rangle \left\langle \psi_{\tau,\vec v}\right|, \tag{45}$$

where $\rho_{(\sigma\vec u)(\tau\vec v)} \in \mathbb{C}$ and by substituting it into (42), we notice that the state $\bar\rho$ is greatly simplified in the GHZ basis. In particular, all the coherences between states of the GHZ basis relative to different vectors $\vec u$ are null:

$$\bar\rho = \sum_{\vec u \in \{0,1\}^{N-1}} \sum_{\sigma,\tau=0}^{1} \rho_{(\sigma\vec u)(\tau \vec v)} \left|\psi_{\sigma,\vec u}\right\rangle \left\langle \psi_{\tau,\vec u}\right|. \tag{46}$$

This means that the matrix representation of $\bar\rho$ is block-diagonal in the GHZ basis. By relabeling the non-zero matrix coefficients, we represent $\bar\rho$ as follows:

$$\bar\rho = \bigoplus_{\vec u \in \{0,1\}^{N-1}} \begin{bmatrix} \lambda_{0\vec u} & r_{\vec u} + \mathbb{i} s_{\vec u} \\ r_{\vec u} - \mathbb{i} s_{\vec u} & \lambda_{1\vec u} \end{bmatrix}, \tag{47}$$

where $\lambda_{j\vec u}, r_{\vec u}$ and $s_{\vec u}$ are real numbers. The number of free parameters characterizing (47) can be further reduced by exploiting the remaining degrees of freedom in the parties' local reference frames [33]. Indeed, although we identified the plane containing the measurement directions to be the (x, y)-plane for every party, they can still choose the orientation of the axes by applying rotations $R(\theta)$ along the z direction. Consequently, the state distributed by Eve without loss of generality is given by:

$$\bar\rho_+ = \bigotimes_{i=1}^{N} R_i(\theta_i)\, \bar\rho \bigotimes_{i=1}^{N} R_i^\dagger(\theta_i), \tag{48}$$

where the rotation $R_i(\theta_i)$ acts on the Hilbert space of party number i and reads:

$$R_i(\theta_i) = \cos\frac{\theta_i}{2} \mathrm{id} + \mathbb{i} \sin\frac{\theta_i}{2} Z_i, \tag{49}$$

where "id" is the identity operator. Similarly to $\bar\rho$, even the global rotation operator is block-diagonal in the GHZ basis:

$$\bigotimes_{i=1}^{N} R_i(\theta_i) = \bigoplus_{\vec u \in \{0,1\}^{N-1}} \begin{bmatrix} \cos\frac{\beta(\vec\theta,\vec u)}{2} & \mathbb{i}\sin\frac{\beta(\vec\theta,\vec u)}{2} \\ \mathbb{i}\sin\frac{\beta(\vec\theta,\vec u)}{2} & \cos\frac{\beta(\vec\theta,\vec u)}{2} \end{bmatrix}, \tag{50}$$

where $\vec\theta$ is the vector defined by the rotation angles $\{\theta_1, \dots, \theta_N\}$ and β is a function of $\vec\theta$ and $\vec u$ defined as:

$$\beta(\vec\theta, \vec u) = \theta_1 + \textstyle\sum_{j=1}^{N-1} (-1)^{u_j} \theta_{j+1}. \tag{51}$$

This fact greatly simplifies the calculation in (48), as it allows to multiply the matrices (47) and (50) block-by-block. The resulting block-diagonal matrix representing the state distributed by Eve reads:

$$\bar\rho_+ = \bigoplus_{\vec u \in \{0,1\}^{N-1}} \begin{bmatrix} \lambda'_{0\vec u} & r_{\vec u} + \mathbb{i} s'_{\vec u} \\ r_{\vec u} - \mathbb{i} s'_{\vec u} & \lambda'_{1\vec u} \end{bmatrix} \tag{52}$$

where the new matrix coefficients are given by:

$$\begin{aligned} \lambda'_{0\vec u} =& \frac{1}{2}\Big[\lambda_{0\vec u} + \lambda_{1\vec u} + (\lambda_{0\vec u} - \lambda_{1\vec u}) \cos\beta(\vec\theta,\vec u) \\ & + 2 s_{\vec u} \sin\beta(\vec\theta,\vec u)\Big] \end{aligned} \tag{53}$$

$$s'_{\vec u} = s_{\vec u} \cos\beta(\vec\theta,\vec u) - \frac{1}{2}(\lambda_{0\vec u} - \lambda_{1\vec u}) \sin\beta(\vec\theta,\vec u) \tag{54}$$

$$\begin{aligned} \lambda'_{1\vec u} =& \frac{1}{2}\Big[\lambda_{0\vec u} + \lambda_{1\vec u} - (\lambda_{0\vec u} - \lambda_{1\vec u}) \cos\beta(\vec\theta,\vec u) \\ & - 2 s_{\vec u} \sin\beta(\vec\theta,\vec u)\Big]. \end{aligned} \tag{55}$$

From (54) we deduce that choosing the rotation angles $\theta_1, \dots, \theta_N$ such that the following linear constraint is verified:

$$\theta_1 + \textstyle\sum_{j=1}^{N-1}(-1)^{u_j}\theta_{j+1} = \arctan \frac{2s_{\vec{u}}}{\lambda_{0\vec{u}} - \lambda_{1\vec{u}}}, \tag{56}$$

sets the corresponding imaginary part in (52) to zero: $s'_{\vec{u}} = 0$. However, we can only impose N constraints like (56) on the N rotation angles, thus we are able to arbitrarily set to zero N terms like $s_{\vec{u}}$ in (52). Moreover, by applying further rotations (note that the composition of rotations is still a rotation) such that:

$$\tilde{\theta}_1 + \textstyle\sum_{j=1}^{N-1}(-1)^{u_j}\tilde{\theta}_{j+1} = \pi, \tag{57}$$

we can exchange the diagonal terms in (52): $\lambda'_{0\vec{u}} = \lambda_{1\vec{u}}$ and $\lambda'_{1\vec{u}} = \lambda_{0\vec{u}}$. This allows us to arbitrarily order up to N pairs $(\lambda_{0\vec{u}}, \lambda_{1\vec{u}})$, for the same argument as above. Note that the blocks with ordered pairs are in general independent from the blocks with null imaginary parts. It is also possible to impose both conditions on the same block: applying (57) in (54) does not introduce a non-zero imaginary part $s'_{\vec{u}}$, if the imaginary part was previously set to zero ($s_{\vec{u}} = 0$) with (56).

Finally we construct the state $\bar{\rho}_-$ starting from $\bar{\rho}_+$ given in (52) by replacing $r_{\vec{u}}$ with $-r_{\vec{u}}$:

$$\bar{\rho}_- = \bigoplus_{\vec{u}\in\{0,1\}^{N-1}} \begin{bmatrix} \lambda'_{0\vec{u}} & -r_{\vec{u}} + \mathbb{i}s'_{\vec{u}} \\ -r_{\vec{u}} - \mathbb{i}s'_{\vec{u}} & \lambda'_{1\vec{u}} \end{bmatrix}. \tag{58}$$

We observe that the two states $\bar{\rho}_\pm$ yield the same measurement statistics and provide Eve with the same information –i.e. their conditional entropies coincide. Additionally, it is not disadvantageous for Eve to prepare a balanced mixture of $\bar{\rho}_+$ and $\bar{\rho}_-$ given by $(\bar{\rho}_+ + \bar{\rho}_-)/2$, rather than preparing one of the two states with certainty. A detailed proof of these observations is given in section III of the Supplementary Information.

We conclude that it is not restrictive to assume that Eve distributes to the parties a mixture of N-qubit states ρ_α together with an ancillary system fixing the parties' measurements. Each state ρ_α is represented by the following block diagonal matrix in the GHZ basis:

$$\rho_\alpha = \frac{\bar{\rho}_+ + \bar{\rho}_-}{2} = \bigoplus_{\vec{u}\in\{0,1\}^{N-1}} \begin{bmatrix} \lambda_{0\vec{u}} & \mathbb{i}s_{\vec{u}} \\ -\mathbb{i}s_{\vec{u}} & \lambda_{1\vec{u}} \end{bmatrix}, \tag{59}$$

where the diagonal elements of N arbitrary blocks are ordered and the off-diagonal elements of N blocks, chosen independently from the previous ones, are zero. This concludes the proof. □

Proof of Theorem 2

We present the proof of Theorem 2, which generalizes the analogous result valid in the bipartite case for the CHSH inequality [63]. This is, to the best of our knowledge, the only existing upper bound on the violation of the N-partite MABK inequality by rank-one projective measurements on an arbitrary N-qubit state, expressed as a function of the state's parameters. Note that an analogous upper bound on the violation of the tripartite MABK inequality was recently derived in [66]. However, here we show that our bound is tight on a broader class of states and valid for an arbitrary number of parties. In order to prove Theorem 2 we make use of the following Lemma 2, which generalizes an analogous result in [63] to rectangular matrices of arbitrary dimensions. The proof of Lemma 2 is reported in section IV of the Supplementary Information.

Lemma 2. *Let Q be an $m \times n$ real matrix and let $\|\vec{v}\|$ be the Euclidean norm of vectors $\vec{v} \in \mathbb{R}^k$, for $k = m, n$. Finally, let "$\cdot$" indicate both the scalar product and the matrix-vector multiplication. Then*

$$\max_{\substack{\vec{c}\perp\vec{c}\,'\ \text{s.t.} \\ \|\vec{c}\|=\|\vec{c}\,'\|=1}} \left[\|Q\cdot\vec{c}\|^2 + \|Q\cdot\vec{c}\,'\|^2\right] = u_1 + u_2\ , \tag{60}$$

where u_1 and u_2 are the largest and second-to-the-largest eigenvalues of $U \equiv Q^TQ$, respectively.

For illustration purposes, here we report the proof of Theorem 2 for the case of $N = 3$ parties. The full proof is given in section IV of the Supplementary Information.

Proof of Theorem 2 for $N = 3$. By assumption we restrict the description of the parties' observables to rank-one projective measurements on their respective qubit [59]. Hence they can be represented as follows:

$$A_x = \vec{a}_x \cdot \vec{\sigma},\ B_y = \vec{b}_y \cdot \vec{\sigma},\ \text{and}\ C_z = \vec{c}_z \cdot \vec{\sigma}, \tag{61}$$

where $\vec{a}_x, \vec{b}_y, \vec{c}_z$ are unit vectors in $\mathbb{R}^3$ and where $\sigma_1 = X, \sigma_2 = Y$ and $\sigma_3 = Z$. We can then express the tripartite MABK operator (8) as follows:

$$M_3 = \sum_{i,j,k=1}^{3} M_{ijk}\sigma_i \otimes \sigma_j \otimes \sigma_k, \tag{62}$$

where we defined

$$M_{ijk} \equiv a_{0i}b_{0j}c_{1k} + a_{0i}b_{1j}c_{0k} + a_{1i}b_{0j}c_{0k} - a_{1i}b_{1j}c_{1k}. \tag{63}$$

A generic 3-qubit state can be expressed in the Pauli basis as follows

$$\rho = \frac{1}{8}\sum_{\mu,\nu,\gamma=0}^{3} \Lambda_{\mu\nu\gamma}\sigma_\mu \otimes \sigma_\nu \otimes \sigma_\gamma, \tag{64}$$

with $\Lambda_{\mu\nu\gamma} = \mathrm{Tr}[\rho\sigma_\mu \otimes \sigma_\nu \otimes \sigma_\gamma]$ and $\sigma_0 = \mathrm{id}$. With the MABK operator in (62), the MABK expectation value on the generic 3-qubit state in (64) is given by:

$$\begin{aligned} \langle M_3 \rangle_\rho &= \mathrm{Tr}(M_3\rho) \\ &= \frac{1}{8}\sum_{i,j,k=1}^{3}\sum_{\mu,\nu,\gamma=0}^{3} M_{ijk}\Lambda_{\mu\nu\gamma}\underbrace{\mathrm{Tr}\left(\sigma_i\sigma_\mu \otimes \sigma_j\sigma_\nu \otimes \sigma_k\sigma_\gamma\right)}_{8\delta_{i,\mu}\delta_{j,\nu}\delta_{k,\gamma}} \\ &= \sum_{i,j,k=1}^{3} M_{ijk}\Lambda_{ijk}. \end{aligned} \tag{65}$$

By recalling the correlation matrix of a tripartite state (c.f. Definition 3), the MABK expectation value in (65) can be recast as follows:

$$\begin{aligned} \langle M_3 \rangle_\rho = &\left(\vec{a}_0 \otimes \vec{b}_1 + \vec{a}_1 \otimes \vec{b}_0\right)^T \cdot T_\rho \cdot \vec{c}_0 \\ &+ \left(\vec{a}_0 \otimes \vec{b}_0 - \vec{a}_1 \otimes \vec{b}_1\right)^T \cdot T_\rho \cdot \vec{c}_1. \end{aligned} \tag{66}$$

Finally, the maximum violation $\mathcal{M}_\rho$ of the MABK inequality achieved by an arbitrary 3-qubit state is obtained by optimizing (66) over all possible observables that the parties can choose to measure:

$$\mathcal{M}_\rho = \max_{\substack{\vec{a}_i,\vec{b}_i,\vec{c}_i \text{ s.t.}\\ \|\vec{a}_i\|=\|\vec{b}_i\|=\|\vec{c}_i\|=1}} (\vec{a}_0\otimes\vec{b}_1+\vec{a}_1\otimes\vec{b}_0)^T\cdot T_\rho\cdot\vec{c}_0 + (\vec{a}_0\otimes\vec{b}_0-\vec{a}_1\otimes\vec{b}_1)^T\cdot T_\rho\cdot\vec{c}_1. \tag{67}$$

Let us now evaluate the norm of the composite vectors in (67):

$$\begin{aligned}\left\|\vec{a}_0\otimes\vec{b}_1+\vec{a}_1\otimes\vec{b}_0\right\|^2 &= 2+2\underbrace{\cos\theta_a\cos\theta_b}_{\equiv\cos\theta_{ab}} \\ &= 4\cos^2\left(\frac{\theta_{ab}}{2}\right) ,\end{aligned} \tag{68}$$

where θ_a (θ_b) is the angle between vectors $\vec{a}_0$ and $\vec{a}_1$ ($\vec{b}_0$ and $\vec{b}_1$). Similarly,

$$\left\|\vec{a}_0\otimes\vec{b}_0-\vec{a}_1\otimes\vec{b}_1\right\|^2 = 4\sin^2\left(\frac{\theta_{ab}}{2}\right). \tag{69}$$

We then define normalized vectors $\vec{v}_0$ and $\vec{v}_1$ such that

$$\vec{a}_0\otimes\vec{b}_1+\vec{a}_1\otimes\vec{b}_0 = 2\cos\left(\frac{\theta_{ab}}{2}\right)\vec{v}_0, \tag{70}$$

$$\vec{a}_0\otimes\vec{b}_0-\vec{a}_1\otimes\vec{b}_1 = 2\sin\left(\frac{\theta_{ab}}{2}\right)\vec{v}_1. \tag{71}$$

It can be easily checked that the normalized vectors $\vec{v}_0$ and $\vec{v}_1$ are orthogonal. By substituting the definitions (70) and (71) into the maximal violation of the MABK inequality (67), we can upper bound the latter as follows:

$$\mathcal{M}_\rho \leq \max_{\substack{\vec{c}_i,\vec{v}_i,\theta_{ab} \text{ s.t.}\\ \|\vec{c}_i\|=\|\vec{v}_i\|=1\,\wedge\,\vec{v}_0\perp\vec{v}_1}} 2\cos\left(\frac{\theta_{ab}}{2}\right)\vec{v}_0^T\cdot T_\rho\cdot\vec{c}_0 + 2\sin\left(\frac{\theta_{ab}}{2}\right)\vec{v}_1^T\cdot T_\rho\cdot\vec{c}_1. \tag{72}$$

The inequality in (72) is due to the fact that now the optimization is over arbitrary orthonormal vectors $\vec{v}_0,\vec{v}_1$ and angle θ_{ab}, while originally the optimization was over variables satisfying the structure imposed by (70) and (71). We now simplify the r.h.s. of (72) to obtain the theorem claim. In particular, we optimize over the unit vectors $\vec{c}_0$ and $\vec{c}_1$ by choosing them in the directions of $T_\rho^T\cdot\vec{v}_0$ and $T_\rho^T\cdot\vec{v}_1$, respectively, and we also optimize over θ_{ab} by exploiting the fact that the general expression $A\,\cos\theta + B\,\sin\theta$ is maximized to $\sqrt{A^2+B^2}$ for $\theta = \arctan B/A$:

$$\begin{aligned}\mathcal{M}_\rho &\leq \max_{\substack{\vec{v}_i,\theta_{ab} \text{ s.t.}\\ \|\vec{v}_i\|=1\,\wedge\,\vec{v}_0\perp\vec{v}_1}} 2\left[\cos\left(\frac{\theta_{ab}}{2}\right)\left\|T_\rho^T\cdot\vec{v}_0\right\| + \sin\left(\frac{\theta_{ab}}{2}\right)\left\|T_\rho^T\cdot\vec{v}_1\right\|\right] \\ &= \max_{\substack{\vec{v}_i \text{ s.t.}\\ \|\vec{v}_i\|=1\,\wedge\,\vec{v}_0\perp\vec{v}_1}} 2\sqrt{\left\|T_\rho^T\cdot\vec{v}_0\right\|^2+\left\|T_\rho^T\cdot\vec{v}_1\right\|^2}.\end{aligned} \tag{73}$$

Finally, by applying the result of Lemma 2, we know that the maximum in (73) is achieved when $\vec{v}_0$ and $\vec{v}_1$ are chosen in the direction of the eigenstates of $T_\rho T_\rho^T$ corresponding to the two largest eigenvalues. This concludes the proof for the $N=3$ case:

$$\mathcal{M}_\rho \leq 2\sqrt{t_0+t_1}\ , \tag{74}$$

where t_0 and t_1 are the two largest eigenvalues of $T_\rho T_\rho^T$. □

Tightness conditions: The bound (10) is tight if the correlation matrix T_ρ of the considered state satisfies certain conditions, i.e. for certain classes of states. Here we report the tightness conditions valid in the $N=3$ case, while the ones for general N and their derivation are given in section IV of the Supplementary Information.

The upper bound (10) on the maximal violation of the tripartite MABK inequality by a given state ρ is tight, that is there exists an honest implementation achieving the bound, if there exist unit vectors $\vec{a}_0,\vec{a}_1,\vec{b}_0$ and $\vec{b}_1$ such that the following identities are satisfied:

$$\begin{aligned}\vec{a}_0\otimes\vec{b}_1+\vec{a}_1\otimes\vec{b}_0 &= 2\sqrt{\frac{t_0}{t_0+t_1}}\,\vec{t}_0 \\ \vec{a}_0\otimes\vec{b}_0-\vec{a}_1\otimes\vec{b}_1 &= 2\sqrt{\frac{t_1}{t_0+t_1}}\,\vec{t}_1,\end{aligned} \tag{75}$$

where $\vec{t}_0$ and $\vec{t}_1$ are the normalized eigenvectors of $T_\rho T_\rho^T$ corresponding to the two largest eigenvalues t_0 and t_1.

It is interesting to compare the tightness of our bound with the bound derived in [66]. The major difference is that our bound can be saturated even when the matrix $T_\rho T_\rho^T$ has no degenerate eigenvalues, opposed to [66] which requires the degeneracy of the largest eigenvalue of $T_\rho T_\rho^T$. When the matrix $T_\rho T_\rho^T$ is degenerate in its largest eigenvalue (i.e. $t_0 = t_1$), we recover the same tightness conditions of [66]. For this reason, our bound is tight on a larger set of states compared to the bound in [66].

DATA AVAILABILITY

No datasets were generated or analysed during the current study.

ACKNOWLEDGEMENTS

We thank Timo Holz and Flavien Hirsch for helpful discussions. This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1 - 390534769, by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675662, and by the Federal Ministry of Education and Research BMBF (Project Q.Link.X and HQS).

AUTHOR CONTRIBUTIONS

HK, GM and DB triggered the consideration of the project. FG and GM developed the project. FG produced most of the analytical proofs and wrote the manuscript. HK and GM provided valuable help in some of the proofs. All the authors contributed in discussing the results and reviewing the manuscript.

COMPETING INTERESTS STATEMENT

The authors declare no competing interests.

[1] E. Commission, “The quantum flagship.” `https://qt.eu`. [Online].

[2] I. Q. Technology, “Quantum key distribution (qkd) markets: 2019-2028.” `https://www.insidequantumtechnology.com/product/quantum-key-distribution-qkd-markets-2019-2028`. [Online].

[3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175 – 179, 1984.

[4] D. Bruß, “Optimal eavesdropping in quantum cryptography with six states,” *Phys. Rev. Lett.*, vol. 81, pp. 3018–3021, Oct 1998.

[5] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[6] R. Renner, “Security of quantum key distribution,” *International Journal of Quantum Information*, vol. 06, no. 01, pp. 1–127, 2008.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[8] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, pp. 595–604, 2014.

[9] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” *npj Quantum Information*, vol. 2, no. 1, p. 16025, 2016.

[10] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography,” 2019. arXiv:quant-ph/1906.01645.

[11] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, “Quantum random number generation,” *npj Quantum Information*, vol. 2, no. 1, p. 16021, 2016.

[12] M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” *Rev. Mod. Phys.*, vol. 89, p. 015004, Feb 2017.

[13] M. Epping, H. Kampermann, and D. Bruß, “Large-scale quantum networks based on graphs,” *New Journal of Physics*, vol. 18, p. 053036, may 2016.

[14] M. Epping, H. Kampermann, and D. Bruß, “Robust entanglement distribution via quantum network coding,” *New Journal of Physics*, vol. 18, p. 103052, oct 2016.

[15] A. Pirker, J. Wallnöfer, and W. Dür, “Modular architectures for quantum networks,” *New Journal of Physics*, vol. 20, p. 053054, may 2018.

[16] F. Hahn, A. Pappa, and J. Eisert, “Quantum network routing and local complementation,” *npj Quantum Information*, vol. 5, no. 1, p. 76, 2019.

[17] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, “Light-matter entanglement over 50 km of optical fibre,” *npj Quantum Information*, vol. 5, no. 1, p. 72, 2019.

[18] A. Tchebotareva, S. L. N. Hermans, P. C. Humphreys, D. Voigt, P. J. Harmsma, L. K. Cheng, A. L. Verlaan, N. Dijkhuizen, W. de Jong, A. Dréau, and R. Hanson, “Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength,” *Phys. Rev. Lett.*, vol. 123, p. 063601, Aug 2019.

[19] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, “Satellite-relayed intercontinental quantum network,” *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018.

[20] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, 2018.

[21] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, “Multi-partite entanglement can speed up quantum key distribution in networks,” *New Journal of Physics*, vol. 19, p. 093012, sep 2017.

[22] F. Grasselli, H. Kampermann, and D. Bruß, “Finite-key effects in multipartite quantum key distribution protocols,” *New Journal of Physics*, vol. 20, p. 113014, nov 2018.

[23] F. Grasselli, H. Kampermann, and D. Bruß, “Conference key agreement with single-photon interference,” *New Journal of Physics*, vol. 21, p. 123002, dec 2019.

[24] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, “Continuous-variable measurement-device-independent multipartite quantum communication,” *Phys. Rev. A*, vol. 93, p. 022325, Feb 2016.

[25] Z. Zhang, R. Shi, and Y. Guo, “Multipartite continuous variable quantum conferencing network with entanglement in the middle,” *Applied Sciences*, vol. 8, no. 8, 2018.

[26] R. L. C. Ottaviani, C. Lupo and S. Pirandola, “Modular network for high-rate quantum conferencing,” *Communications Physics*, vol. 2, no. 118, 2019.

[27] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, “Quantum conference key agreement: A review,” 2020. arXiv:quant-ph/2003.10186.

[28] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, “Experimental quantum conference key agreement,” 2020. arXiv:quant-ph/2002.01491.

[29] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics.* Cambridge University Press, 2004.

[30] A. Yao and D. Mayers, "Quantum cryptography with imperfect apparatus," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, (Los Alamitos, CA, USA), p. 503, IEEE Computer Society, nov 1998.

[31] A. Acín, N. Gisin, and L. Masanes, "From bell's theorem to secure quantum key distribution," *Phys. Rev. Lett.*, vol. 97, p. 120405, Sep 2006.

[32] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun 2007.

[33] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, p. 045021, apr 2009.

[34] L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nature Communications*, vol. 2, no. 1, p. 238, 2011.

[35] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, p. 140501, Sep 2014.

[36] S. Pironio, L. Masanes, A. Leverrier, and A. Acín, "Security of device-independent quantum key distribution in the bounded-quantum-storage model," *Phys. Rev. X*, vol. 3, p. 031007, Aug 2013.

[37] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature Communications*, vol. 9, no. 1, p. 459, 2018.

[38] T. Holz, H. Kampermann, and D. Bruß, "Device-independent secret-key-rate analysis for quantum repeaters," *Phys. Rev. A*, vol. 97, p. 012337, Jan 2018.

[39] V. Scarani and N. Gisin, "Quantum communication between n partners and bell's inequalities," *Phys. Rev. Lett.*, vol. 87, p. 117901, Aug 2001.

[40] V. Scarani and N. Gisin, "Quantum key distribution between n partners: Optimal eavesdropping and bell's inequalities," *Phys. Rev. A*, vol. 65, p. 012311, Dec 2001.

[41] J. Ribeiro, G. Murta, and S. Wehner, "Reply to "comment on 'fully device-independent conference key agreement' "," *Phys. Rev. A*, vol. 100, p. 026302, Aug 2019.

[42] T. Holz, H. Kampermann, and D. Bruß, "A genuine multipartite bell inequality for device-independent conference key agreement," 2019. arXiv:quant-ph/1910.11360.

[43] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," 2007. PhD thesis, University of Cambridge. Also available at: arXiv:quant-ph/0911.3814.

[44] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[45] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *Journal of Physics A: Mathematical and Theoretical*, vol. 44, p. 095305, feb 2011.

[46] U. Vazirani and T. Vidick, "Certifiable quantum dice," 2012.

[47] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio, "Device-independent randomness generation from several bell estimators," *New Journal of Physics*, vol. 20, p. 023049, feb 2018.

[48] M. Coudron, J. Stark, and T. Vidick, "Trading locality for time: certifiable randomness from low-depth circuits," 2018. quant-ph/1810.04233.

[49] E. Woodhead, B. Bourdoncle, and A. Acín, "Randomness versus nonlocality in the Mermin-Bell experiment with three parties," *Quantum*, vol. 2, p. 82, Aug. 2018.

[50] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices," *J. ACM*, vol. 63, Oct. 2016.

[51] S. Pironio and S. Massar, "Security of practical private randomness generation," *Phys. Rev. A*, vol. 87, p. 012336, Jan 2013.

[52] S. Fehr, R. Gelles, and C. Schaffner, "Security and composability of randomness expansion from bell inequalities," *Phys. Rev. A*, vol. 87, p. 012335, Jan 2013.

[53] R. Ramanathan, F. G. S. L. Brandão, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka, "Randomness amplification under minimal fundamental assumptions on the devices," *Phys. Rev. Lett.*, vol. 117, p. 230501, Nov 2016.

[54] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," *Phys. Rev. Lett.*, vol. 98, p. 010401, Jan 2007.

[55] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New Journal of Physics*, vol. 10, p. 073013, jul 2008.

[56] O. Nieto-Silleras, S. Pironio, and J. Silman, "Using complete measurement statistics for optimal device-independent randomness evaluation," *New Journal of Physics*, vol. 16, p. 013035, jan 2014.

[57] J.-D. Bancal, L. Sheridan, and V. Scarani, "More randomness from the same data," *New Journal of Physics*, vol. 16, p. 033011, mar 2014.

[58] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.

[59] R. F. Werner and M. M. Wolf, "All-multipartite bell-correlation inequalities for two dichotomic observables per site," *Phys. Rev. A*, vol. 64, p. 032112, Aug 2001.

[60] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states," *Phys. Rev. Lett.*, vol. 65, pp. 1838–1840, Oct 1990.

[61] M. Ardehali, "Bell inequalities with a magnitude of violation that grows exponentially with the number of particles," *Phys. Rev. A*, vol. 46, pp. 5375–5378, Nov 1992.

[62] A. V. Belinskiĭ and D. N. Klyshko, "Interference of light and bell's theorem," *Phys. Rev. A*, vol. 36, pp. 653–693, 1993.

[63] R. Horodecki, P. Horodecki, and M. Horodecki, "Violating bell inequality by mixed spin-12 states: necessary and sufficient condition," *Physics Letters A*, vol. 200, no. 5, pp. 340 – 344, 1995.

[64] J. Ribeiro, G. Murta, and S. Wehner, "Fully device-independent conference key agreement," *Phys. Rev. A*, vol. 97, p. 022307, Feb 2018.

[65] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, "Bell-type inequalities to detect true n-body nonseparability," *Phys. Rev. Lett.*, vol. 88, p. 170405, Apr 2002.

[66] M. A. Siddiqui and S. Sazim, "Tight upper bound for the maximal expectation value of the mermin operators," *Quantum Information Processing*, vol. 18, p. 131, Mar 2019.

[67] T. Vértesi and E. Bene, “Two-qubit bell inequality for which positive operator-valued measurements are relevant,” *Phys. Rev. A*, vol. 82, p. 062115, Dec 2010.

[68] Y.-C. Liang and A. C. Doherty, “Bounds on quantum correlations in bell-inequality experiments,” *Phys. Rev. A*, vol. 75, p. 042103, Apr 2007.

[69] M. Zukowski and C. Brukner, “Bell’s theorem for general n-qubit states,” *Phys. Rev. Lett.*, vol. 88, p. 210401, May 2002.

[70] W. Laskowski, T. Paterek, M. Żukowski, and i. c. v. Brukner, “Tight multipartite bell’s inequalities involving many measurement settings,” *Phys. Rev. Lett.*, vol. 93, p. 200401, Nov 2004.

[71] M. Li and S.-M. Fei, “Bell inequalities for multipartite qubit quantum systems and their maximal violation,” *Phys. Rev. A*, vol. 86, p. 052119, Nov 2012.

[72] F. Dupuis and O. Fawzi, “Entropy accumulation with improved second-order term,” *IEEE Transactions on Information Theory*, vol. 65, pp. 7596–7612, Nov 2019.

[73] P. J. Brown, S. Ragy, and R. Colbeck, “A framework for quantum-secure device-independent randomness expansion,” *IEEE Transactions on Information Theory*, vol. 66, no. 5, pp. 2964–2987, 2020.

[74] T. Holz, D. Miller, H. Kampermann, and D. Bruß, “Comment on “fully device-independent conference key agreement”,” *Phys. Rev. A*, vol. 100, p. 026301, Aug 2019.

[75] G. Tóth and O. Gühne, “Entanglement detection in the stabilizer formalism,” *Phys. Rev. A*, vol. 72, p. 022340, Aug 2005.

[76] M. Tomamichel, R. Colbeck, and R. Renner, “A fully quantum asymptotic equipartition property,” *IEEE Transactions on Information Theory*, vol. 55, pp. 5840–5847, Dec 2009.

[77] L. Masanes, “Asymptotic violation of bell inequalities and distillability,” *Phys. Rev. Lett.*, vol. 97, p. 050503, Aug 2006.

[78] W. Karush, “Minima of functions of several variables with inequalities as side conditions,” 1939.

[79] H. W. Kuhn and A. W. Tucker, “Nonlinear programming,” in *Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability*, (Berkeley, Calif.), pp. 481–492, University of California Press, 1951.

Supplementary Information

Federico Grasselli[1], *Gláucia Murta*[2], *Hermann Kampermann and Dagmar Bruß*
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany

I. REDUCTION TO QUBITS AND RANK-ONE PROJECTIVE MEASUREMENTS

We now provide a detailed proof of Lemma 1 which is a consequence of a result proved in Ref. [77].

Lemma 1. *Let* $\{P_0, P_1\}$ *and* $\{Q_0, Q_1\}$ *be two projective measurements acting on a Hilbert space* $\mathcal{H}$*, such that* P_0, P_1, Q_0 *and* Q_1 *are projectors,* $P_0 + P_1 = \mathrm{id}$ *and* $Q_0 + Q_1 = \mathrm{id}$*. There exists an orthonormal basis in an enlarged Hilbert space* $\mathcal{H}^*$ *such that the four projectors are simultaneously block diagonal, in blocks of size* 2×2*. Moreover, within a* 2×2 *block, each projector has rank one.*

Proof. Let us consider the following three positive operators P_0, $P_0Q_0P_0$ and $P_0Q_1P_0$. One can check that they commute and therefore can be simultaneously diagonalized. Let $|v\rangle$ be one of their simultaneous eigenvector. Since $P_1 \cdot P_0 = 0$, then $P_1 |v\rangle = 0$. So $|v\rangle$ is also an eigenvector of P_1 with eigenvalue zero. Now, because $Q_0 + Q_1 = I$, we cannot have that $Q_0 |v\rangle = 0$ and $Q_1 |v\rangle = 0$. Therefore one of the following cases hold:

- If $Q_0 |v\rangle = 0$: then $Q_1 |v\rangle = |v\rangle$, and the span of $|v\rangle$ corresponds to a 1×1 block in which P_0, P_1, Q_0, Q_1 have $|v\rangle$ as a common eigenvector with respective eigenvalues $1, 0, 0, 1$.
- If $Q_1 |v\rangle = 0$: then similarly we have a 1×1 block in which P_0, P_1, Q_0, Q_1 have $|v\rangle$ as a common eigenvector with respective eigenvalues $1, 0, 1, 0$.
- If $Q_0 |v\rangle \neq 0$ and $Q_1 |v\rangle \neq 0$: then we define the orthogonal vectors $|u_0\rangle = Q_0 |v\rangle$ and $|u_1\rangle = Q_1 |v\rangle$ and the 2-dimensional subspace $E_v = \{c_0 |u_0\rangle + c_1 |u_1\rangle : c_0, c_1 \in \mathbb{C}\}$. We have that $|v\rangle \in E_v$ since $|v\rangle = |u_0\rangle + |u_1\rangle$. Because $|v\rangle$ is also an eigenvector of $P_0Q_0P_0$ and $P_0Q_1P_0$, then $P_0 |u_0\rangle = P_0Q_0 |v\rangle = P_0Q_0P_0 |v\rangle \propto |v\rangle$, similarly $P_0 |u_1\rangle \propto |v\rangle$. Therefore, $\exists\, |w\rangle \in E_v$ such that $P_0 |w\rangle = 0$ and then $P_1 |w\rangle = |w\rangle$. So the vectors $|u_0\rangle, |u_1\rangle \in E_v$ are simultaneous eigenvectors of Q_0 and Q_1, and the vectors $|v\rangle, |w\rangle \in E_v$ are simultaneous eigenvectors of P_0 and P_1. And the subspace E_v corresponds to a 2×2 simultaneous diagonal block for the measurements operators P_0, P_1, Q_0, Q_1.

This procedure can be performed on all the simultaneous eigenvectors of P_0, $P_0Q_0P_0$ and $P_0Q_1P_0$, and similarly on the remaining simultaneous eigenvectors of P_1, $P_1Q_0P_1$ and $P_1Q_1P_1$.

Now, if we restrict to a 2×2 subspace E_v with Π_v being the projector on the subspace E_v, the projectors $\Pi_v P_0 \Pi_v, \Pi_v P_1 \Pi_v, \Pi_v Q_0 \Pi_v, \Pi_v Q_1 \Pi_v$ are given by

$$\begin{aligned} \Pi_v P_0 \Pi_v &= \frac{|v\rangle\langle v|}{\langle v|v\rangle} \\ \Pi_v P_1 \Pi_v &= \frac{|w\rangle\langle w|}{\langle w|w\rangle} \\ \Pi_v Q_0 \Pi_v &= \frac{|u_0\rangle\langle u_0|}{\langle u_0|u_0\rangle} \\ \Pi_v Q_1 \Pi_v &= \frac{|u_1\rangle\langle u_1|}{\langle u_1|u_1\rangle} \end{aligned} \tag{I.76}$$

i.e., they are all rank-one projectors.

Within a 1×1 block, the two measurements defined by $\{P_0, P_1\}$ and $\{Q_0, Q_1\}$ have fixed outputs. Let $|\tilde{v}\rangle$ be a normalized simultaneous eigenvector of P_0, $P_0Q_0P_0$ and $P_0Q_1P_0$ and consider the case $Q_0 |\tilde{v}\rangle = 0$, which leads to a block of size 1×1 formed by the span of the vector $|\tilde{v}\rangle$. We can now artificially enlarge the system dimension by

[1] corresponding author: federico.grasselli@hhu.de

[2] corresponding author: glaucia.murta@hhu.de

embedding this block into a block of size 2 × 2. Let $|\tilde{w}\rangle\langle\tilde{w}|$ be a projector on the extra artificial dimension, with $|\tilde{w}\rangle$ a normalized vector. Then we can define the two-dimensional subspace $E_{\tilde{v}} = \{c_0 |\tilde{v}\rangle + c_1 |\tilde{w}\rangle : c_0, c_1 \in \mathbb{C}\}$, and we define the projectors within this subspace to be given by: $\Pi_{\tilde{v}} P_0 \Pi_{\tilde{v}} = |\tilde{v}\rangle\langle\tilde{v}|$, $\Pi_{\tilde{v}} P_1 \Pi_{\tilde{v}} = |\tilde{w}\rangle\langle\tilde{w}|$, $\Pi_{\tilde{v}} Q_0 \Pi_{\tilde{v}} = |\tilde{w}\rangle\langle\tilde{w}|$, and $\Pi_v Q_1 \Pi_v = |\tilde{v}\rangle\langle\tilde{v}|$. One can perform a similar embedding for the other case that leads to a 1 × 1 block, that is $Q_1 |\tilde{v}\rangle = 0$. Note that the new projective measurements defined on $\mathcal{H}^*$, when applied to a quantum state ρ on $\mathcal{H}$ that has no components in the artificial dimensions, have still fixed outcomes in the enlarged subspaces like $E_{\tilde{v}}$.

With this artificial construction, the representation of the four projectors P_0, P_1, Q_0 and Q_1 in the artificially enlarged Hilbert space $\mathcal{H}^*$ is only composed of 2 × 2 diagonal blocks. Moreover, if we restrict to one of these blocks, the two measurements defined by $\{P_0, P_1\}$ and $\{Q_0, Q_1\}$ are rank-one projective measurements. □

II. EVE'S UNCERTAINTY IS NON-INCREASING UNDER SYMMETRIZATION OF THE OUTCOMES

In proving Theorem 1, we argue that all the marginals are random (39) without loss of generality. This can be enforced by assuming that Eve flips the classical outcomes of the measurements in specific combinations. Otherwise, Eve could also provide the parties with a state that inherently leads to the symmetrized marginals, which is the mixture $\bar{\rho}$ given in Eq. (42). However, Eve would provide such a state in place of the original (unknown) state ρ only if her uncertainty on the parties' outcomes does not increase.

In the paper, we quantify Eve's uncertainty via the von Neumann entropy of the classical outcomes conditioned on Eve's quantum side information E. The specific outcomes that we consider depend on the cryptographic application that is being addressed. For instance, in the paper we employ Theorem 1 to tightly estimate Eve's uncertainty on Alice's random outcome X by computing $H(X|E)$, when Alice, Bob and Charlie test the MABK inequality. This result finds potential application in DICKA and DIRG protocols. Indeed, in a DICKA scheme Bob and Charlie would correct their raw key bits to match Alice's bits represented by X, while in a DIRG protocol the goal is to ensure that Alice's random outcome X is unknown to Eve. Additionally, we employ Theorem 1 to estimate Eve's uncertainty on the outcomes of Alice (X) and Bob (Y) jointly, by computing $H(XY|E)$.

For illustration purposes, here we provide the full proof that Eve's uncertainty of Alice's outcome X is non-increasing if she distributes the state $\bar{\rho}$ in place of ρ to $N = 3$ parties. However, we remark that an analogous proof would hold for any number of parties and any number of outcomes. Therefore, we must verify that the following condition is met:

$$H(X|E)_\rho \geq H(X|E_{\text{tot}})_{\bar{\rho}}, \tag{II.1}$$

where Eve's quantum system $E_{\text{tot}} = ETT'$ contains: the quantum side information E, the outcome of the random variable T indicating to Eve which of the four states in the mixture $\bar{\rho}$ to distribute, and the purifying system T'. Indeed, Eve preparing $\bar{\rho}$ can be interpreted as she preparing one of the four states:

$$\rho,\ (Z \otimes Z \otimes \text{id})\,\rho\,(Z \otimes Z \otimes \text{id}),\ (Z \otimes \text{id} \otimes Z)\,\rho\,(Z \otimes \text{id} \otimes Z),\ (\text{id} \otimes Z \otimes Z)\,\rho\,(\text{id} \otimes Z \otimes Z) \tag{II.2}$$

depending on the outcome t of a random variable stored in the register T. Since Eve holds the purification of every state in (II.2): $\{|\phi^t_{ABCE}\rangle\}_{t=1}^4$, the global state prepared by Eve is:

$$\bar{\rho}_{ABCET} = \frac{1}{4} \sum_t |\phi^t_{ABCE}\rangle \langle\phi^t_{ABCE}| \otimes |t\rangle\langle t|_T \tag{II.3}$$

Finally, we assume that Eve holds the purifying system of the global state, thus the state she prepares is:

$$|\bar{\phi}_{ABCETT'}\rangle = \frac{1}{2} \sum_t |\phi^t_{ABCE}\rangle \otimes |t\rangle_T \otimes |t\rangle_{T'}\,, \tag{II.4}$$

which is a purification of (II.3), where both registers T and T' are held by Eve and thus appear in E_{tot}.

In order to prove (II.1), we start by using the strong subadditivity property:

$$H(X|E_{\text{tot}})_{\bar{\rho}} \leq H(X|ET)_{\bar{\rho}} \tag{II.5}$$

where the r.h.s. entropy is computed on the following state:

$$\begin{aligned}
\bar{\rho}_{XET} &= (\mathcal{E}_X \otimes \text{id}_{ET}) \operatorname{Tr}_{BC} [\bar{\rho}_{ABCET}] \\
&= \frac{1}{4} (\mathcal{E}_X \otimes \text{id}_{ET}) \operatorname{Tr}_{BC} \left[\sum_t |\phi^t_{ABCE}\rangle \langle\phi^t_{ABCE}| \otimes |t\rangle\langle t|_T \right] \\
&\equiv \frac{1}{4} \sum_t \rho^t_{XE} \otimes |t\rangle\langle t|_T,
\end{aligned} \tag{II.6}$$

where the quantum map

$$\mathcal{E}_X(\sigma) = \sum_{a=0}^{1} |a\rangle\langle a| \langle a| \sigma |a\rangle$$

represents the projective measurement performed by Alice. Being the state in Eq. (II.6) a c.q. state, its entropy simplifies to:

$$H(X|ET)_{\bar{\rho}} = \frac{1}{4}\sum_t H(X|E)_{\rho^t}. \tag{II.7}$$

The last part of the proof shows that $H(X|E)_{\rho^t}$ is actually independent of t and equal to conditional entropy of the original state $H(X|E)_\rho$. This is clear if the state ρ^t_{XE} is made explicit. From Eq. (II.6) we have that:

$$\rho^t_{XE} = (\mathcal{E}_X \otimes \mathrm{id}_{ET})\,\mathrm{Tr}_{BC}\left[|\phi^t_{ABCE}\rangle\langle\phi^t_{ABCE}|\right], \tag{II.8}$$

where $|\phi^t_{ABCE}\rangle$ is the purification of one of the four states in (II.2) prepared by Eve according to the random variable T. For definiteness, let's fix that state to be $(Z \otimes Z \otimes \mathrm{id})\,\rho\,(Z \otimes Z \otimes \mathrm{id})$, although an analogous reasoning holds for any other state in Eq. (II.2). By writing ρ in its spectral decomposition:

$$\rho = \sum_\lambda \lambda |\lambda\rangle\langle\lambda|, \tag{II.9}$$

we can immediately explicit $|\phi^t_{ABCE}\rangle$ as follows:

$$|\phi^t_{ABCE}\rangle = \sum_\lambda \sqrt{\lambda}\,|\lambda^t\rangle_{ABC} \otimes |e_\lambda\rangle_E, \tag{II.10}$$

where the eigenstates of the operator $(Z \otimes Z \otimes \mathrm{id})\,\rho\,(Z \otimes Z \otimes \mathrm{id})$ read: $|\lambda^t\rangle = (Z \otimes Z \otimes \mathrm{id})\,|\lambda\rangle$. By substituting (II.10) into (II.8) and by expliciting the map $\mathcal{E}_X$ we obtain the following expression:

$$\begin{aligned}
\rho^t_{XE} &= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\,\mathrm{Tr}_{BC}\left[\langle a|\,|\lambda^t\rangle\,\langle\sigma^t|\,|a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\,\mathrm{Tr}_{BC}\left[\langle a|\,(Z \otimes Z \otimes \mathrm{id})\,|\lambda\rangle\,\langle\sigma|\,(Z \otimes Z \otimes \mathrm{id})\,|a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\,\mathrm{Tr}_{BC}\left[\langle\bar{a}|\,|\lambda\rangle\,\langle\sigma|\,|\bar{a}\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&= \sum_{a=0}^{1} |\bar{a}\rangle\langle\bar{a}| \otimes \sum_{\lambda,\sigma} \sqrt{\lambda\sigma}\,\mathrm{Tr}_{BC}\left[\langle a|\,|\lambda\rangle\,\langle\sigma|\,|a\rangle\right] |e_\lambda\rangle\langle e_\sigma| \\
&\equiv \sum_{a=0}^{1} |\bar{a}\rangle\langle\bar{a}| \otimes \rho^a_E,
\end{aligned} \tag{II.11}$$

where in the third equality we used the fact that Alice's measurement lies in the (x, y)-plane hence the Z operator flips its outcome ($a \to \bar{a}$) and the cyclic property of the trace. In the fourth equality we relabelled the classical outcomes: $a \leftrightarrow \bar{a}$. Finally, by comparing (II.11) with the analogous state ρ_{XE} obtained from the original state ρ (i.e. in the case where Eve does not prepare the mixture of states in (II.2)):

$$\rho_{XE} = \sum_{a=0}^{1} |a\rangle\langle a| \otimes \rho^a_E, \tag{II.12}$$

we observe that ρ^t_{XE} and ρ_{XE} are the same state up to a permutation of the classical outcomes, thus their conditional entropies coincide:

$$H(X|E)_{\rho^t} = H(X|E)_\rho \quad \forall\, t. \tag{II.13}$$

In conclusion, by combining Eqs. (II.13), (II.7) and (II.5), we obtain the claim given in Eq. (II.1). This concludes the proof.

III. EQUIVALENCE OF $\bar{\rho}_+$ AND $\bar{\rho}_-$

In the main text we claim that it is not restrictive to assume that Eve distributes the following mixture

$$\rho_\alpha = \frac{\bar{\rho}_+ + \bar{\rho}_-}{2}, \tag{III.1}$$

in place of the state $\bar{\rho}_+$ given in Eq. (52). As argued in section II, for illustration purposes we prove the claim in the case where three parties, Alice, Bob and Charlie, test a $(3,2,2)$ full-correlator Bell inequality and are interested in bounding Eve's uncertainty about Alice's outcome X, quantified by the conditional von Neumann entropy $H(X|E)$. Nevertheless, an analogous proof would hold for any number of parties and joint entropies.

In the first part of the proof, we verify that the states $\bar{\rho}_+$ and $\bar{\rho}_-$ are equivalent from the viewpoint of the protocol. Precisely, the statistics generated by the two states coincides, as well as Eve's uncertainty about Alice's outcome, quantified by the conditional entropy $H(X|E)$. In the second part we show that Eve's uncertainty does not increase if she prepares a balanced mixture of the two states (III.1), instead of preparing one of the two states singularly.

We start by computing the statistics generated by the states $\bar{\rho}_+$ and $\bar{\rho}_-$ (52), which read as follows for $N=3$:

$$\bar{\rho}_\pm = \sum_{i,j,k=0}^{1} \lambda_{ijk} \left|\psi_{i,j,k}\right\rangle \left\langle\psi_{i,j,k}\right| \pm \sum_{j,k=0}^{1} r_{jk} \left(\left|\psi_{0,j,k}\right\rangle \left\langle\psi_{1,j,k}\right| + \text{h.c.}\right) + \mathbb{i} s \left(\left|\psi_{0,1,1}\right\rangle \left\langle\psi_{1,1,1}\right| - \text{h.c.}\right), \tag{III.2}$$

where h.c. indicates the Hermitian conjugate of the term appearing alongside it. Note that we arbitrarily assumed three out of four off-diagonal elements to be purely real, according to the prescription characterizing $\bar{\rho}_+$ and $\bar{\rho}_-$ (52).

Since we fixed the parties' measurements to be in the (x,y)-plane, their observables and the relative eigenstates can be written as follows:

$$\begin{aligned}
A &= \cos(\varphi_A)X + \sin(\varphi_A)Y, \quad \left|a\right\rangle_A = \frac{1}{\sqrt{2}}(\left|0\right\rangle + (-1)^a e^{\mathbb{i}\varphi_A}\left|1\right\rangle) \\
B &= \cos(\varphi_B)X + \sin(\varphi_B)Y, \quad \left|b\right\rangle_B = \frac{1}{\sqrt{2}}(\left|0\right\rangle + (-1)^b e^{\mathbb{i}\varphi_B}\left|1\right\rangle) \\
C &= \cos(\varphi_C)X + \sin(\varphi_C)Y, \quad \left|c\right\rangle_C = \frac{1}{\sqrt{2}}(\left|0\right\rangle + (-1)^c e^{\mathbb{i}\varphi_C}\left|1\right\rangle),
\end{aligned} \tag{III.3}$$

where X, Y and Z are the Pauli operators, A, B and C are the observables of Alice, Bob and Charlie, respectively, and the measurement outcomes are defined to be $a,b,c \in \{0,1\}$ (where $a=0$ corresponds to eigenvalue $+1$ and $a=1$ to eigenvalue -1). Then, the statistics generated by the states $\bar{\rho}_+$ and $\bar{\rho}_-$ reads:

$$\begin{aligned}
\Pr[A=a, B=b, C=c]_{\bar{\rho}_\pm} = &\sum_{i,j,k=0}^{1} \lambda_{ijk} \langle\psi_{i,j,k}|\,|a,b,c\rangle\langle a,b,c|\,|\psi_{i,j,k}\rangle \\
&\pm 2\sum_{j,k=0}^{1} r_{jk} \mathrm{Re}[\langle\psi_{0,j,k}|\,|a,b,c\rangle\langle a,b,c|\,|\psi_{1,j,k}\rangle] \\
&- 2\,s\,\mathrm{Im}[\langle\psi_{1,1,1}|\,|a,b,c\rangle\langle a,b,c|\,|\psi_{0,1,1}\rangle].
\end{aligned} \tag{III.4}$$

Therefore, the two statistics coincide if and only if the coefficients of the terms r_{jk} are all identically null:

$$\mathrm{Re}[\langle\psi_{0,j,k}|\,|a,b,c\rangle\langle a,b,c|\,|\psi_{1,j,k}\rangle] = 0 \quad \forall\, j,k,a,b,c. \tag{III.5}$$

A straightforward calculation of the coefficients of r_{jk}, by using the expressions in Eqs. (III.3) and (3), leads to the following result:

$$\langle\psi_{0,j,k}|\,|a,b,c\rangle\langle a,b,c|\,|\psi_{1,j,k}\rangle = \mathbb{i}\,\frac{2(-1)^{a+b+c}\mathrm{Im}[e^{\mathbb{i}\varphi_A} e^{\mathbb{i}\varphi_B(-1)^j} e^{\mathbb{i}\varphi_C(-1)^k}]}{16}, \tag{III.6}$$

which is indeed purely imaginary. This proves the condition (III.5) and thus that the statistics of $\bar{\rho}_+$ and $\bar{\rho}_-$ are identical.

The next step of the proof consists in showing that Eve's uncertainty about Alice's outcome is unchanged if she distributes $\bar{\rho}_+$ or $\bar{\rho}_-$, i.e. the following condition must be verified:

$$H(X|E)_{\bar{\rho}_+} = H(X|E)_{\bar{\rho}_-}. \tag{III.7}$$

In order to show (III.7), we compute the conditional entropy produced by each state as follows:

$$H(X|E) = H(E|X) + H(X) - H(E) \tag{III.8}$$

and verify that each term in (III.8) is identical for the two states $\bar{\rho}_+$ and $\bar{\rho}_-$. To begin with, we know that the Shannon entropy $H(X)$ is given by:

$$H(X) = h(\Pr[A = 0]), \tag{III.9}$$

where $h(\cdot)$ is the binary entropy, defined as: $h(p) = -p \log_2 p - (1-p)\log_2(1-p)$. Since we proved that the statistics generated by $\bar{\rho}_+$ and $\bar{\rho}_-$ are the same, it follows that:

$$H(X)_{\bar{\rho}_+} = H(X)_{\bar{\rho}_-}. \tag{III.10}$$

In order to compute the other two terms in (III.8), we write $\bar{\rho}_+$ and $\bar{\rho}_-$ in their spectral decomposition:

$$\bar{\rho}_\pm \sum_{i,j,k=0}^{1} \rho_{ijk} |\rho^\pm_{ijk}\rangle\langle\rho^\pm_{ijk}|, \tag{III.11}$$

where ρ_{ijk} are the states' eigenvalues, which one can easily verify to be identical for the two states, while $|\rho^\pm_{ijk}\rangle$ are the normalized eigenvectors, expressed for simplicity in terms of the following non-normalized eigenvectors:

$$\begin{aligned}
|\tilde{\rho}^\pm_{ijk}\rangle &= \frac{\lambda_{0jk} - \lambda_{1jk} - (-1)^i \sqrt{4r_{jk}^2 + (\lambda_{0jk} - \lambda_{1jk})^2}}{\pm 2 r_{jk}} \, |\psi_{0,j,k}\rangle + |\psi_{1,j,k}\rangle \\
&\equiv \pm f^i_{jk} \, |\psi_{0,j,k}\rangle + |\psi_{1,j,k}\rangle \quad (j,k) \neq (1,1) && \text{(III.12)} \\
|\tilde{\rho}^\pm_{i11}\rangle &= (\pm r_{11} + \mathbb{i} s) \frac{\lambda_{011} - \lambda_{111} - (-1)^i \sqrt{4r_{11}^2 + 4s^2 + (\lambda_{011} - \lambda_{111})^2}}{2(r_{11}^2 + s^2)} \, |\psi_{0,1,1}\rangle + |\psi_{1,1,1}\rangle \\
&\equiv (\pm g^i_{11} + \mathbb{i} h^i_{11}) \, |\psi_{0,1,1}\rangle + |\psi_{1,1,1}\rangle \, . && \text{(III.13)}
\end{aligned}$$

Since $\bar{\rho}_+$ and $\bar{\rho}_-$ have the same eigenvalues, it holds that:

$$H(ABC)_{\bar{\rho}_+} = H(ABC)_{\bar{\rho}_-}. \tag{III.14}$$

Assuming that Eve holds the purification

$$|\bar{\phi}^\pm_{ABCE}\rangle = \sum_{i,j,k=0}^{1} \sqrt{\rho_{ijk}} \, |\rho^\pm_{ijk}\rangle \otimes |e_{ijk}\rangle \tag{III.15}$$

of the parties' state, where $\{|e_{ijk}\rangle\}$ is an orthonormal basis in E, it follows that:

$$H(E)_{\bar{\rho}_+} = H(E)_{\bar{\rho}_-}. \tag{III.16}$$

The remaining term in (III.8) is $H(E|X)$, which is computed on the c.q. state:

$$\begin{aligned}
\bar{\rho}^\pm_{XE} &= \sum_{a=0}^{1} |a\rangle\langle a| \otimes \sum_{\substack{i,j,k=0 \\ l,m,n=0}}^{1} \sqrt{\rho_{ijk}\rho_{lmn}} \, \mathrm{Tr}_{BC} \left[\langle a| \, |\rho^\pm_{ijk}\rangle \, \langle \rho^\pm_{lmn}| \, |a\rangle \right] |e_{ijk}\rangle\langle e_{lmn}| \\
&\equiv \sum_{a=0}^{1} \Pr[A = a] |a\rangle\langle a| \otimes \rho^{a,\pm}_E, && \text{(III.17)}
\end{aligned}$$

where $\rho^{a,\pm}_E$ is the conditional state of Eve, given that Alice obtained outcome a. By employing the expressions in Eqs. (III.12) and (III.13), one can verify that the operators $\rho^{a,\pm}_E$ are one the transpose of the other: $\rho^{a,+}_E = (\rho^{a,-}_E)^T$. Thus $\rho^{a,+}_E$ and $\rho^{a,-}_E$ have the same eigenvalues, which implies that:

$$H(\rho^{a,+}_E) = H(\rho^{a,-}_E) \tag{III.18}$$

Finally, since the conditional entropy $H(E|X)$ is computed as follows on the classical quantum states in (III.17):

$$H(E|X)_{\bar{\rho}_\pm} = \sum_{a=0}^{1} \Pr[A=a] H(\rho_E^{a,\pm}), \tag{III.19}$$

we conclude that:

$$H(E|X)_{\bar{\rho}_+} = H(E|X)_{\bar{\rho}_-}. \tag{III.20}$$

By combining the results in Eqs. (III.10), (III.16) and (III.20) into (III.7), we verified that the states $\bar{\rho}_+$ and $\bar{\rho}_-$ lead to the same conditional entropy.

The final part of the proof shows that Eve's uncertainty in preparing the mixture ρ_α (III.1) does not increase with respect to preparing one of the two states $\bar{\rho}_\pm$:

$$H(X|E_{\text{tot}})_{\rho_\alpha} \leq H(X|E)_{\bar{\rho}_+}. \tag{III.21}$$

In this way we can guarantee that it is not restrictive to assume that Eve prepares the mixture (III.1). In giving Eve maximum power, we assume that she prepares the following global pure state (similarly to section II):

$$|\phi_{ABCEMM'}\rangle \, \frac{1}{\sqrt{2}} \sum_{m=+,-} |\bar{\phi}^m_{ABCE}\rangle \otimes |m\rangle_M \otimes |m\rangle_{M'} \,, \tag{III.22}$$

where $|\bar{\phi}^\pm_{ABCE}\rangle$ are the purifications of the individual states $\bar{\rho}_\pm$ defined in (III.15), while M is an ancillary system informing Eve on which of the two purified states she prepared and M' is the purifying system of the global state. Therefore, Eve has maximum power and her quantum system comprises: $E_{\text{tot}} = EMM'$. Naturally, it holds that:

$$\rho_\alpha = \mathrm{Tr}_{E_{\text{tot}}} \left[|\phi_{ABCEMM'}\rangle\langle\phi_{ABCEMM'}| \right]. \tag{III.23}$$

For the strong subadditivity property, we have that:

$$H(X|E_{\text{tot}})_{\rho_\alpha} = H(X|EMM')_{\rho_\alpha} \leq H(X|EM)_{\rho_\alpha} = \frac{1}{2} \sum_{m=+,-} H(X|E)_{\bar{\rho}_m}, \tag{III.24}$$

where the last equality is due to the fact that the state $\mathrm{Tr}_{M'}[|\phi_{ABCEMM'}\rangle \langle\phi_{ABCEMM'}|]$ is classical on M. Finally, by employing the result (III.7) into (III.24), we obtain the claim in (III.21). This concludes the proof. The same argument can be used to generalized the proof for the case of N parties and for the conditional entropy of the joint outcome of more than one party.

IV. MAXIMAL MABK VIOLATION BY AN N-QUBIT STATE: PROOF

Here we provide the full proof of Theorem 2 and of Lemma 2, which combined provide an analytical upper bound on the maximal violation of the N-partite MABK inequality by an arbitrary N-qubit state, for rank-one projective measurements. This is, to our knowledge, the only existing upper bound on the violation of an N-partite Bell inequality by an N-qubit state, expressed as a function of the state's parameters. In Ref. [66] the authors only conjectured a bound for the N-party case based on their result valid for three parties. Analogously to the three-party case (see the Methods section in the main text), our N-partite bound is tight on a broader class of states than the bound conjectured in Ref. [66].

We start by proving Lemma 2, which plays an important role in the proof of Theorem 2.

Lemma 2. *Let Q be an $m \times n$ real matrix and let $\|\vec{v}\|$ be the Euclidean norm of vectors $\vec{v} \in \mathbb{R}^k$, for $k = m, n$. Finally, let "$\cdot$" indicate both the scalar product and the matrix-vector multiplication. Then*

$$\max_{\substack{\vec{c} \perp \vec{c}\,' \text{ s.t.} \\ \|\vec{c}\| = \|\vec{c}\,'\| = 1}} \left[\|Q \cdot \vec{c}\|^2 + \|Q \cdot \vec{c}\,'\|^2 \right] = u_1 + u_2 \,, \tag{IV.1}$$

where u_1 and u_2 are the largest and second-to-the-largest eigenvalues of $U \equiv Q^T Q$, respectively.

Proof. Note that U is a symmetric $n \times n$ real matrix, thus it can be diagonalized. The eigenvalue equation for U reads:

$$U \cdot \vec{u}_i = u_i \, \vec{u}_i \quad i = 1, \ldots, n \ , \tag{IV.2}$$

where the set of eigenvectors forms an orthonormal basis of $\mathbb{R}^n$: $\vec{u}_i^T \cdot \vec{u}_j = \delta_{i,j}$ and without loss of generality we ordered the eigenvalues as: $u_1 \geq u_2 \geq \ldots \geq u_n \geq 0$. Note that every eigenvalue is non-negative:

$$u_i = \vec{u}_i^T \cdot U \cdot \vec{u}_i = \vec{u}_i^T \cdot Q^T Q \cdot \vec{u}_i = \left\| Q \cdot \vec{u}_i \right\|^2 \geq 0 \ .$$

By considering that: $\left\| Q \cdot \vec{c} \right\|^2 = \vec{c}^{\,T} \cdot Q^T Q \cdot \vec{c} = \vec{c}^{\,T} \cdot U \cdot \vec{c}$ and by expressing the vectors $\vec{c}$ and $\vec{c}\,'$ in the eigenbasis of U:

$$\vec{c} = \sum_{i=1}^{n} c_i \vec{u}_i$$
$$\vec{c}\,' = \sum_{i=1}^{n} c_i' \vec{u}_i \ ,$$

we can recast the claim in (60) as follows:

$$\max_{\substack{\vec{c} \perp \vec{c}\,' \text{ s.t.} \\ \|\vec{c}\| = \|\vec{c}\,'\| = 1}} \sum_{i=1}^{n} u_i (c_i^2 + {c_i'}^2) = u_1 + u_2 \ . \tag{IV.3}$$

Let us consider the most general scenario in which some of the eigenvalues of U are degenerate: $u_1 \geq u_2 = u_3 = \cdots = u_d > u_{d+1} \geq \ldots u_n \geq 0$, where $d = 2, \ldots, n$. Note that we also account for the possibility that $u_1 = u_2$.
We are now going to prove (IV.3) by showing that for any couple of mutually-orthogonal unit vectors $\vec{c}$ and $\vec{c}\,'$ the left-hand-side of (IV.3) is upper bounded by $u_1 + u_2$ and that the bound is tight.
We start by considering two unit vectors in $\mathbb{R}^n$:

$$\begin{cases} \vec{c}^{\,T} = (c_1, \ldots, c_n) \quad \text{s.t.} \ \left\|\vec{c}\right\|^2 = 1 \\ \vec{c}\,'^T = (c_1', \ldots, c_n') \quad \text{s.t.} \ \left\|\vec{c}\,'\right\|^2 = 1 \ , \end{cases} \tag{IV.4}$$

and we define two unit vectors $\vec{v}, \vec{w} \in \mathbb{R}^{d-1}$ along the directions individuated by $(c_2, \ldots, c_d)$ and $(c_2', \ldots, c_d')$, i.e.:

$$c_v \vec{v}^{\,T} \equiv (c_2, \ldots, c_d)$$
$$c_w' \vec{w}^{\,T} \equiv (c_2', \ldots, c_d') \ , \tag{IV.5}$$

where c_v and c_w' are the norms of $(c_2, \ldots, c_d)$ and $(c_2', \ldots, c_d')$, respectively. For $d = 2$ we simply have that $c_v \vec{v}^{\,T} = c_2$ and $c_w' \vec{w}^{\,T} = c_2'$.
With an abuse of notation, we can rewrite (IV.4) as:

$$\begin{cases} \vec{c}^{\,T} = (c_1, c_v \vec{v}^{\,T}, c_{d+1}, \ldots, c_n) \quad \text{s.t.} \ c_1^2 + c_v^2 + r = 1 \\ \vec{c}\,'^T = (c_1', c_w' \vec{w}^{\,T}, c_{d+1}', \ldots, c_n') \quad \text{s.t.} \ {c_1'}^2 + {c_w'}^2 + r' = 1 \ , \end{cases} \tag{IV.6}$$

where $r \equiv \sum_{i=d+1}^{n} c_i^2$ and $r' \equiv \sum_{i=d+1}^{n} {c_i'}^2$ and for both holds that: $0 \leq r \leq 1$ and $0 \leq r' \leq 1$. From the orthogonality condition $\vec{c}^{\,T} \cdot \vec{c}\,' = 0$ we get that:

$$|c_1 c_1'| = \left| \sum_{i=2}^{n} c_i c_i' \right| \ , \tag{IV.7}$$

and from the Cauchy-Schwarz inequality we deduce that:

$$\left| \sum_{i=2}^{n} c_i c_i' \right| \leq \sqrt{(c_v^2 + r)({c_w'}^2 + r')} \ . \tag{IV.8}$$

By employing (IV.7), (IV.8) and the normalization conditions in (IV.6), we show that $c_1^2 + {c'_1}^2 \leq 1$ holds:

$$\begin{aligned} \left(c_1^2 + {c'_1}^2\right)^2 &= c_1^4 + {c'_1}^4 + 2c_1^2{c'_1}^2 \\ &\leq c_1^4 + {c'_1}^4 + 2\left(1 - c_1^2\right)\left(1 - {c'_1}^2\right) \\ &= 2 - 2\left(c_1^2 + {c'_1}^2\right) + \left(c_1^2 + {c'_1}^2\right)^2 \ . \end{aligned} \tag{IV.9}$$

By comparing the left-hand-side with the right-hand-side one gets the desired result:

$$c_1^2 + {c'_1}^2 \leq 1 \ . \tag{IV.10}$$

We now prove the claim in (IV.3) through the following chain of equalities and inequalities:

$$\begin{aligned} \sum_{i=1}^n u_i(c_i^2 + {c'_i}^2) &= u_1(c_1^2 + {c'_1}^2) + u_2(c_v^2 + {c'_w}^2) + \sum_{i=d+1}^n u_i(c_i^2 + {c'_i}^2) \\ &\leq u_1(c_1^2 + {c'_1}^2) + u_2(1 - r - c_1^2 + 1 - r' - {c'_1}^2) + u_{d+1}(r + r') \\ &= u_2 + (u_1 - u_2)(c_1^2 + {c'_1}^2) + u_2 - (r + r')(u_2 - u_{d+1}) \\ &\leq u_1 + u_2 \ , \end{aligned} \tag{IV.11}$$

where we used the normalization conditions and the fact that the eigenvalues are ordered in descending order for the first inequality, and we used (IV.10) together with the fact that $r, r' \geq 0$ for the second inequality.

We are left to show that (IV.11) is tight, that is there exist unit vectors $\vec{c}$ and $\vec{c}'$ for which the equality sign holds. If $u_1 = u_2$, the upper bound is attained when $r = r' = 0$. Thus the most general pair of vectors satisfying (IV.3) is given by:

$$\begin{cases} \vec{c}^T = (\vec{V}^T, 0, \dots, 0) \\ \vec{c}'^T = (\vec{W}^T, 0, \dots, 0) \end{cases} , \vec{V}, \vec{W} \in \mathbb{R}^d \text{ s.t. } \left\|\vec{V}\right\| = \left\|\vec{W}\right\| = 1 \ \wedge \ (\vec{V}, \vec{W}) = 0 \ . \tag{IV.12}$$

If instead $u_1 > u_2$, the upper bound is attained when $r = r' = 0$ and $c_1^2 + {c'_1}^2 = 1$. The second condition is verified when the equality holds in (IV.8), which in turn happens when the unit vectors $\vec{v}$ and $\vec{w}$ are parallel. Thus the most general pair of vectors satisfying (IV.3) is given by:

$$\begin{cases} \vec{c}^T = (c_1, c_v\vec{v}^T, 0, \dots, 0) \\ \vec{c}'^T = (c'_1, c'_w\vec{v}^T, 0, \dots, 0) \end{cases} , \vec{v} \in \mathbb{R}^{d-1} \ \wedge \ c_1^2 + {c'_1}^2 = 1 \ , \tag{IV.13}$$

and where the orthogonality and normalization conditions hold: $c_1c'_1 + c_vc'_w = 0$, $c_1^2 + c_v^2 = 1$ and ${c'_1}^2 + {c'_w}^2 = 1$. Such solutions can always be parametrized as follows:

$$\begin{cases} \vec{c}^T = (\cos\alpha, \sin\alpha\,\vec{v}^T, 0, \dots, 0) \\ \vec{c}'^T = (-\sin\alpha, \cos\alpha\,\vec{v}^T, 0, \dots, 0) \end{cases} , \alpha \in \mathbb{R} \ . \tag{IV.14}$$

This concludes the proof. □

We are now ready to prove Theorem 2.

Theorem 2. *The maximum violation $\mathcal{M}_\rho$ of the N-partite MABK inequality* (9)*, attained with rank-one projective measurements on an N-qubit state ρ, satisfies*

$$\mathcal{M}_\rho \leq 2\sqrt{t_0 + t_1} \tag{IV.15}$$

where t_0 and t_1 are the largest and second-to-the-largest eigenvalues of the matrix $T_\rho T_\rho^T$, where T_ρ is the correlation matrix of ρ.

Proof. Firstly, we present closed expressions for the N-partite MABK operator, defined recursively in Definition 2. In particular, in Ref. [74] the explicit expression of the N-partite MABK operator when N is odd is given:

$$M_N^{\text{odd}} = \frac{1}{2^{\frac{N-3}{2}}} \sum_{\mathbf{x} \in \mathcal{L}_N} (-1)^{\frac{1}{2}\left(\frac{N-1}{2} - \omega(\mathbf{x})\right)} \bigotimes_{i=1}^N A_{x_i}^{(i)}, \tag{IV.16}$$

where $A_0^{(i)}$ and $A_1^{(i)}$ are the two binary observables of Alice$_i$, while $\mathbf{x} = (x_1, \ldots, x_N)$ is a bit string with Hamming weight given by:

$$\omega(\mathbf{x}) = |\{1 \leq i \leq N | x_i = 1\}|, \tag{IV.17}$$

and the set $\mathcal{L}_N$ is defined as follows:

$$\mathcal{L}_N = \left\{ \mathbf{x} \in \{0,1\}^N \middle| \omega(\mathbf{x}) = \frac{N-1}{2} \mod 2 \right\}. \tag{IV.18}$$

By applying once the MABK recursive formula (7) on (IV.16), one obtains an explicit expression of the N-partite MABK operator for N even. We distinguish the case $N/2$ even:

$$\frac{N}{2} \text{ even:} \quad M_N^{\text{even}} = \frac{1}{2^{\frac{N-2}{2}}} \sum_{\mathbf{x} \in \{0,1\}^N} (-1)^{\frac{N}{4} - \lceil \frac{\omega(\mathbf{x})}{2} \rceil} \bigotimes_{i=1}^{N} A_{x_i}^{(i)}, \tag{IV.19}$$

and the case $N/2$ odd:

$$\frac{N}{2} \text{ odd:} \quad M_N^{\text{even}} = \frac{1}{2^{\frac{N-2}{2}}} \sum_{\mathbf{x} \in \{0,1\}^N} (-1)^{\frac{N-2}{4} - \lfloor \frac{\omega(\mathbf{x})}{2} \rfloor} \bigotimes_{i=1}^{N} A_{x_i}^{(i)}, \tag{IV.20}$$

where $\lceil a \rceil$ and $\lfloor a \rfloor$ are the ceiling and floor functions, respectively.

We now derive an explicit expression of the MABK expectation value for a generic N-qubit state. As shown above, the N-party MABK operator can be written in explicit form as follows:

$$M_N = \frac{1}{\mathcal{N}_N} \sum_{\mathbf{x} \in \mathcal{S}_N} (-1)^{\xi_N(\mathbf{x})} \bigotimes_{i=1}^{N} A_{x_i}^{(i)}, \tag{IV.21}$$

where the normalization factor $\mathcal{N}_N$, the set of N-bit strings $\mathcal{S}_N$ and the exponent $\xi_N(\mathbf{x})$ depend on the parity of N (e.g. $\mathcal{S}_N = \{0,1\}^N$ for N even and $\mathcal{S}_N = \mathcal{L}_N$ for N odd). By assumption we restrict to rank-one projective measurements, hence every observable $A_{x_i}^{(i)}$ can be individuated by a unit vector $\vec{a}_{x_i}^{\,i} \in \mathbb{R}^3$ such that:

$$A_{x_i}^{(i)} = \vec{a}_{x_i}^{\,i} \cdot \vec{\sigma} = \sum_{\nu_i=1}^{3} a_{x_i,\nu_i}^{i} \sigma_{\nu_i}, \tag{IV.22}$$

where $\vec{\sigma} = (X, Y, Z)^T$. By substituting (IV.22) into (IV.21) are by rearranging the terms we get:

$$\begin{aligned} M_N &= \frac{1}{\mathcal{N}_N} \sum_{\nu_1,\ldots,\nu_N=1}^{3} \left[\sum_{\mathbf{x} \in \mathcal{S}_N} (-1)^{\xi_N(\mathbf{x})} \prod_{i=1}^{N} a_{x_i,\nu_i}^{i} \right] \sigma_{\nu_1} \otimes \ldots \otimes \sigma_{\nu_N} \\ &\equiv \frac{1}{\mathcal{N}_N} \sum_{\nu_1,\ldots,\nu_N=1}^{3} M_{\nu_1,\ldots,\nu_N} \sigma_{\nu_1} \otimes \ldots \otimes \sigma_{\nu_N}. \end{aligned} \tag{IV.23}$$

We now employ (IV.23) and the expression for a generic N-qubit state:

$$\rho = \frac{1}{2^N} \sum_{\mu_1 \ldots \mu_N=0}^{3} \Lambda_{\mu_1 \ldots \mu_N} \sigma_{\mu_1} \otimes \ldots \otimes \sigma_{\mu_N}, \tag{IV.24}$$

to derive an explicit expression for the MABK expectation value as follows:

$$\begin{aligned} \langle M_N \rangle_\rho = \mathrm{Tr}[M_N \rho] &= \frac{1}{\mathcal{N}_N} \sum_{\nu_1,\ldots,\nu_N=1}^{3} M_{\nu_1,\ldots,\nu_N} \Lambda_{\nu_1 \ldots \nu_N} \\ &= \frac{1}{\mathcal{N}_N} \sum_{\nu_1,\ldots,\nu_N=1}^{3} \left[\sum_{\mathbf{x} \in \mathcal{S}_N} (-1)^{\xi_N(\mathbf{x})} \, a_{x_1,\nu_1}^{1} \cdot \ldots \cdot a_{x_N,\nu_N}^{N} \, \Lambda_{\nu_1 \ldots \nu_N} \right], \end{aligned} \tag{IV.25}$$

where we used the fact that $\mathrm{Tr}[\sigma_i\sigma_j] = 2\delta_{i,j}$.

We now specify the expressions for $\mathcal{N}_N, \mathcal{S}_N$ and $\xi_N(\mathbf{x})$ when $N/2$ is even and prove the theorem's statement in this particular case. However, a similar procedure applies to the $N/2$ odd and N odd cases and leads to the same final result.

We thus have the following expression for the MABK expectation value:

$$\langle M_N\rangle_\rho = \frac{1}{2^{\frac{N-2}{2}}} \sum_{\nu_1,\ldots,\nu_N=1}^{3} \left[\sum_{\mathbf{x}\in\{0,1\}^N} (-1)^{\frac{N}{4}-\lceil\frac{\omega(\mathbf{x})}{2}\rceil}\, a^1_{x_1,\nu_1}\cdot\ldots\cdot a^N_{x_N,\nu_N}\ \Lambda_{\nu_1\ldots\nu_N}\right], \tag{IV.26}$$

and we rearrange it as follows:

$$\begin{aligned}\langle M_N\rangle_\rho = {} & \frac{1}{2^{\frac{N-2}{2}}} \sum_{\nu_1,\ldots,\nu_N=1}^{3} \left[\sum_{\mathbf{x}\in\{0,1\}^{N/2}} \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\frac{N}{4}-\lceil\frac{\omega(\mathbf{x})+\omega(\mathbf{y})}{2}\rceil}\right.\\ & \left. a^1_{x_1,\nu_1}\cdot\ldots\cdot a^{N/2}_{x_{N/2},\nu_{N/2}}\ \Lambda_{\nu_1\ldots\nu_N}\ a^{N/2}_{y_1,\nu_{N/2}}\cdot\ldots\cdot a^N_{y_{N/2},\nu_N}\right]\\ = {} & \frac{1}{2^{\frac{N-2}{2}}} \sum_{\nu_1,\ldots,\nu_N=1}^{3} \left[\sum_{\mathbf{x}\in\mathcal{E}_{N/2}} \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\frac{N}{4}-\lceil\frac{\omega(\mathbf{x})+\omega(\mathbf{y})}{2}\rceil}\right.\\ & a^1_{x_1,\nu_1}\cdot\ldots\cdot a^{N/2}_{x_{N/2},\nu_{N/2}}\ \Lambda_{\nu_1\ldots\nu_N}\ a^{N/2}_{y_1,\nu_{N/2}}\cdot\ldots\cdot a^N_{y_{N/2},\nu_N}\\ & + \sum_{\mathbf{x}\in\mathcal{O}_{N/2}} \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\frac{N}{4}-\lceil\frac{\omega(\mathbf{x})+\omega(\mathbf{y})}{2}\rceil}\\ & \left. a^1_{x_1,\nu_1}\cdot\ldots\cdot a^{N/2}_{x_{N/2},\nu_{N/2}}\ \Lambda_{\nu_1\ldots\nu_N}\ a^{N/2}_{y_1,\nu_{N/2}}\cdot\ldots\cdot a^N_{y_{N/2},\nu_N}\right],\end{aligned} \tag{IV.27}$$

where the sets $\mathcal{E}_{N/2}$ and $\mathcal{O}_{N/2}$ are defined as follows:

$$\mathcal{E}_{N/2} = \Big\{\mathbf{x}\in\{0,1\}^{N/2} | \omega(\mathbf{x}) \mod 2 = 0\Big\} \tag{IV.28}$$

$$\mathcal{O}_{N/2} = \Big\{\mathbf{x}\in\{0,1\}^{N/2} | \omega(\mathbf{x}) \mod 2 = 1\Big\}. \tag{IV.29}$$

We basically split the bit strings $\mathbf{x}$ into those with an even Hamming weight and those with an odd Hamming weight. Now considering that the following identity holds:

$$\left\lceil\frac{\omega(\mathbf{x})+\omega(\mathbf{y})}{2}\right\rceil = \begin{cases} \omega(\mathbf{x}) \text{ even: } & \lfloor\frac{\omega(\mathbf{x})}{2}\rfloor + \lfloor\frac{\omega(\mathbf{y})}{2}\rfloor + (\omega(\mathbf{y}) \mod 2) \\ \omega(\mathbf{x}) \text{ odd: } & \lfloor\frac{\omega(\mathbf{x})}{2}\rfloor + \lfloor\frac{\omega(\mathbf{y})}{2}\rfloor + 1, \end{cases} \tag{IV.30}$$

we can recast the MABK expectation value in (IV.27) as follows:

$$\begin{aligned}\langle M_N\rangle_\rho = {} & \frac{1}{2^{\frac{N-2}{2}}} \sum_{\nu_1,\ldots,\nu_N=1}^{3} \left[\left(\sum_{\mathbf{x}\in\mathcal{E}_{N/2}} (-1)^{\frac{N}{4}-\lfloor\frac{\omega(\mathbf{x})}{2}\rfloor}\, a^1_{x_1,\nu_1}\cdot\ldots\cdot a^{N/2}_{x_{N/2},\nu_{N/2}} \right)\right.\\ & \Lambda_{\nu_1\ldots\nu_N} \left(\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor+(\omega(\mathbf{y}) \mod 2)}\, a^{N/2}_{y_1,\nu_{N/2}}\cdot\ldots\cdot a^N_{y_{N/2},\nu_N} \right)\\ & + \left(\sum_{\mathbf{x}\in\mathcal{O}_{N/2}} (-1)^{\frac{N}{4}-\lfloor\frac{\omega(\mathbf{x})}{2}\rfloor}\, a^1_{x_1,\nu_1}\cdot\ldots\cdot a^{N/2}_{x_{N/2},\nu_{N/2}} \right)\\ & \left. \Lambda_{\nu_1\ldots\nu_N} \left(\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor+1}\, a^{N/2}_{y_1,\nu_{N/2}}\cdot\ldots\cdot a^N_{y_{N/2},\nu_N} \right)\right]\\ \equiv {} & \frac{1}{2^{\frac{N-2}{2}}} \left[\vec{v}_0^{\,T}\cdot T_\rho\cdot\vec{u}_0 + \vec{v}_1^{\,T}\cdot T_\rho\cdot\vec{u}_1\right].\end{aligned} \tag{IV.31}$$

In the expression (IV.31) we defined the vectors:

$$\vec{v}_0 = \sum_{\mathbf{x}\in\mathcal{E}_{N/2}} (-1)^{\frac{N}{4}-\lfloor\frac{\omega(\mathbf{x})}{2}\rfloor} \bigotimes_{i=1}^{N/2} \vec{a}^{\,i}_{x_i}, \tag{IV.32}$$

$$\vec{v}_1 = \sum_{\mathbf{x}\in\mathcal{O}_{N/2}} (-1)^{\frac{N}{4}-\lfloor\frac{\omega(\mathbf{x})}{2}\rfloor} \bigotimes_{i=1}^{N/2} \vec{a}^{\,i}_{x_i}, \tag{IV.33}$$

$$\vec{u}_0 = \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor+(\omega(\mathbf{y}) \mod 2)} \bigotimes_{i=1}^{N/2} \vec{a}^{\,N/2+i}_{y_i}, \tag{IV.34}$$

$$\vec{u}_1 = \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor+1} \bigotimes_{i=1}^{N/2} \vec{a}^{\,N/2+i}_{y_i}, \tag{IV.35}$$

and we used Definition 3 of the correlation matrix of an N-qubit state. The $3^{N/2}$-dimensional vectors in (IV.32),(IV.33),(IV.34) and (IV.35) are heavily constrained by their tensor-product structure and satisfy the following properties:

$$\text{Prop. 1:} \quad \|\vec{v}_0\|^2 + \|\vec{v}_1\|^2 = 2^{N/2} \tag{IV.36}$$

$$\text{Prop. 2:} \quad \|\vec{u}_0\|^2 = \|\vec{u}_1\|^2 = 2^{N/2} \tag{IV.37}$$

$$\text{Prop. 3:} \quad \vec{v}_0 \cdot \vec{v}_1 = 0. \tag{IV.38}$$

These properties play a fundamental role in deriving a meaningful upper bound on the MABK expectation value.

We prove the first property (IV.36) by directly computing the l.h.s.:

$$\begin{aligned}\|\vec{v}_0\|^2 + \|\vec{v}_1\|^2 &= \vec{v}_0\cdot\vec{v}_0 + \vec{v}_1\cdot\vec{v}_1 \\ &= \sum_{\mathbf{x},\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\frac{N}{2}-\lfloor\frac{\omega(\mathbf{x})}{2}\rfloor-\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor} \prod_{i=1}^{N/2} (\cos\theta_i)^{x_i\oplus y_i} \\ &+ \sum_{\mathbf{x},\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\frac{N}{2}-\lfloor\frac{\omega(\mathbf{x})}{2}\rfloor-\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor} \prod_{i=1}^{N/2} (\cos\theta_i)^{x_i\oplus y_i},\end{aligned} \tag{IV.39}$$

where we used the fact that $\vec{a}^{\,i}_{x_i}$ are unit vectors and we called θ_i the angle between the two measurement directions of party number i: $\cos\theta_i = \vec{a}^{\,i}_0 \cdot \vec{a}^{\,i}_1$. Note that the symbol $\oplus$ is the binary operation XOR. We now define the bit string: $\mathbf{r} = \mathbf{x}\oplus\mathbf{y}$, whose Hamming weight can be computed as:

$$\omega(\mathbf{r}) = \omega(\mathbf{x}\oplus\mathbf{y}) = \omega(\mathbf{x}) + \omega(\mathbf{y}) - 2\omega(\mathbf{x}\wedge\mathbf{y}), \tag{IV.40}$$

where $\wedge$ is the binary operation AND. From (IV.40) it follows immediately that the Hamming weight of the string $\mathbf{r}$ is always even, since the Hamming weights of $\mathbf{x}$ and $\mathbf{y}$ are either both even or both odd in (IV.39). With this information, we can recast (IV.39) as follows:

$$\|\vec{v}_0\|^2 + \|\vec{v}_1\|^2 = \sum_{\mathbf{r}\in\mathcal{E}_{N/2}} \left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\lfloor\frac{\omega(\mathbf{r}\oplus\mathbf{y})}{2}\rfloor+\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor} + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\lfloor\frac{\omega(\mathbf{r}\oplus\mathbf{y})}{2}\rfloor+\lfloor\frac{\omega(\mathbf{y})}{2}\rfloor} \right] \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i}, \tag{IV.41}$$

where we used the fact that $N/2$ is even and where the string $\mathbf{x}$ is completely fixed once $\mathbf{r}$ and $\mathbf{y}$ are fixed: $\mathbf{x} = \mathbf{r}\oplus\mathbf{y}$. Now we employ the relation (IV.40) in (IV.41) and we make use of the information on the parity of the Hamming weights appearing in the two sums:

$$\begin{aligned}\|\vec{v}_0\|^2 + \|\vec{v}_1\|^2 = &\sum_{\mathbf{r}\in\mathcal{E}_{N/2}} \left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})}{2}+\omega(\mathbf{y})-\omega(\mathbf{r}\wedge\mathbf{y})} + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})+\omega(\mathbf{y})-2\omega(\mathbf{r}\wedge\mathbf{y})-1}{2}+\frac{\omega(\mathbf{y})-1}{2}} \right] \\ &\times \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i}.\end{aligned} \tag{IV.42}$$

Note that $\lfloor a/2 \rfloor = (a-1)/2$ if a is an odd number. The expression in (IV.42) can be further simplified by considering that even addends in the exponents of (-1) can be ignored:

$$\begin{aligned}
\|\vec{v}_0\|^2 + \|\vec{v}_1\|^2 &= \sum_{\mathbf{r}\in\mathcal{E}_{N/2}} \left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})}{2} - \omega(\mathbf{r}\wedge\mathbf{y})} + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})}{2} - \omega(\mathbf{r}\wedge\mathbf{y})} \right] \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i} \\
&= \sum_{\mathbf{r}\in\mathcal{E}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})}{2}} \left[\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} \right] \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i} \\
&= 2^{N/2} + \sum_{\substack{\mathbf{r}\in\mathcal{E}_{N/2} \\ \mathbf{r}\neq\mathbf{0}}} (-1)^{\frac{\omega(\mathbf{r})}{2}} \left[\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} \right] \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i}, \qquad \text{(IV.43)}
\end{aligned}$$

where we extracted the term $\mathbf{r} = \mathbf{0}$ from the sum in the last equality.

The last step to prove the first property (IV.36) is to show that every term in the remaining sum in (IV.43) is identically zero, i.e. we want to show that:

$$\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} = 0 \quad \forall \mathbf{r} \neq \mathbf{0}. \qquad \text{(IV.44)}$$

In order for (IV.44) to be verified, there must be as many (-1) terms as $+1$ terms, and since there are in total $2^{N/2}$ terms, there must be exactly $2^{N/2-1}$ terms (half of the total) that are (-1). We can count the number of (-1) terms in (IV.44) as follows:

$$\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (\omega(\mathbf{r}\wedge\mathbf{y}) \mod 2), \qquad \text{(IV.45)}$$

and check whether it equals $2^{N/2-1}$, as claimed. Note that $\omega(\mathbf{r}\wedge\mathbf{y})$ represents the number of ones in $\mathbf{r}$ that are also in $\mathbf{y}$. The parity of this number is then summed over all the possible bit strings $\mathbf{y}$ of length $N/2$. We can thus recast the sum, as a sum over the number of ones that $\mathbf{r}$ and $\mathbf{y}$ have in common (k), times the number of bit strings $\mathbf{y}$ that share k ones with $\mathbf{r}$:

$$\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (\omega(\mathbf{r}\wedge\mathbf{y}) \mod 2) = \sum_{k=0}^{\omega(\mathbf{r})} (k \mod 2) \binom{\omega(\mathbf{r})}{k} 2^{N/2-\omega(\mathbf{r})}. \qquad \text{(IV.46)}$$

Note that the number of bit strings $\mathbf{y}$ that have k ones in common with a fixed string $\mathbf{r}$, is given by the number of possible combinations of k ones from the total number of ones ($\omega(\mathbf{r})$) populating the string $\mathbf{r}$, times the number of possibilities ($2^{N/2-\omega(\mathbf{r})}$) that we have to fill the remaining bits of $\mathbf{y}$ that are not part of the k ones in common with $\mathbf{r}$.

We can now adjust the r.h.s. of (IV.46) to the following computable form:

$$\begin{aligned}
2^{N/2-\omega(\mathbf{r})} \sum_{\substack{k=0 \\ k\,\text{odd}}}^{\omega(\mathbf{r})} \binom{\omega(\mathbf{r})}{k} &= 2^{N/2-\omega(\mathbf{r})}\ 2^{\omega(\mathbf{r})-1} \\
&= 2^{N/2-1}, \qquad \text{(IV.47)}
\end{aligned}$$

where the first equality is obtained by combining two known facts about the binomial coefficient, namely:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \text{(IV.48)}$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0. \qquad \text{(IV.49)}$$

Indeed, by subtracting (IV.49) from (IV.48) one gets that:

$$\sum_{k\,\text{odd}} \binom{n}{k} = 2^{n-1}, \qquad \text{(IV.50)}$$

which is used in the first equality in (IV.47).

Combining (IV.46) and (IV.47) we conclude that (IV.44) is verified. We have thus shown the validity of the first property (IV.36).

We move on to prove the second property (IV.37). We start from (IV.34) and use the fact that $\lfloor \frac{\omega(\mathbf{x})}{2} \rfloor + (\omega(\mathbf{x}) \mod 2) = (\omega(\mathbf{x}) + [\omega(\mathbf{x}) \mod 2)]/2)$:

$$\begin{aligned}
\|\vec{u}_0\|^2 &= \sum_{\mathbf{x},\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\frac{\omega(\mathbf{x})+(\omega(\mathbf{x}) \mod 2)}{2}+\frac{\omega(\mathbf{y})+(\omega(\mathbf{y}) \mod 2)}{2}} \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{x_i \oplus y_i} \\
&= \sum_{\mathbf{r}\in\{0,1\}^{N/2}} \left[\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\frac{\omega(\mathbf{r})+\omega(\mathbf{y})-2\omega(\mathbf{r}\wedge\mathbf{y})+(\omega(\mathbf{r})+\omega(\mathbf{y}) \mod 2)}{2}+\frac{\omega(\mathbf{y})+(\omega(\mathbf{y}) \mod 2)}{2}} \right] \\
&\times \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{r_i}, \qquad \text{(IV.51)}
\end{aligned}$$

where we defined $\mathbf{r} = \mathbf{x} \oplus \mathbf{y}$ and we used the relation (IV.40). We proceed to simplify (IV.51) by splitting the sum over $\mathbf{y}$ over the strings with even and odd Hamming weight:

$$\begin{aligned}
\|\vec{u}_0\|^2 = \sum_{\mathbf{r}\in\{0,1\}^{N/2}} &\left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})+(\omega(\mathbf{r}) \mod 2)}{2}-\omega(\mathbf{r}\wedge\mathbf{y})} \right. \\
&\left. + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})+1+(\omega(\mathbf{r})+1 \mod 2)}{2}-\omega(\mathbf{r}\wedge\mathbf{y})+\omega(\mathbf{y})} \right] \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{r_i}. \qquad \text{(IV.52)}
\end{aligned}$$

By employing the following identities:

$$\frac{\omega(\mathbf{r}) + (\omega(\mathbf{r}) \mod 2)}{2} = \left\lceil \frac{\omega(\mathbf{r})}{2} \right\rceil \qquad \text{(IV.53)}$$

$$(-1)^a = (-1)^1 \quad a \text{ odd} \qquad \text{(IV.54)}$$

$$\frac{\omega(\mathbf{r}) + 1 + (\omega(\mathbf{r}) + 1 \mod 2)}{2} = \left\lceil \frac{\omega(\mathbf{r}) + 1}{2} \right\rceil = \left\lceil \frac{\omega(\mathbf{r})}{2} \right\rceil + 1 - (\omega(\mathbf{r}) \mod 2) \qquad \text{(IV.55)}$$

into (IV.52) we obtain:

$$\begin{aligned}
\|\vec{u}_0\|^2 &= \sum_{\mathbf{r}\in\{0,1\}^{N/2}} (-1)^{\lceil \frac{\omega(\mathbf{r})}{2} \rceil} \left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} \right. \\
&\left. + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})+(\omega(\mathbf{r}) \mod 2)} \right] \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{r_i} \\
&= 2^{N/2} + \sum_{\substack{\mathbf{r}\in\{0,1\}^{N/2} \\ \mathbf{r}\neq\mathbf{0}}} (-1)^{\lceil \frac{\omega(\mathbf{r})}{2} \rceil} \left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} \right. \\
&\left. + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})+(\omega(\mathbf{r}) \mod 2)} \right] \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{r_i} \\
&= 2^{N/2} + \sum_{\substack{\mathbf{r}\in\mathcal{E}_{N/2} \\ \mathbf{r}\neq\mathbf{0}}} (-1)^{\lceil \frac{\omega(\mathbf{r})}{2} \rceil} \left[\sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} \right] \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{r_i} \\
&+ \sum_{\mathbf{r}\in\mathcal{O}_{N/2}} (-1)^{\lceil \frac{\omega(\mathbf{r})}{2} \rceil} \left[\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} - \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} \right] \prod_{i=1}^{N/2} (\cos(\theta_{N/2+i}))^{r_i}, \qquad \text{(IV.56)}
\end{aligned}$$

where we isolated the $\mathbf{r} = \mathbf{0}$ term in the second equality and we split the sum over $\mathbf{r}$ in two sums over the strings with even and odd Hamming weights in the third equality.

The first sum in (IV.56) is zero thanks to (IV.44). From (IV.44) we also deduce that:

$$\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} + \sum_{\mathbf{y}\in\mathcal{O}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} = 0, \tag{IV.57}$$

which means that the term in square brackets in the second sum can be reduced to:

$$2 \sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{y})} = 0. \tag{IV.58}$$

The proof that (IV.58) holds is analogous to that of (IV.44). In particular, (IV.58) is verified if the number of (-1) terms is exactly half the total number of terms, that is $2^{N/2-2}$. We show that this is true by computing the number of (-1) terms as follows:

$$\begin{aligned}\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (\omega(\mathbf{r}\wedge\mathbf{y}) \mod 2) &= \sum_{k=0}^{\omega(\mathbf{r})} (k \mod 2) \binom{\omega(\mathbf{r})}{k} 2^{N/2-\omega(\mathbf{r})-1} \\ &= 2^{N/2-\omega(\mathbf{r})-1} \sum_{\substack{k=0\\ k \text{ odd}}}^{\omega(\mathbf{r})} \binom{\omega(\mathbf{r})}{k}. \end{aligned} \tag{IV.59}$$

Note that this time, compared to (IV.46), the number of possibilities ($2^{N/2-\omega(\mathbf{r})-1}$) to fill the non-fixed bits of $\mathbf{y}$ is halved. The reason is that in this case $\mathbf{y}$ is constrained to have an even number of ones, thus after fixing $N/2-1$ of its bits, no degree of freedom is left.

By employing again the result on binomial distributions (IV.50) in (IV.59), we obtain:

$$\sum_{\mathbf{y}\in\mathcal{E}_{N/2}} (\omega(\mathbf{r}\wedge\mathbf{y}) \mod 2) = 2^{N/2-2}, \tag{IV.60}$$

which proves (IV.58).

We have thus shown that both the sums in (IV.56) are zero, thus proving the second property (IV.37) for $\vec{u}_0$. The proof of (IV.37) for $\vec{u}_1$ is analogous and we omit it.

Finally we show that the third property (IV.38) is satisfied by direct computation:

$$\begin{aligned}\vec{v}_0 \cdot \vec{v}_1 &= \sum_{\substack{\mathbf{x}\in\mathcal{E}_{N/2}\\ \mathbf{y}\in\mathcal{O}_{N/2}}} (-1)^{\lfloor \frac{\omega(\mathbf{x})}{2} \rfloor + \lfloor \frac{\omega(\mathbf{y})}{2} \rfloor} \prod_{i=1}^{N/2} (\cos\theta_i)^{x_i \oplus y_i} \\ &= \sum_{\substack{\mathbf{x}\in\mathcal{E}_{N/2}\\ \mathbf{y}\in\mathcal{O}_{N/2}}} (-1)^{\frac{\omega(\mathbf{x})}{2} + \frac{\omega(\mathbf{y})-1}{2}} \prod_{i=1}^{N/2} (\cos\theta_i)^{x_i \oplus y_i} \\ &= \sum_{\mathbf{r}\in\mathcal{O}_{N/2}} \left[\sum_{\mathbf{x}\in\mathcal{E}_{N/2}} (-1)^{\frac{\omega(\mathbf{x})-1+\omega(\mathbf{x})+\omega(\mathbf{r})-2\omega(\mathbf{r}\wedge\mathbf{x})}{2}} \right] \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i} \\ &= \sum_{\mathbf{r}\in\mathcal{O}_{N/2}} (-1)^{\frac{\omega(\mathbf{r})-1}{2}} \left[\sum_{\mathbf{x}\in\mathcal{E}_{N/2}} (-1)^{\omega(\mathbf{r}\wedge\mathbf{x})} \right] \prod_{i=1}^{N/2} (\cos\theta_i)^{r_i} \\ &= 0, \end{aligned} \tag{IV.61}$$

where we defined $\mathbf{r} = \mathbf{x} \oplus \mathbf{y}$ and used (IV.40) in the third equality, and used (IV.58) in the last equality.

Thanks to the properties (IV.36), (IV.37) and (IV.38), we can express the vectors $\vec{v}_k$ and $\vec{u}_k$ ($k = 0, 1$) as follows:

$$\vec{v}_0 = 2^{N/4} \cos\theta \, \hat{v}_0 \tag{IV.62}$$

$$\vec{v}_1 = 2^{N/4} \sin\theta \, \hat{v}_1 \tag{IV.63}$$

$$\vec{u}_k = 2^{N/4} \, \hat{u}_k \tag{IV.64}$$

where $\hat{v}_k$ and $\hat{u}_k$ are unit vectors in the directions of $\vec{v}_k$ and $\vec{u}_k$, respectively, and where θ is a real number. With the expressions (IV.62), (IV.63) and (IV.64) we recast the MABK expectation value (IV.31) as follows:

$$\begin{aligned}\langle M_N\rangle_\rho &= \frac{2^{N/2}}{2^{\frac{N-2}{2}}}\left[\cos\theta\, \hat{v}_0^T \cdot T_\rho \cdot \hat{u}_0 + \sin\theta\, \hat{v}_1^T \cdot T_\rho \cdot \hat{u}_1\right] \\ &= 2\left[\cos\theta\, \hat{v}_0^T \cdot T_\rho \cdot \hat{u}_0 + \sin\theta\, \hat{v}_1^T \cdot T_\rho \cdot \hat{u}_1\right]. \qquad \text{(IV.65)}\end{aligned}$$

The maximal violation $\mathcal{M}_\rho$ of the N-partite MABK inequality is then obtained by maximizing (IV.65) over all the parties' measurements directions $\vec{a}_0^i$ and $\vec{a}_1^i$ (for $i = 1, \ldots, N$). A valid upper bound on the maximal violation $\mathcal{M}_\rho$ is thus given by:

$$\mathcal{M}_\rho \leq \max_{\substack{\hat{v}_k, \hat{u}_k, \theta \\ \hat{v}_0 \perp \hat{v}_1}} 2\left[\cos\theta\, \hat{v}_0^T \cdot T_\rho \cdot \hat{u}_0 + \sin\theta\, \hat{v}_1^T \cdot T_\rho \cdot \hat{u}_1\right], \qquad \text{(IV.66)}$$

where the inequality is due to the fact that we are now optimizing the expectation value over all the possible unit vectors $\hat{v}_k$ (such that $\hat{v}_0 \cdot \hat{v}_1 = 0$) and $\hat{u}_k$, and freely over θ, ignoring the more stringent structures (IV.32)-(IV.35) characterizing these vectors and their relation to θ. By choosing $\hat{u}_0$ and $\hat{u}_1$ in the direction of $\hat{v}_0^T \cdot T_\rho$ and $\hat{v}_1^T \cdot T_\rho$, respectively, and by fixing θ such that:

$$\tan\theta = \frac{\left\|T_\rho^T \cdot \hat{v}_1\right\|}{\left\|T_\rho^T \cdot \hat{v}_0\right\|}, \qquad \text{(IV.67)}$$

we can simplify the maximization in (IV.66) as follows:

$$\begin{aligned}\mathcal{M}_\rho &\leq \max_{\substack{\hat{v}_k, \hat{u}_k, \theta \\ \hat{v}_0 \perp \hat{v}_1}} 2\left[\cos\theta\, \hat{v}_0^T \cdot T_\rho \cdot \hat{u}_0 + \sin\theta\, \hat{v}_1^T \cdot T_\rho \cdot \hat{u}_1\right] \\ &= \max_{\substack{\hat{v}_k, \theta \\ \hat{v}_0 \perp \hat{v}_1}} 2\left[\cos\theta\, \left\|T_\rho^T \cdot \hat{v}_0\right\| + \sin\theta\, \left\|T_\rho^T \cdot \hat{v}_1\right\|\right] \\ &= \max_{\substack{\hat{v}_k \\ \hat{v}_0 \perp \hat{v}_1}} 2\sqrt{\left\|T_\rho^T \cdot \hat{v}_0\right\|^2 + \left\|T_\rho^T \cdot \hat{v}_1\right\|^2}. \qquad \text{(IV.68)}\end{aligned}$$

Finally, by employing the result of Lemma 2 in (IV.68), we obtain the statement of the theorem:

$$\mathcal{M}_\rho \leq \sqrt{t_0 + t_1}, \qquad \text{(IV.69)}$$

where t_0 and t_1 are the two largest eigenvalues of $T_\rho T_\rho^T$. This concludes the proof. □

Tightness conditions: Here we derive the conditions for which the upper bound on the MABK violation given in (10) is tight. That is, there exist observables for the N parties such that the violation achieved on the state ρ is exactly given by the r.h.s. of (10). We first address the case $N/2$ even since it is the one explicitly derived in the proof, then we present the tightness conditions valid in the other cases.

The bound is tight when equality holds in (IV.66). Considering that we made specific choices for the unit vectors $\hat{v}_i$ and $\hat{u}_i$ and for θ, the vectors in (IV.32)-(IV.35) should comply with these specific choices. In particular, consider the eigenvalue equation for $T_\rho T_\rho^T$ with normalized eigenvectors and where t_0 and t_1 are the two largest eigenvalues:

$$T_\rho T_\rho^T \hat{t}_k = t_k \hat{t}_k. \qquad \text{(IV.70)}$$

In order to use Lemma 2 in (IV.68), it must hold that:

$$\hat{v}_k = \frac{\vec{v}_k}{\|\vec{v}_k\|} = \hat{t}_k \quad k = 0, 1, \qquad \text{(IV.71)}$$

where $\vec{v}_k$ ($k = 0, 1$) are defined in (IV.32) and (IV.33). Employing (IV.71) into the relation (IV.67) that fixes θ we get:

$$\frac{\|\vec{v}_1\|}{\|\vec{v}_0\|} = \tan\theta = \frac{\left\|T_\rho^T \cdot \hat{t}_1\right\|}{\left\|T_\rho^T \cdot \hat{t}_0\right\|} = \sqrt{\frac{t_1}{t_0}}, \qquad \text{(IV.72)}$$

where the last equality is due to (IV.70). Combining (IV.72) with property (IV.36) we completely fix the norms of vectors $\vec{v}_0$ and $\vec{v}_1$, while their direction is already fixed by (IV.71). In conclusion we get the following tightness conditions for $\vec{v}_0$ and $\vec{v}_1$, which we recall being specific combinations (IV.32) and (IV.33) of the parties' measurement directions:

$$\vec{v}_k = 2^{N/4}\sqrt{\frac{t_k}{t_0+t_1}}\hat{t}_k \quad k=0,1. \tag{IV.73}$$

In addition to this, we also fixed the directions $\hat{u}_0$ and $\hat{u}_1$ to those of $T_\rho^T \cdot \hat{v}_0$ and $T_\rho^T \cdot \hat{v}_1$, respectively. Due to (IV.71) and recalling property (IV.37), we derive the following tightness conditions on $\vec{u}_0$ and $\vec{u}_1$:

$$\vec{u}_k = \frac{2^{N/4}}{\sqrt{t_k}} T_\rho^T \hat{t}_k \quad k=0,1. \tag{IV.74}$$

One can verify that upon substituting the tightness conditions (IV.73) and (IV.74) into the MABK expectation value (IV.31), the theorem claim is obtained.

Here we recapitulate the tightness conditions of theorem 2 for the two cases N even and N odd. The bound in (10) is tight if there exist unit vectors $\vec{a}_0^i, \vec{a}_1^i$ (with $i=1,\dots,N$) such that:

- *N even*:

$$\vec{v}_k = 2^{N/4}\sqrt{\frac{t_k}{t_0+t_1}}\hat{t}_k \quad , \quad \vec{u}_k = \frac{2^{N/4}}{\sqrt{t_k}} T_\rho^T \hat{t}_k \quad k=0,1, \tag{IV.75}$$

  where vectors $\vec{v}_k$ and $\vec{u}_k$ are defined in (IV.32)-(IV.35) if $N/2$ is even, or as follows if $N/2$ is odd:

$$\vec{v}_0 = \sum_{\mathbf{x}\in\mathcal{E}_{N/2}} (-1)^{\frac{N-2}{4}-\left\lfloor\frac{\omega(\mathbf{x})}{2}\right\rfloor} \bigotimes_{i=1}^{N/2} \vec{a}_{x_i}^i, \tag{IV.76}$$

$$\vec{v}_1 = \sum_{\mathbf{x}\in\mathcal{O}_{N/2}} (-1)^{\frac{N-2}{4}-\left\lfloor\frac{\omega(\mathbf{x})}{2}\right\rfloor} \bigotimes_{i=1}^{N/2} \vec{a}_{x_i}^i, \tag{IV.77}$$

$$\vec{u}_0 = \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\left\lfloor\frac{\omega(\mathbf{y})}{2}\right\rfloor} \bigotimes_{i=1}^{N/2} \vec{a}_{y_i}^{N/2+i}, \tag{IV.78}$$

$$\vec{u}_1 = \sum_{\mathbf{y}\in\{0,1\}^{N/2}} (-1)^{\left\lceil\frac{\omega(\mathbf{y})}{2}\right\rceil} \bigotimes_{i=1}^{N/2} \vec{a}_{y_i}^{N/2+i}, \tag{IV.79}$$

  where the sets $\mathcal{E}_{N/2}$ and $\mathcal{O}_{N/2}$ are defined in (IV.28) and (IV.29), respectively.

- *N odd*:

$$\vec{v}_k = 2^{(N+1)/4}\sqrt{\frac{t_k}{t_0+t_1}}\hat{t}_k \quad , \quad \vec{u}_k = \frac{2^{(N-3)/4}}{\sqrt{t_k}} T_\rho^T \hat{t}_k \quad k=0,1, \tag{IV.80}$$

  where vectors $\vec{v}_k$ and $\vec{u}_k$ are defined as follows:

$$\vec{v}_0 = \sum_{\mathbf{x}\in\mathcal{E}_{(N+1)/2}} (-1)^{\left\lfloor\frac{N-1}{4}\right\rfloor-\left\lfloor\frac{\omega(\mathbf{x})}{2}\right\rfloor} \bigotimes_{i=1}^{(N+1)/2} \vec{a}_{x_i}^i, \tag{IV.81}$$

$$\vec{v}_1 = \sum_{\mathbf{x}\in\mathcal{O}_{(N+1)/2}} (-1)^{\left\lfloor\frac{N-1}{4}\right\rfloor-\left\lfloor\frac{\omega(\mathbf{x})}{2}\right\rfloor} \bigotimes_{i=1}^{(N+1)/2} \vec{a}_{x_i}^i, \tag{IV.82}$$

$$\vec{u}_0 = \sum_{\mathbf{y}\in\mathcal{J}_{(N-1)/2}} (-1)^{\left\lfloor\frac{\omega(\mathbf{y})}{2}\right\rfloor} \bigotimes_{i=1}^{(N-1)/2} \vec{a}_{y_i}^{(N+1)/2+i}, \tag{IV.83}$$

$$\vec{u}_1 = \sum_{\mathbf{y}\in\overline{\mathcal{J}}_{(N-1)/2}} (-1)^{\left\lceil\frac{\omega(\mathbf{y})}{2}\right\rceil} \bigotimes_{i=1}^{(N-1)/2} \vec{a}_{y_i}^{(N+1)/2+i}, \tag{IV.84}$$

with the sets $\mathcal{J}_{(N-1)/2}$ and $\overline{\mathcal{J}}_{(N-1)/2}$ fixed as:

$$\mathcal{J}_{(N-1)/2} = \left\{ \mathbf{x} \in \{0,1\}^{(N-1)/2} \middle| \omega(\mathbf{x}) = \frac{N-1}{2} \mod 2 \right\} \tag{IV.85}$$

$$\overline{\mathcal{J}}_{(N-1)/2} = \left\{ \mathbf{x} \in \{0,1\}^{(N-1)/2} \middle| \omega(\mathbf{x}) + 1 = \frac{N-1}{2} \mod 2 \right\}. \tag{IV.86}$$

V. ANALYTICAL PROOF OF THE LOWER BOUND ON $H(X|E)_{\rho_\alpha}$

We want to derive an analytical lower bound on $H(X|E)_{\rho_\alpha}$, given by:

$$H(X|E)_{\rho_\alpha} = 1 - H(\{\rho_{ijk}\}) + H(\{\rho_{ijk} + \rho_{i\bar{j}\bar{k}}\}), \tag{V.1}$$

for an observed MABK violation m_α. For ease of notation, in the following we drop the subscript α in the observed violation.

In the Methods section we provide an upper bound on the maximal MABK violation achieved on ρ_α, given by:

$$\mathcal{M}_\alpha \leq \mathcal{M}_\alpha^\uparrow = 4\sqrt{\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk})^2}. \tag{V.2}$$

Thus, we want to solve the following optimization problem:

$$\begin{aligned} H(X|E)^\downarrow_{\rho_\alpha}(m) = \min_{\{\rho_{ijk}\}} & \; H(X|E)_{\rho_\alpha} \\ \text{sub. to } & \; \mathcal{M}_\alpha^\uparrow \geq m \; ; \; \rho_{0jk} \geq \rho_{1jk} \; ; \; \sum_{ijk} \rho_{ijk} = 1, \end{aligned} \tag{V.3}$$

where the second constraint is given in (19) and where $m \geq 2\sqrt{2}$, otherwise the conditional entropy is null (see figure 1 of the paper). Because of the symmetry of the problem, we can assume w.l.o.g. that the largest element in $\{\rho_{ijk}\}$ is ρ_{000}. Then, a necessary condition such that $\mathcal{M}_\alpha^\uparrow \geq 2\sqrt{2}$ is given by $\rho_{000} \geq 1/2$. Indeed, the following upper bound on $\mathcal{M}_\alpha^\uparrow$:

$$\mathcal{M}_\alpha^\uparrow = 4\sqrt{\sum_{j,k=0}^{1} (\rho_{0jk} - \rho_{1jk})^2} \leq 4\sqrt{\sum_{j,k=0}^{1} \rho_{0jk}^2} \leq 4\sqrt{\sum_{j,k=0}^{1} \rho_{000} \cdot \rho_{0jk}} = 4\sqrt{\rho_{000}\left(\sum_{j,k=0}^{1} \rho_{0jk}\right)} \leq 4\sqrt{\rho_{000}}, \tag{V.4}$$

is greater than or equal to $2\sqrt{2}$ when $\rho_{000} \geq 1/2$.

Note that, by definition, the minimal entropy $H(X|E)^\downarrow_{\rho_\alpha}(m)$ in (V.3) is monotonically increasing in m.

The upper bound on the maximal MABK violation (V.2) is tight on the following class of states (the tightness conditions (75) are verified):

$$\tau(\nu) = \nu|\psi_{0,0,0}\rangle\langle\psi_{0,0,0}| + (1-\nu)|\psi_{0,1,1}\rangle\langle\psi_{0,1,1}|, \tag{V.5}$$

and reads in this case

$$\mathcal{M}_\tau(\nu) = \mathcal{M}_\tau^\uparrow(\nu) = 4\sqrt{\nu^2 + (1-\nu)^2}. \tag{V.6}$$

It is straightforward to verify that

$$\mathcal{M}_\tau(\rho_{000}) \geq \mathcal{M}_\alpha^\uparrow \quad \forall \{\rho_{ijk}\}. \tag{V.7}$$

Moreover, the entropy (V.1) evaluated on the states (V.5) reads:

$$H(X|E)_\tau(\nu) = 1 - h(\nu), \tag{V.8}$$

where we used the binary entropy $h(p) = -p\log p - (1-p)\log(1-p)$. Here and in the following, "log" represents the logarithm in base 2.

By definition, the entropy minimized over all the states with $\mathcal{M}_\alpha^\uparrow \geq m$ (V.3) is upper bounded by the entropy of any particular state with $\mathcal{M}_\alpha^\uparrow = m$:

$$H(X|E)^\downarrow_{\rho_\alpha}(m) \leq H(X|E)_\tau(\nu_m) \tag{V.9}$$

where ν_m is fixed such that the maximal violation of the state $\tau(\nu_m)$ is given by m:

$$\mathcal{M}_\tau^\uparrow(\nu_m) = 4\sqrt{\nu_m^2 + (1-\nu_m)^2} = m. \tag{V.10}$$

On the other hand, in the following we prove that:

$$H(X|E)_{\rho_\alpha} \geq H(X|E)_\tau(\rho_{000}) \quad \forall\,\{\rho_{ijk}\}, \tag{V.11}$$

where $\rho_{000} \geq 1/2$ is the largest element in $\{\rho_{ijk}\}$. In particular, the last expression holds for the state ρ^*_α which is the solution of the minimization in (V.3):

$$\begin{aligned} H(X|E)^\downarrow_{\rho_\alpha}(m) = H(X|E)_{\rho^*_\alpha} &\geq H(X|E)_\tau(\rho^*_{000}) \\ &\geq H(X|E)_\tau(\nu_m). \end{aligned} \tag{V.12}$$

The last inequality in (V.12) is due to a couple of observations. Firstly, by applying (V.7) to the state ρ^*_α we obtain $\mathcal{M}_\tau(\rho^*_{000}) \geq m$, which combined with (V.10) implies that $\rho^*_{000} \geq \nu_m$ (in the interval of interest $\rho^*_{000}, \nu_m \geq 1/2$). Then, we observe that the entropy of the states τ in (V.8) is monotonically increasing in the interval $\nu \in [1/2, 1]$. The two observations lead to the second inequality in (V.12).

By combining (V.12) with (V.9), we obtain the desired lower bound:

$$H(X|E)^\downarrow_{\rho_\alpha}(m) = H(X|E)_\tau(\nu_m). \tag{V.13}$$

Note that the family of states $\tau(\nu)$ in (V.5) minimizes the entropy for every observed violation m. The bound in (V.13) can be expressed in terms of the violation m by reverting (V.10) and by using it in (V.8), thus obtaining Eq. (27) of the paper.

The derived bound is tight since, for every violation m, there exists a state $\tau(\nu_m)$ (where ν_m is defined in (V.10)) such that its entropy coincides with the derived lower bound (V.13) and such that it can yield an MABK violation equal to m. Indeed, we stated that for the family $\tau(\nu)$ the upper bound $\mathcal{M}_\tau^\uparrow$ is tight (V.6), i.e. there exists a set of measurements that attain the violation $\mathcal{M}_\tau^\uparrow$.

We are thus left to prove the inequality in (V.11), which can be recast as follows:

$$h(\rho_{000}) + H(\{\rho_{ijk} + \rho_{i\bar{j}\bar{k}}\}) - H(\{\rho_{ijk}\}) \geq 0. \tag{V.14}$$

To start with, we simplify the difference of the following entropies:

$$h(\rho_{000}) - H(\{\rho_{ijk}\}) = -(1-\rho_{000})\log(1-\rho_{000}) + \sum_{(i,j,k)\neq(0,0,0)} \rho_{ijk}\log\rho_{ijk}. \tag{V.15}$$

By substituting (V.15) into the l.h.s. of (V.14), we get:

$$\begin{aligned} &H(X|E)_{\rho_\alpha} - H(X|E)_\tau(\rho_{000}) = \\ &H(\{\rho_{ijk} + \rho_{i\bar{j}\bar{k}}\}) + \sum_{(i,j,k)\neq(0,0,0)} \rho_{ijk}\log\rho_{ijk} - (1-\rho_{000})\log(1-\rho_{000}). \end{aligned} \tag{V.16}$$

We then apply Jensen's inequality

$$f(x+y) \geq \frac{f(2x) + f(2y)}{2}, \tag{V.17}$$

where $f(x) = -x\log x$ is a concave function, to the last three terms of the first entropy in (V.16):

$$\begin{aligned} H(\{\rho_{ijk} + \rho_{i\bar{j}\bar{k}}\}) = &-(\rho_{000}+\rho_{011})\log(\rho_{000}+\rho_{011}) - (\rho_{001}+\rho_{010})\log(\rho_{001}+\rho_{010}) \\ &-(\rho_{100}+\rho_{111})\log(\rho_{100}+\rho_{111}) - (\rho_{101}+\rho_{110})\log(\rho_{101}+\rho_{110}), \end{aligned} \tag{V.18}$$

such that we get

$$\begin{aligned} H(\{\rho_{ijk}+\rho_{i\bar{j}\bar{k}}\}) &\geq -(\rho_{000}+\rho_{011})\log(\rho_{000}+\rho_{011}) + \sum_{(i,j,k)\neq {(0,0,0) \atop (0,1,1)}} -\rho_{ijk}\log(2\rho_{ijk}) \\ &= -(\rho_{000}+\rho_{011})\log(\rho_{000}+\rho_{011}) - (1-\rho_{000}-\rho_{011}) + \sum_{(i,j,k)\neq {(0,0,0) \atop (0,1,1)}} -\rho_{ijk}\log\rho_{ijk}. \end{aligned} \tag{V.19}$$

With this result, the difference of entropies in (V.16) can be estimated by

$$\begin{aligned} &H(X|E)_{\rho_\alpha} - H(X|E)_{\tau}(\rho_{000}) \geq \\ &-(\rho_{000}+\rho_{011})\log(\rho_{000}+\rho_{011}) - (1-\rho_{000})\log(2(1-\rho_{000})) + \rho_{011}\log(2\rho_{011}) \\ &=: g(\rho_{000},\rho_{011}). \end{aligned} \tag{V.20}$$

In the function g the first two terms are positive and the last is negative. We further analyze and estimate the function $g(x,y)$ in the range of interest, i.e. $1/2 \leq x \leq 1$, $0 \leq y \leq 1-x$. In this range $g(x,y)$ is concave in x because its second derivative is always negative:

$$\frac{\partial^2 g(x,y)}{\partial x^2} = -\frac{1}{\ln(2)}\left(\frac{1}{(1-x)} + \frac{1}{(x+y)}\right) < 0. \tag{V.21}$$

Consider the boundary $x+y=1$ of $g(x,y)$ for which we get $g(1-y,y)=0$. Due to the concavity it holds for $0 \leq p \leq 1$ that:

$$g\left(p\frac{1}{2} + (1-p)(1-y), y\right) \geq pg\left(\frac{1}{2}, y\right) + (1-p)g(1-y,y),$$

or equivalently that:

$$g(x,y) \geq \left(\frac{1-x-y}{\frac{1}{2}-y}\right) g\left(\frac{1}{2}, y\right). \tag{V.22}$$

Note that from the parameter regimes of x and y it follows that

$$0 \leq \left(\frac{1-x-y}{\frac{1}{2}-y}\right) \leq 1. \tag{V.23}$$

We finally analyze the properties of $g(\frac{1}{2}, y)$, which is convex in y as its second derivative is always positive:

$$\frac{\partial^2 g(\frac{1}{2},y)}{\partial y^2} = \frac{1}{y\ln(2) + y^2\ln(4)} > 0. \tag{V.24}$$

A convex function has a unique minimum if it exists in the parameter regime. In our case this is given by:

$$\frac{\partial g(\frac{1}{2},y)}{\partial y} = \log(2y) - \log(\frac{1}{2}+y) \overset{!}{=} 0 \quad \Leftrightarrow \quad y = \frac{1}{2} \tag{V.25}$$

for which $g(\frac{1}{2},\frac{1}{2}) = 0$ holds. Thus in general it holds:

$$g\left(\frac{1}{2}, y\right) \geq 0. \tag{V.26}$$

By combining these considerations we obtain the desired inequality (V.11):

$$\begin{aligned} H(X|E)_{\rho_\alpha} - H(X|E)_{\tau}(\rho_{000}) &\overset{(V.20)}{\geq} g(\rho_{000},\rho_{011}) \\ &\overset{(V.22)}{\geq} \left(\frac{1-\rho_{000}-\rho_{011}}{\frac{1}{2}-\rho_{011}}\right) g\left(\frac{1}{2}, \rho_{011}\right) \\ &\geq 0, \end{aligned} \tag{V.27}$$

where in the last inequality we used the fact that the pre-factor is positive (V.23) and that $g(\frac{1}{2}, \rho_{011})$ is lower bounded by zero (V.26).

VI. ANALYTICAL PROOF OF THE LOWER BOUND ON $H(XY|E)_{\rho_\alpha}$

In order to derive an analytical lower bound on $H(XY|E)_{\rho_\alpha}$, we employ the same argument used in minimizing $H(X|E)_{\rho_\alpha}$ and perform the optimization over the eigenvalues $\{\rho_{ijk}\}$ of ρ_α and over the parameter q given in (18). This implies that we want to solve the following optimization problem:

$$\begin{aligned} H(XY|E)^{\downarrow}_{\rho_\alpha}(m) = & \min_{\{\rho_{ijk},q,\varphi_A,\varphi_B\}} H(XY|E)_{\rho_\alpha} \\ & \text{sub. to} \quad \mathcal{M}^{\uparrow}_\alpha \geq m \ ; \ \rho_{0jk} \geq \rho_{1jk} \ ; \ \sum_{ijk} \rho_{ijk} = 1, \end{aligned} \tag{VI.1}$$

where $\mathcal{M}^{\uparrow}_\alpha$ is the upper bound on the MABK violation derived in the Methods section (see (V.2)), while φ_A and φ_B determine the unknown measurement directions of Alice and Bob in the (x, y)-plane.

Eve is assumed to hold the purifying system E of the state ρ_α shared by Alice, Bob and Charlie. The purification of ρ_α can thus be written as follows:

$$|\phi^{\alpha}_{ABCE}\rangle = \sum_{ijk} \sqrt{\rho_{ijk}}\, |\rho_{ijk}\rangle \otimes |e_{ijk}\rangle \,, \tag{VI.2}$$

where $|\rho_{ijk}\rangle$ are the eigenstates of ρ_α defined in (17), while $\{|e_{ijk}\rangle\}$ is an orthonormal basis of Eve's eight-dimensional Hilbert space $\mathcal{H}_E$.

We restrict our proof to states ρ_α with a non-negative off-diagonal term $s \geq 0$, which corresponds to $q \geq 0$. The complementary case corresponds to states ρ^*_α which would lead to the same result. For this, we employ a parametrization of the eigenstates slightly different from (17), which reads as follows:

$$\begin{aligned} |\rho_{ijk}\rangle &= |\psi_{ijk}\rangle \,, \quad \text{for} \ \ (j,k) \neq (1,1) \\ |\rho_{011}\rangle &= \sqrt{(1-p)}\, |\psi_{011}\rangle - \mathbb{i}\sqrt{p}\, |\psi_{111}\rangle \\ |\rho_{111}\rangle &= \sqrt{p}\, |\psi_{011}\rangle + \mathbb{i}\sqrt{(1-p)}\, |\psi_{111}\rangle \,, \end{aligned} \tag{VI.3}$$

where $|\psi_{ijk}\rangle$ are the GHZ basis states (Definition 1) and where p is completely fixed by q through the relation:

$$p = \frac{q^2}{1+q^2}, \tag{VI.4}$$

from which we deduce that $0 \leq p \leq 1$ and that $p = 0$ when $q = 0$.

From now on, we omit the subscript ρ_α in the entropy symbol for ease of notation. We thus have that the conditional entropy $H(XY|E)$ can be expressed as:

$$\begin{aligned} H(XY|E) &= H(XY) + H(E|XY) - H(E) \\ &= 2 + H(E|XY) - H(\{\rho_{ijk}\}). \end{aligned} \tag{VI.5}$$

where the last equation follows from the fact that all marginals have been symmetrized and from the fact that the state on $ABCE$ is pure (VI.2), thus $H(E) = H(ABC) = H(\{\rho_{ijk}\})$.

The proof of the analytical lower bound on $H(XY|E)$ as a function of the MABK violation is subdivided in three parts: (i) we first derive an analytical expression for $H(E|XY)$; (ii) we minimize $H(E|XY)$ with respect to q, φ_A and φ_B; (iii) we proceed minimizing the resulting expression in (VI.5) given a certain MABK violation. Note that we are allowed to minimize $H(E|XY)$ over q, φ_A and φ_B independently of $H(E)$, since the latter is independent of the mentioned optimization variables.

Step 1 - Analytical expression for $H(E|XY)$:

In order to derive the analytical expression for $H(E|XY)$, we will use the following Lemma.

Lemma 3. *It holds that*

$$H(E|XY) = H(C|XY). \tag{VI.6}$$

Proof. The proof follows from the fact that the state shared by Charlie and Eve conditioned on the outcomes $X = a$ of Alice and $Y = b$ of Bob, is a pure state. Indeed, if projective measurements are applied to a pure state, the resulting state, conditioned on a specific outcome, remains pure. Moreover, for a pure state, the entropies of its subsystems are equal, which implies

$$H(E|X\!=\!a,Y\!=\!b) = H(C|X\!=\!a,Y\!=\!b) \tag{VI.7}$$

Therefore

$$\begin{aligned} H(E|XY) &= \sum_{a,b} \Pr(a,b) H(E|X=a,Y=b) &\text{(VI.8)}\\ &= \sum_{a,b} \Pr(a,b) H(C|X=a,Y=b) &\text{(VI.9)}\\ &= H(C|XY). &\text{(VI.10)}\end{aligned}$$

□

This Lemma is of great use as Eve's system is described by an eight-dimensional Hilbert space, whereas Charlie is only in possession of a single qubit. So the computation of $H(C|XY)$ is significantly simpler.

We obtain Charlie's state, conditioned on the outcomes $X = a$ and $Y = b$, by partially tracing over Eve's degrees of freedom

$$\rho^{\alpha}_{C_{ab}} = \mathrm{Tr}_E \left(|\phi^{\alpha}_{CE_{ab}}\rangle\langle\phi^{\alpha}_{CE_{ab}}| \right), \tag{VI.11}$$

where $|\phi^{\alpha}_{CE_{ab}}\rangle$ is the state of Charlie and Eve given that Alice and Bob obtain outcomes $X = a$ and $Y = b$ respectively, which is determined by

$$[|a\rangle\langle a|\otimes|b\rangle\langle b|\otimes\mathrm{id}_{CE}]\,[|\phi^{\alpha}_{ABCE}\rangle\langle\phi^{\alpha}_{ABCE}|]\,[|a\rangle\langle a|\otimes|b\rangle\langle b|\otimes\mathrm{id}_{CE}] = \frac{1}{4}|a\rangle\langle a|\otimes|b\rangle\langle b|\otimes|\phi^{\alpha}_{CE_{ab}}\rangle\langle\phi^{\alpha}_{CE_{ab}}|. \tag{VI.12}$$

The projected state $|\phi^{\alpha}_{CE_{ab}}\rangle$ can be computed using the definition of the purification given in Eq. (VI.2), the definition of the eigenstates in Eq. (VI.3), and the fact that the measurements performed by Alice and Bob have been restricted to the (x, y)-plane. Indeed, the measurements are defined by the projectors in (32) of the main text, that we report here:

$$\begin{aligned} |a\rangle_X &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a e^{\mathbb{i}\varphi_A}|1\rangle) \quad a \in \{0,1\}\\ |b\rangle_Y &= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b e^{\mathbb{i}\varphi_B}|1\rangle) \quad b \in \{0,1\}. \end{aligned} \tag{VI.13}$$

In the following we abbreviate $\xi_a = (-1)^a \mathrm{e}^{\mathbb{i}\varphi_A}$ and $\xi_b = (-1)^b \mathrm{e}^{\mathbb{i}\varphi_B}$. We then have that

$$\begin{aligned} |\phi^{\alpha}_{CE_{ab}}\rangle = &\sum_{\substack{ljk\\ jk\neq 11}} \frac{1}{\sqrt{2}} \left((\delta_{0j} + \delta_{1j}\xi_b)\,|k\rangle + (\delta_{0\bar{j}}\xi_a + \delta_{1\bar{j}}\xi_a\xi_b)(-1)^l\,|\bar{k}\rangle \right) \otimes |e_{ljk}\rangle \sqrt{\rho_{ljk}}\\ &+ \left(\left(\sqrt{(1-p)} - \mathbb{i}\sqrt{p}\right) \xi_b\,|1\rangle + \left(\sqrt{(1-p)} + \mathbb{i}\sqrt{p}\right) \xi_a\,|0\rangle \right) \otimes |e_{011}\rangle \sqrt{\rho_{011}}\\ &+ \left(\left(\sqrt{p} + \mathbb{i}\sqrt{(1-p)}\right) \xi_b\,|1\rangle + \left(\sqrt{p} - \mathbb{i}\sqrt{(1-p)}\right) \xi_a\,|0\rangle \right) \otimes |e_{111}\rangle \sqrt{\rho_{111}}. \end{aligned} \tag{VI.14}$$

Finally, the partial trace over Eve results in

$$\rho^{\alpha}_{C_{ab}} = \mathrm{Tr}_E \left(|\phi^{\alpha}_{CE_{ab}}\rangle\langle\phi^{\alpha}_{CE_{ab}}| \right) \tag{VI.15}$$

$$\begin{aligned} = &\left(\sum_{\substack{ljk\\ jk\neq 11}} \frac{1}{\sqrt{2}} \left((\delta_{0j} + \delta_{1j}\xi_b)\,|k\rangle + (\delta_{0\bar{j}}\xi_a + \delta_{1\bar{j}}\xi_a\xi_b)(-1)^l\,|\bar{k}\rangle \right) \right) \cdot (\text{h.c.})\,\rho_{ljk}\\ &+ \left(\left(\sqrt{(1-p)} - \mathbb{i}\sqrt{p}\right) \xi_b\,|1\rangle + \left(\sqrt{(1-p)} + \mathbb{i}\sqrt{p}\right) \xi_a\,|0\rangle \right) \cdot (\text{h.c.})\,\rho_{011}\\ &+ \left(\left(\sqrt{p} + \mathbb{i}\sqrt{(1-p)}\right) \xi_b\,|1\rangle + \left(\sqrt{p} - \mathbb{i}\sqrt{(1-p)}\right) \xi_a\,|0\rangle \right) \cdot (\text{h.c.})\,\rho_{111}. \end{aligned} \tag{VI.16}$$

As $\rho^{\alpha}_{C_{ab}}$ is a qubit state, we can now analytically calculate its eigenvalues, which can be reduced to

$$\lambda_{1,2}(\rho^{\alpha}_{C_{ab}}) = \frac{1}{2}\left(1 \pm |C|\right), \tag{VI.17}$$

where:

$$\begin{aligned} C =& \left(\rho_{000} - \rho_{100}\right)\xi_a^2 + \left(\rho_{001} - \rho_{101}\right)\left(\xi_b^2\right)^* + \left(\rho_{010} - \rho_{110}\right)\xi_a^2\left(\xi_b^2\right)^* + \left(\rho_{011} - \rho_{111}\right)\left(1 - 2p - 2\mathbb{i}\sqrt{p(1-p)}\right) \\ =& \left(\rho_{000} - \rho_{100}\right)\mathrm{e}^{\mathbb{i}2\varphi_A} + \left(\rho_{001} - \rho_{101}\right)\mathrm{e}^{-\mathbb{i}2\varphi_B} + \left(\rho_{010} - \rho_{110}\right)\mathrm{e}^{\mathbb{i}2(\varphi_A - \varphi_B)} + \left(\rho_{011} - \rho_{111}\right)\mathrm{e}^{\mathbb{i}\varphi_3}, \end{aligned} \tag{VI.18}$$

where φ_3 is a function of the parameter p. We see that the eigenvalues do not depend on the measurement outcomes a and b of Alice and Bob. The entropy is then given by

$$H(E|XY) = H(C|XY) = h\left(\frac{1}{2}\left(1 + |C|\right)\right), \tag{VI.19}$$

where $h(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy.

Step 2 - Minimization of $H(E|XY)$:
Minimizing the binary entropy in (VI.19), with respect to the measurement directions and the parameter p, is equivalent to maximizing the largest eigenvalue of $\rho^{\alpha}_{C_{ab}}$. The optimum can directly be deduced from Eq. (VI.17). Since it holds that $(\rho_{0jk} - \rho_{1jk}) \geq 0\,\forall\, j,k$, the largest eigenvalue is maximized if

$$\mathrm{e}^{\mathbb{i}2\varphi_A} = \mathrm{e}^{-\mathbb{i}2\varphi_B} = \mathrm{e}^{\mathbb{i}2(\varphi_A - \varphi_B)} = \mathrm{e}^{\mathbb{i}\varphi_3}, \tag{VI.20}$$

which holds e.g. for $\varphi_A = \varphi_B = \varphi_3 = 0$. Since $\varphi_3 = 0$ implies $p = q = 0$, we verified that even in the minimization of the conditional entropy of two parties' outcomes, $H(XY|E)$, it is optimal for Eve to distribute a GHZ-diagonal state which Alice and Bob measure in the X basis. The largest eigenvalue is then given by

$$\lambda_{\max} = \sum_{jk}\rho_{0jk}, \tag{VI.21}$$

where we used normalization of the eigenvalues to eliminate the terms ρ_{1jk}. The lower bound on the conditional entropy $H(E|XY)$ is thus given by

$$H(E|XY) \geq h\left(\sum_{jk}\rho_{0jk}\right). \tag{VI.22}$$

Step 3 - Minimization of $H(XY|E)$ with given MABK violation:
Using the result of Step 2 in (VI.5), we can concentrate on minimizing the following expression:

$$\begin{aligned} H(E|XY) - H(E) \geq& h\left(\sum_{jk}\rho_{0jk}\right) - H(\{\rho_{ijk}\}) && \text{(VI.23)} \\ =& -\left(\sum_{jk}\rho_{0jk}\right)\log\left(\sum_{jk}\rho_{0jk}\right) - \left(\sum_{jk}\rho_{1jk}\right)\log\left(\sum_{jk}\rho_{1jk}\right) + \sum_{ijk}\rho_{ijk}\log\rho_{ijk} && \text{(VI.24)} \\ =& p_0\sum_{jk}\frac{\rho_{0jk}}{p_0}\log\frac{\rho_{0jk}}{p_0} + (1-p_0)\sum_{jk}\frac{\rho_{1jk}}{(1-p_0)}\log\frac{\rho_{1jk}}{(1-p_0)} && \text{(VI.25)} \\ =& -p_0 H\left(\left\{\frac{\rho_{0jk}}{p_0}\right\}\right) - (1-p_0)H\left(\left\{\frac{\rho_{1jk}}{(1-p_0)}\right\}\right), && \text{(VI.26)} \end{aligned}$$

where we abbreviated the probability $p_0 := \sum_{jk}\rho_{0jk}$. We now use the concavity of the Shannon entropy over probability distributions $\vec{u}$ and $\vec{v}$, i.e.

$$p_0 H(\vec{u}) + (1-p_0)H(\vec{v}) \leq H(p_0\vec{u} + (1-p_0)\vec{v}), \tag{VI.27}$$

to get

$$H(E|XY) - H(E) \geq -\, p_0 H\left(\left\{\frac{\rho_{0jk}}{p_0}\right\}\right) - (1-p_0) H\left(\left\{\frac{\rho_{1jk}}{(1-p_0)}\right\}\right) \tag{VI.28}$$

$$\geq -\, H\left(\{\rho_{0jk}+\rho_{1jk}\}\right). \tag{VI.29}$$

With the lower bound obtained in (VI.29), the optimization problem we have to solve is now the following:

$$\begin{aligned} &\max_{\{\rho_{ijk}\}} H\left(\{\rho_{0jk}+\rho_{1jk}\}\right) \\ &\text{sub. to } \frac{m^2}{16} \leq \sum_{jk} (\rho_{0jk}-\rho_{1jk})^2 \ ; \ \sum_{ijk} \rho_{ijk} = 1 \ ; \ \rho_{ijk} \geq 0, \end{aligned} \tag{VI.30}$$

where m is the observed MABK violation. Now notice that for every solution $\{\rho_{0jk}, \rho_{1jk}\}$ of the maximization problem, there exists another equivalent solution –i.e. that leads to the same value for $H\left(\{\rho_{0jk}+\rho_{1jk}\}\right)$– of the form $\{\rho'_{0jk} = \rho_{0jk}+\rho_{1jk}, \rho'_{1jk} = 0\}$. Therefore, we can restrict the optimization to the solutions of that form:

$$\begin{aligned} &\max_{\{\rho_{0jk}\}} H\left(\{\rho_{0jk}\}\right) \\ &\text{sub. to } \frac{m^2}{16} \leq \sum_{jk} \rho_{0jk}^2 \\ &\qquad\quad \sum_{jk} \rho_{0jk} = 1 \\ &\qquad\quad \rho_{000} \geq \rho_{001} \geq \rho_{010} \geq \rho_{011} \geq 0, \end{aligned} \tag{VI.31}$$

where we imposed the ordering of the eigenvalues without loss of generality, since the optimization problem is symmetric with respect to their permutations.

We have thus reduced the problem to the constrained maximization of $H\left(\{\rho_{0jk}\}\right)$, as described in (VI.31). In the following calculations, we rescale the function $H\left(\{\rho_{0jk}\}\right)$ by $\ln 2$, so that it is expressed in terms of natural logarithms instead of the logarithm in base 2. This simplifies the notation when computing its derivatives but does not change the solution of the optimization problem.

We use the Karush-Kuhn-Tucker multipliers method [78, 79] to identify necessary conditions for extremal points of the optimization problem in (VI.31). The Lagrangian for our maximization problem is then given by:

$$\begin{aligned} \mathcal{L}(\rho_{000}, \rho_{001}, \rho_{010}, \rho_{011}, u, v) =& H\left(\rho_{000}, \rho_{001}, \rho_{010}, \rho_{011}\right) + u\left(\rho_{000}^2 + \rho_{001}^2 + \rho_{010}^2 + \rho_{011}^2 - \frac{m^2}{16}\right) \\ &+ v\left(\rho_{000}+\rho_{001}+\rho_{010}+\rho_{011}-1\right) \end{aligned} \tag{VI.32}$$

The necessary conditions to have an extremal point are given by the solution of the following system:

$$\begin{cases} \nabla_{\rho_{0jk}} \mathcal{L} = 0 \\ \rho_{000}^2 + \rho_{001}^2 + \rho_{010}^2 + \rho_{011}^2 \geq \frac{m^2}{16} \\ \rho_{000}+\rho_{001}+\rho_{010}+\rho_{011} = 1 \\ u \geq 0 \\ u\left(\rho_{000}^2 + \rho_{001}^2 + \rho_{010}^2 + \rho_{011}^2 - \frac{m^2}{16}\right) = 0. \end{cases} \tag{VI.33}$$

The last equation in (VI.33) implies that either $u = 0$ or the inequality constraint holds with the equal sign. Let us first consider the case that $u = 0$ and compute the derivative of $\mathcal{L}$ with respect to ρ_{0jk} in the first equation of (VI.33):

$$\frac{\partial \mathcal{L}}{\partial \rho_{0jk}} = -\ln \rho_{0jk} + v - 1 = 0 \quad \forall\, \rho_{0jk}. \tag{VI.34}$$

Since the logarithm is a monotonic function, the set of equations in the last expression imply one of the following cases:

(a) $\rho_{000} = \rho_{001} = \rho_{010} = \rho_{011}$,

(b) $\rho_{000} = \rho_{001} = \rho_{010}$ and $\rho_{011} = 0$,

(c) $\rho_{000} = \rho_{001}$ and $\rho_{010} = \rho_{011} = 0$,

(d) $\rho_{001} = \rho_{010} = \rho_{011} = 0$.

where we accounted for the border conditions, i.e. when one or more ρ_{0jk} are equal to zero.

By combining the equality conditions with the constraint that ρ_{0jk} sum to one, we can easily obtain the solution of the system (VI.33) for each of the above cases. Note that the inequality constraint is still valid, therefore the derived solutions will only hold for certain values of m:

(a) $H(\{\rho_{0jk}\}) = 2$, valid for $m \leq 2$,

(b) $H(\{\rho_{0jk}\}) = \log 3$, valid for $m \leq 4/\sqrt{3}$

(c) $H(\{\rho_{0jk}\}) = 1$, valid for $m \leq 2\sqrt{2}$

(d) $H(\{\rho_{0jk}\}) = 0$, valid for $m \leq 4$.

The cases (a) and (d) are useless since the former is never valid in the range of interest for the observed violation (i.e. above the classical bound), while the latter leads to zero entropy, which is definitely not the solution of our maximization problem.

Let us consider now the case $u > 0$, which implies that the inequality constraint becomes an equality (the last equation in (VI.33) must be satisfied). We compute the derivatives in the first equation of (VI.33):

$$\frac{\partial \mathcal{L}}{\partial \rho_{0jk}} = 2\rho_{0jk} u - \ln \rho_{0jk} + v - 1 = 0 \qquad \forall\, \rho_{0jk}. \tag{VI.35}$$

Notice that the function $g(x) = ax - \ln x + b$ can have at most two roots (zero points), because

$$g'(x) = a - \frac{1}{x}, \tag{VI.36}$$

has at most a single root (zero point), corresponding to one extremum for $g(x)$. It follows that there can be at most a single $y \neq x$ such that $g(x) = g(y) = 0$. The potential critical points of the Lagrangian $\mathcal{L}$ are hence restricted to the following cases (remember we use the ordering $\rho_{000} \geq \rho_{001} \geq \rho_{010} \geq \rho_{011} \geq 0$)

(i) $\rho_{000} = \rho_{001} = \rho_{010} = \rho_{011}$,

(ii) $\rho_{000} = \rho_{001} = \rho_{010} > \rho_{011}$,

(iii) $\rho_{000} > \rho_{001} = \rho_{010} = \rho_{011}$,

(iv) $\rho_{000} = \rho_{001} > \rho_{010} = \rho_{011}$.

We again account for the border conditions, and analog conditions directly follow in case some ρ_{0jk} are zero:

(v) $\rho_{000} = \rho_{001} = \rho_{010}$ and $\rho_{011} = 0$,

(vi) $\rho_{000} = \rho_{001} > \rho_{010}$ and $\rho_{011} = 0$,

(vii) $\rho_{000} > \rho_{001} = \rho_{010}$ and $\rho_{011} = 0$,

(viii) $\rho_{000} > \rho_{001}$ and $\rho_{010} = \rho_{011} = 0$,

(ix) $\rho_{000} = \rho_{001}$ and $\rho_{010} = \rho_{011} = 0$,

(x) $\rho_{001} = \rho_{010} = \rho_{011} = 0$.

Note that in all the listed cases there are a maximum of two distinct eigenvalues, which are thus completely fixed by the two equality constraints. Moreover, we observe that the cases (i), (v), (ix) and (x) correspond to the already investigated cases (a), (b), (c) and (d), respectively.

Analysing the resulting entropy H as a function of the MABK violation m for each of the ten possible extremal points, we conclude that the maximum is achieved for the case (iii) for every value of m. In this case, the eigenvalues are fixed to:

$$\rho_{000} = \frac{1}{8}\left(2+\sqrt{3}\sqrt{m^2-4}\right) =: \nu_m \tag{VI.37}$$

$$\rho_{0jk} = \frac{(1-\nu_m)}{3} \quad (j,k) \neq (0,0). \tag{VI.38}$$

The solution of the optimization problem in (VI.31) then reads:

$$H\left(\{\rho_{0jk}\}\right) = H\left(\left\{\nu_m, \frac{1-\nu_m}{3}, \frac{1-\nu_m}{3}, \frac{1-\nu_m}{3}\right\}\right) \tag{VI.39}$$

The lower bound on the entropy difference (VI.29) is thus given by:

$$H(E|XY) - H(E) \geq -H\left(\left\{\nu_m, \frac{1-\nu_m}{3}, \frac{1-\nu_m}{3}, \frac{1-\nu_m}{3}\right\}\right) \tag{VI.40}$$

Finally we can lower bound the entropy of Alice and Bob's outcomes given Eve's quantum side information by

$$H(XY|E) = 2 + H(E|XY) - H(E) \geq 2 - H\left(\left\{\nu_m, \frac{1-\nu_m}{3}, \frac{1-\nu_m}{3}, \frac{1-\nu_m}{3}\right\}\right), \tag{VI.41}$$

with

$$\nu_m = \frac{1}{4} + \frac{\sqrt{3}}{8}\sqrt{m^2-4}. \tag{VI.42}$$

On the tightness of the bound:
Similarly to the bound on $H(X|E)$ (section V), we could identify a family of quantum states $\eta(\nu)$ defined as:

$$\eta(\nu) = \nu|\psi_{0,0,0}\rangle\langle\psi_{0,0,0}| + \frac{1-\nu}{3}\sum_{(j,k)\neq(0,0)}|\psi_{0,j,k}\rangle\langle\psi_{0,j,k}|, \tag{VI.43}$$

that attains the lower bound in (VI.41) for every observed violation m. Indeed, the conditional entropy $H(XY|E)_\eta(\nu_m)$ computed on the state $\eta(\nu_m)$, where ν_m is given by (VI.42), is equal to the r.h.s. of (VI.41).

The upper bound $\mathcal{M}_\eta^\uparrow$ on the MABK violation (V.2) relative to the family of states (VI.43) reads:

$$\mathcal{M}_\eta(\nu) = \frac{4}{\sqrt{3}}\sqrt{4\nu^2 - 2\nu + 1}, \tag{VI.44}$$

and for $\nu = \nu_m$ it reduces to:

$$\mathcal{M}_\eta^\uparrow(\nu_m) = m. \tag{VI.45}$$

Now, numerical computations suggest that the tightness conditions (75) of the MABK violation upper bound are in general not satisfied by the states $\eta(\nu)$. In other words, there exist no measurements that the parties can perform on $\eta(\nu)$ such that the violation of the MABK inequality reaches the value given by (VI.44). In particular, when $\nu = \nu_m$, there are no measurements such that the violation of value m is observed (due to Eq. VI.45).

Therefore, although the states $\eta(\nu_m)$ are such that their entropy attains the lower bound (VI.41) for a given observed violation m, they do not prove the tightness of the bound since they cannot yield a violation of value m.

The tightness of the lower bound in (VI.41) is still an open question.