

Heinrich-Heine-Universität Düsseldorf



Multipartite cryptographic protocols for quantum networks

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

Giacomo Carrara

from Como, Italy

Düsseldorf, October 2023

From the Institute for Theoretical Physics III
of 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: 19/12/2023

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, October 2023

Giacomo Carrara

Acknowledgements

Before diving into the fascinating world of quantum cryptography, I would like to take a moment to thank all the people that made all of this possible. Of course, I would need the same amount of pages as the thesis itself to properly thank everyone, but I will try to be concise.

First of all, I would like to thank my (unofficial) supervisor, Gláucia Murta, for helping me grow as a scientist during these 4 years, always giving me the best advice and scientific guidance I could have asked for, and my (official) supervisor and co-supervisor, Dagmar Bruß and Hermann Kampermann, for being the perfect group leaders and role models to aspire to as professors and scientists. I had the luck of having three amazing people guiding me in the process of becoming a scientist and I will always be grateful for that.

The fantastic environment I was lucky to work in was not only made possible by the group leaders, but also by the other PhD students and postdocs. I then thank all past and present colleagues, which it is safe to say they were friends more than colleagues: Giulio Gianfelici, Carlo Liorni and Federico Grasselli (the italian lineage that will fade away after I'm gone), Sarnava Datta, Lucas Tendick, Thomas Wagner, Julia Kunzelmann and Nikolai Wyderka (the old guard) Raphael Brieger, Lennart Bittel, Christopher Cedzich and Matthias Zipper (the other side of the corridor) including Juan Manuel Henning (the traitor) and Justus Neumann, Ghislain Coulter-de-Wit, Monika Mothsara, Yien Liang and Anton Trusheckin (the new deal). Thanks to all of you for all the discussions, some even scientific, and for the incredible time I had in these four years outside and inside the university, also thanks to you. In particular I would like to acknowledge the help of Federico Grasselli, Gláucia Murta, Justus Neumann and Nikolai Wyderka in proofreading this thesis. Many thanks also to the other members of the institute, Cornelia Glowacki, Jens Bremer and Cordula Hoffjan.

A thank goes also to the people that wait for me in Italy. In particular my mom and dad, Maria and Pier, who always supported me like the best parents that they are, my aunts and uncles, Betta, Kurt, Emilia, Silvia and Ubaldo and my cousin Edoardo. A special thank goes to Carlina and Emilio, my beloved grandparents, who were there for me for my whole life and, even though cannot be here for this achievement, I am sure would also be proud of me now. I would also like to thank all my friends outside the university, too many to single out individually, with a

special mention for Simone, whom I have known for literally 23 years now and never stopped enjoying the company since.

The most special thank is of course for the person who is always there for me and without whom none of this would be possible. Thank you Sara, for being the best person to have at my side and to be the person that, hopefully, will be with me for the rest of my life. Life that would be much more sad and empty without you.

Abstract

Among the many applications of quantum information processes, one of the most mature both from a theoretical and practical point of view is undoubtedly Quantum Key Distribution (QKD). QKD allows two parties, commonly referred to as Alice and Bob, to establish a secret, shared string of bits, called key, which they can use for secure communication. In a QKD protocol the parties exploit the unique features of quantum mechanical systems to guarantee security against possible attacks of a third malicious party, called Eve, even when Eve is given unlimited power.

This thesis is devoted to expanding the theoretical knowledge about fundamental and practical applications of quantum cryptography. In particular, with the perspective of building true quantum networks in the future, we focus on the extension of QKD to many users, namely Conference Key Agreement (CKA). CKA allows, by exploiting a shared quantum resource, an arbitrary number of parties to establish a common secret key used for secure shared communication.

Among the different CKA protocols, the most relevant of them require the strongest form of entanglement, called Genuine Multipartite Entanglement (GME). After a theoretical background, we try to relax these strong entanglement requirements and design more weakly entangled multipartite states that can be employed successfully in CKA protocols. Furthermore, we highlight an insightful connection between CKA and the theory of entanglement witnesses.

Then, we focus on a more practical application of CKA. We start from a bipartite protocol, namely Twin-Field QKD (TF-QKD), which has two major advantages over usual QKD protocols: it is well suited for long-distance communication and it requires only simple optical devices to be implemented. Our effort is then put into designing a novel CKA protocol that retains the same desirable properties.

Finally, we dive in the most adversarial scenario, namely the Device-Independent (DI) scenario, where all the parties' devices are untrusted and can be under Eve's control. In this scenario, we analyze how a task, which can be considered as a primitive to QKD, namely DI randomness expansion (DIRE), can be tackled with less-than-optimal resources. In particular we show how the parties can certify uniform randomness in the multipartite scenario using almost separable states.

Our works represent a significant step towards realistic, practical implementations of quantum cryptographic protocols with reduced resource requirements, paving the way for near-term implementations of quantum cryptographic tasks.

Zusammenfassung

Unter den vielen Anwendungen von Quanteninformationsprozessen gehört die Quantenschlüsselverteilung (Quantum Key Distribution, kurz QKD) sowohl aus theoretischer Sicht als auch aus praktischer Sicht zu den ausgereiftesten. QKD erlaubt es zwei Parteien, die für gewöhnlich als Alice und Bob bezeichnet werden, geheim eine gemeinsame Bitfolge zu erstellen, einen sogenannten Schlüssel, welchen sie dann für eine sichere Kommunikation verwenden können. In einem QKD-Protokoll werden die fundamentalen Eigenschaften der Quantenmechanik genutzt, die die Sicherheit der Kommunikation vor möglichen Angriffen einer dritten Partei, genannt Eve, gewährleistet, selbst wenn Eve alle Möglichkeiten zur Verfügung stünden.

Diese Arbeit widmet sich der Erweiterung der Theorie über grundlegende und praktische Anwendungen der Quantenkryptografie. Mit der Perspektive auf den Aufbau echter Quantennetze in der Zukunft, setzten wir den Schwerpunkt insbesondere auf die Erweiterung von QKD auf mehrere Benutzer, die sogenannte Conference Key Agreement (kurz CKA). CKA erlaubt es einer beliebigen Anzahl an Parteien unter der Verwendung einer geteilten Quantumressource einen gemeinsamen sicheren Schlüssel zu konstruieren, der für eine sicher gemeinsame Kommunikation genutzt werden kann.

Unter den verschiedenen CKA-Protokollen erfordern die relevantesten die stärkste Form der Verschränkung, genannt Genuine Multipartite Entanglement (kurz GME). Nachdem wir einen theoretischen Hintergrund eingeführt haben, versuchen wir diese starken Verschränkungsbedingungen zu lockern und weniger stark verschränkte Zustände zu konstruieren, die erfolgreich in CKA-Protokollen verwendet werden können. Des Weiteren zeigen wir eine Relation zwischen CKA und der Theorie der Verschränkungszeugen.

Anschließend werden wir die praktische Anwendung von CKA diskutieren. Wir beginnen dabei mit einem Zwei-Parteien-Protokoll, der sogenannten Twin-Field QKD (kurz TF-QKD), welche gegenüber herkömmlichen QKD-Protokollen zwei große Vorteile hat: Zu einem eignet es sich gut für Kommunikation über große Entfernungen und zum anderen werden für die Implementierung nur einfache optische Geräte benötigt. Wir stellen ein neues CKA-Protokoll vor, das die genannten Eigenschaften beinhaltet.

Zum Schluss befassen wir uns noch mit dem ungünstigsten Szenario, dem Device Independent (DI) Szenario, indem die Geräte aller Parteien nicht sicher sind und von Eve manipuliert werden können. In solch einem Szenario analysieren wir, wie eine bestimmte Aufgabe, nämlich die Device Independent Randomness Expansion (kurz DIRE), welche gleichzeitig auch als Vorstufe zur QKD gesehen werden kann, unter der Verwendung von nicht optimalen Ressourcen gelöst werden kann. Insbesondere zeigen wir, wie die Parteien in einem Szenario mit mehreren Parteien unter der Verwendung von fast separablen Zuständen einheitlich Zufälligkeit (uniform randomness) sicherstellen können.

Unsere Arbeit stellt einen wichtigen Schritt in Richtung realistischer und praktischer Anwendung von Quantenkryptografie mit reduzierten Bedingungen der Ressourcen, die den Weg für Implementierungen in naher Zukunft ebnet.

Contents

List of Figures	xiii
1. Introduction and motivation	1
2. Basics of Quantum Information Theory	3
2.1. Quantum mechanics' postulates	3
2.1.1. First postulate: vector states	3
2.1.2. Second postulate: state evolution	5
2.1.3. Third postulate: quantum measurement	6
2.2. Density operator formalism	8
2.3. Composite systems	10
2.3.1. Bipartite systems	10
2.3.2. Partial trace and purification	12
2.3.3. Multipartite systems	13
2.4. Quantum Operations	15
2.5. Qubit systems	17
2.5.1. Pauli operators and the Bloch sphere	17
2.5.2. The depolarizing channel	18
2.5.3. Bell states	19
3. Introduction to Quantum Key Distribution	21
3.1. Measures of uncertainty: entropies	21
3.1.1. Classical entropy	21
3.1.2. The von Neumann entropy	23
3.1.3. Conditional min- and max-entropy	25
3.1.4. Entropic uncertainty relation	27
3.2. Quantum Key Distribution protocols	28
3.2.1. Security of QKD	31
3.2.2. The BB84 protocol	34
4. Conference Key Agreement	39
4.1. Basics of Conference Key Agreement	39
4.1.1. The N-BB84 protocol	41
4.1.2. CKA with the W state	43

4.2. Requirements for Conference Key Agreement	45
4.2.1. Conference Key Agreement with biseparable states	45
4.2.2. Conference key rate as an entanglement witness	48
4.2.3. Biseparable states in the triangle network	49
5. Measurement-Device-Independent protocols	53
5.1. Introduction to MDI protocols	53
5.1.1. Introduction to quantum optics	54
5.1.2. Ideal MDI-QKD protocol	56
5.1.3. Overcoming fundamental limitation on the communication rate	58
5.1.4. Ideal MDI-CKA protocol	60
5.2. Practical protocols	63
5.2.1. Twin-Field QKD	63
5.2.2. Security proof and decoy-state method	66
5.2.3. Practical MDI-CKA protocol	68
5.2.4. Overcoming fundamental limitations in networks	71
6. Device-Independent randomness expansion	75
6.1. Device-Independent scenario	75
6.1.1. Bell inequalities	77
6.1.2. Multipartite DI scenario	80
6.2. Device-Independent Randomness Expansion	81
6.2.1. DIRE with partially entangled states	83
7. Overview of the results	87
8. Conclusions and Outlook	89
Bibliography	91
A. Proofs	101
B. Genuine multipartite entanglement is not a precondition for secure conference key agreement	105
C. Overcoming Fundamental Bounds on Quantum Conference Key Agreement	115

List of Figures

2.1. Schematic representation of the set of tripartite states	15
3.1. Schematic representation of PM- and EB-QKD protocols	30
4.1. Schematic representation of the considered class of CKA protocols	41
4.2. Asymptotic key rate of the N-BB84 protocol when employing the family of states in Eq. (4.13)	47
4.3. Depiction of the triangle network scenario.	50
5.1. Schematic representation of the TF-QKD protocol.	65
5.2. Schematic representation of the practical CKA protocol for $N = 4$	70
5.3. Asymptotic conference key rate of the practical CKA protocol as a function of the loss, compared with the single-message multicast bound.	72
6.1. Sketch of the DI scenario	76
6.2. Depiction of the set of correlations	78
6.3. Plot of the conditional min-entropy of the joint outcomes of parties A_2 and A_3 as a function of the Bell violation S_θ , for $N = 3$ and different θ . .	84
6.4. Plot of the conditional min-entropy of the joint outcomes of parties A_2 , A_3 and A_4 as a function of the Bell violation S_θ , for $N = 4$ and different θ .	85

Introduction and motivation

The need of concealing information is as old as civilization itself: the first testimony of ciphered text is a carved stone discovered in Egypt, dating back to 1900 BC. Cryptography is the discipline that studies ways to encrypt messages such that they can be shared between two or more parties without concerns about them being intercepted by other malicious parties. Throughout history many cryptographic methods have been developed, starting from ciphers used by the Greeks and Romans to exchange secret information during war, such as the famous *Caesar cipher*, all the way to modern cryptography used to make day-to-day communication secure.

The most desirable feature of an encryption scheme is *unconditional (or information-theoretical) security*, meaning that the message cannot be deciphered by malicious parties, even with the assumption of unlimited power and resources. Surprisingly, most encryption methods are not unconditionally secure: one famous historical example is the Vigenér cipher, which was believed to be secure for more than three centuries, before being cracked in the mid 19th century. Even modern cryptographic schemes are not information-theoretically secure. One notable example is the RSA protocol, used to encrypt all messages that we exchange daily, which is not unconditionally secure as it is based on the computational complexity of factorizing products of large prime numbers. In fact, even the most powerful computer currently available would take years to break the RSA protocol. However, it has already been shown that the advent of quantum computers will change that, with efficient algorithms capable of breaking the security of RSA encryption [Sho94] and thus jeopardizing the secrecy of all encrypted data.

One of the few information-theoretically secure encryption methods is the *Vernam cipher* [Ver26], or *one-time pad* encryption method. We will not go into details about this cipher, which has been shown to be secure by Claude Shannon in 1949 [Sha48]. This encryption scheme has, however, one crucial requirement: the parties that exchange the message must possess a shared *key*, i.e., a string of bits, which must be as long as the message, completely random and unknown to any malicious party. The task of encryption and decryption of a message thus reduces to the following problem: how can the parties share a random string of bits, without any leakage of information to any other (potentially malicious) party?

Quantum mechanics, with its intrinsic randomness and peculiar properties, provides an answer for this problem, in the form of *Quantum Key Distribution (QKD)*.

QKD schemes, in fact, exploit inherent properties of quantum mechanical systems to allow two or more parties to remotely establish a secret, random string of bits. The first QKD protocol was proposed in 1984 by Bennett and Brassard [BB84] and since then an enormous amount of effort has been put in developing new QKD schemes, exploiting a wide range of quantum resources for cryptographic purposes.

Furthermore, modern day applications of encryption schemes require more than just two users to exchange information, with many devices interacting throughout the whole world. It is thus of crucial importance to generalize QKD schemes, usually developed only for two users, to more complicated network scenarios. The task of sharing a common, secret key among many users is called *Conference Key Agreement (CKA)* and, once again, the properties of quantum mechanics can help to develop information-theoretically secure encryption schemes for network uses. This thesis is devoted to exploring and expanding the knowledge of such multi-user quantum encryption schemes, which will be crucial for the future building of a secure quantum internet network. Specifically, as increasingly more practical solutions for quantum encryption schemes are developed, it also increases the urge for reducing the resource requirements for such practical applications. In this thesis we will analyze the convoluted landscape of resources required for multipartite CKA protocols and design new methods and protocols to reduce the requirements to successfully perform quantum cryptographic tasks, in sight of near-term practical applications.

The thesis is structured as following: chapter 2 is devoted to the introduction of the fundamental theoretical concepts and tools required for the following chapters. In chapter 3 we introduce the basics of QKD, outlining all the fundamental elements of a QKD protocol and analyzing the first, most simple protocols in detail. In chapter 4 we extend the scenario to more parties, going in details of CKA and presenting the first original work, in which we investigate the resources needed for CKA protocols. Following the same line, in chapter 5, inspired by a practically implementable QKD protocol called *Twin-Field QKD*, we present an original CKA protocol, designed to be realizable with simple optical devices, paving the way for future quantum networks. Then, in chapter 6, we investigate an adversarial scenario where the parties do not need to trust their devices, called the *Device-Independent scenario*, and show how the parties can certify the randomness of their outcomes with limited resources. After a summary, given in chapter 7, of the published results, which can be found attached in Appendix B and C, we conclude and give an outlook of future possible research lines in chapter 8.

Basics of Quantum Information Theory

We begin the thesis with a basic overview of the fundamental concepts of quantum information theory that are needed as a foundation for the rest of the thesis. We start by introducing the basic postulates of quantum mechanics, in section 2.1. In section 2.2 we introduce the density operator formalism and review the postulates to adapt for this new formalism and extend the formalism to composite systems in section 2.3. We then introduce the quantum operations framework in section 2.4, to allow for a complete description of any possible quantum state evolution and finally we focus, in section 2.5, specifically on qubit systems, which are extensively utilized in the rest of the thesis. This chapter is based mainly on [NC00; Wil17].

2.1 Quantum mechanics' postulates

In this section we review the basic description of quantum mechanics, by reviewing the three fundamental postulates that allow for a complete and satisfactory description of any quantum system. Such description allows to characterize the properties of any quantum states, as well as to describe its evolution, interaction and the process of performing a measurement.

2.1.1 First postulate: vector states

The first necessity when describing a quantum system is to find a suitable description for the state of the system. In quantum mechanics, the state of a quantum system is described by a normalized vector $|\psi\rangle$ of a *Hilbert space* \mathcal{H} with dimension d . A Hilbert space is defined as a complete vector space equipped with an inner product. The vector $|\psi\rangle$ is usually called a "ket" vector and it completely characterizes the state of the quantum system. This notation, that is conventionally adopted in quantum mechanics and that we will utilize throughout the thesis, is called *Dirac notation*.

By definition, any Hilbert space is equipped with an inner product, i.e., an operation, linear in the second argument and antilinear in the first, that maps any two vectors $|\psi\rangle$ and $|\phi\rangle$ to a complex number, indicated by the notation $\langle\phi|\psi\rangle$, called "bra-ket" notation. If the inner product of two vectors is zero, the two vectors are

orthogonal. Moreover, the inner product induces a *norm* in the Hilbert space, defined as $\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle}$. The vectors that represent the state of quantum systems are thus normalized with respect to this norm, i.e., $\| |\psi\rangle \| = 1$, or, in other terms, $\langle \psi | \psi \rangle = 1$.

The Dirac notation allows us to see the inner product from another point of view: any vector $|\phi\rangle$ defines a linear map $\langle \phi |$ that maps any other vector $|\psi\rangle$ of the Hilbert space to a complex number through the inner product $\langle \phi | \psi \rangle$. This map is called the *dual vector* or "bra" vector (hence the "bra-ket" notation) and the space of dual vectors, i.e., the space of linear maps from \mathcal{H} to the complex numbers, is called *dual space* of \mathcal{H} and is indicated by \mathcal{H}^* .

Moreover, given two vectors $|\psi\rangle$ and $|\phi\rangle$ we can define, using the Dirac notation, the so-called *outer product* $|\psi\rangle\langle \phi |$. This notation is often indicated as "ket-bra" notation. Any outer product defines a linear operation from \mathcal{H} to itself. In fact, given any vector $|\gamma\rangle \in \mathcal{H}$ we can describe the operation that maps it to the vector $|\psi\rangle\langle \phi | \gamma \rangle$ (which is simply the vector $|\psi\rangle$ multiplied by the complex number $\langle \phi | \gamma \rangle$) by applying the outer product as $(|\psi\rangle\langle \phi |)|\gamma\rangle$. We can also consider linear combinations of outer products $\sum_i p_i |\psi_i\rangle\langle \phi_i |$. These linear combinations map any vector $|\gamma\rangle$ to the vector $\sum_i p_i |\psi_i\rangle\langle \phi_i | \gamma \rangle$, which is also a vector in \mathcal{H} due to its linearity. As a final note, the outer product $|\psi\rangle\langle \psi |$ is called *projector* on $|\psi\rangle$ because the associated linear operation projects any vector state onto the one-dimensional subspace spanned by $|\psi\rangle$.

To conclude the description of vector states we review the concept of an *orthonormal basis* for \mathcal{H} . A set of d vectors $\{|a_i\rangle\}_{i=1}^d$ is said to be an orthonormal basis for \mathcal{H} if it is a basis for \mathcal{H} , i.e., is a set of linearly independent vectors that span the whole vector space, and if all vectors in the set are orthonormal to each other, i.e., $\langle a_i | a_j \rangle = \delta_{i,j}$. Here $\delta_{i,j}$ is the *Kronecker delta*, with $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise. Given an orthonormal basis $\{|a_i\rangle\}_{i=1}^d$, any vector $|\psi\rangle \in \mathcal{H}$ can be written as $|\psi\rangle = \sum_{i=1}^d a_i |a_i\rangle$ where $a_i = \langle a_i | \psi \rangle$. It is thus possible to write

$$|\psi\rangle = \sum_{i=1}^d \langle a_i | \psi \rangle |a_i\rangle = \left(\sum_{i=1}^d |a_i\rangle\langle a_i | \right) |\psi\rangle, \quad (2.1)$$

which, in turn, implies

$$\sum_{i=1}^d |a_i\rangle\langle a_i | = \mathbf{1}_{\mathcal{H}}, \quad (2.2)$$

where $\mathbf{1}_{\mathcal{H}}$ is the identity operator. This important relation is known as *completeness relation* and is crucial in characterizing linear operators on the Hilbert space.

2.1.2 Second postulate: state evolution

The second necessary ingredient to characterize a quantum system is the description of the evolution of the system in time. In quantum mechanics, we describe the evolution of a state vector with *unitary operators*. Let us then first review the basics of algebraic theory of operators on Hilbert spaces.

We consider *linear operators* $\hat{A} : \mathcal{H} \rightarrow \mathcal{H}$. We first note that the completeness relation of Eq. (2.2) allows us to characterize any linear operator simply using inner and outer products. In fact, we can write, using two times the completeness relation,

$$\hat{A} = \mathbf{1}_{\mathcal{H}} \hat{A} \mathbf{1}_{\mathcal{H}} = \left(\sum_{i=1}^d |a_i\rangle \langle a_i| \right) \hat{A} \left(\sum_{j=1}^d |a_j\rangle \langle a_j| \right) = \sum_{i,j=1}^d \langle a_i | \hat{A} | a_j \rangle |a_i\rangle \langle a_j|. \quad (2.3)$$

We can thus associate to \hat{A} a matrix A that has as elements $A_{i,j}$ the quantities $\langle a_i | \hat{A} | a_j \rangle$. This is the *matrix representation* of \hat{A} with respect to the basis $\{|a_i\rangle\}_{i=1}^d$.

Given any linear operator \hat{A} there exists a unique linear operator \hat{A}^\dagger such that

$$\langle \phi | \hat{A} | \psi \rangle = (\langle \psi | \hat{A}^\dagger | \phi \rangle)^* \quad (2.4)$$

for any $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. The operator \hat{A}^\dagger is called *adjoint operator* of A . It follows straightforwardly that the matrix representation of \hat{A}^\dagger is $(A^*)^T$, i.e., the conjugate transpose of the matrix A . It can also easily be shown that $(\hat{A}\hat{B})^\dagger = \hat{B}^\dagger \hat{A}^\dagger$ and $(\hat{A}^\dagger)^\dagger = \hat{A}$. We say that a linear operator \hat{A} is *self-adjoint* or *Hermitian* if $\hat{A} = \hat{A}^\dagger$. The most important property of a Hermitian operator is that its eigenvalues are real and its eigenvectors form an orthonormal basis, allowing us to write it in its spectral decomposition as

$$\hat{A} = \sum_{i=1}^d a_i |a_i\rangle \langle a_i|, \quad (2.5)$$

where the set of eigenvectors $\{|a_i\rangle\}_{i=1}^d$, with respective eigenvalues a_i form an orthonormal basis of \mathcal{H} .

We are now ready to introduce the main ingredient to describe the time evolution of any quantum system, i.e., *unitary operators*. A linear operator \hat{U} is said to be unitary if $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \mathbf{1}_{\mathcal{H}}$. One can easily see that an operator is unitary if and only if its matrix representation in any basis is unitary, i.e., $UU^\dagger = \mathbf{1}_d$ where $\mathbf{1}_d$ is the d -dimensional identity matrix and $U^\dagger = (U^*)^T$ by definition. The most important property of unitary operators is that they preserve the inner product. In fact, we can write

$$\langle \psi | \phi \rangle = \langle \psi | \hat{U}^\dagger \hat{U} | \phi \rangle = \langle \psi' | \phi' \rangle, \quad (2.6)$$

where $|\psi'\rangle = \hat{U}|\psi\rangle$ and $|\phi'\rangle = \hat{U}|\phi\rangle$ and where $(\hat{A}|\psi\rangle)^\dagger = \langle\psi|\hat{A}^\dagger$. Since unitary operators preserve the inner product, one can show that they also transform orthonormal bases into other orthonormal bases. Thus, if we consider two orthonormal bases $\{|a_i\rangle\}_{i=1}^d$ and $\{|b_i\rangle\}_{i=1}^d$ we can write $|b_i\rangle = \hat{U}|a_i\rangle$ for some unitary operator \hat{U} .

As we anticipated at the beginning of the section, the evolution of a quantum state is described using unitary operators. More specifically, let us consider the state of a *closed* quantum system at time t_0 , namely $|\psi(t_0)\rangle$. The state of the system at time t_1 will be described as

$$|\psi(t_1)\rangle = \hat{U}(t_0, t_1)|\psi(t_0)\rangle. \quad (2.7)$$

We remark that this postulate is valid only for closed systems, i.e., systems that are not interacting with other systems. Even though this condition is never fulfilled in realistic scenarios, there are many systems that are closed (whose time evolution is thus unitary) to a good approximation.

Eq. (2.7) describes the discrete evolution of quantum states. If we instead consider *continuous evolution* of a quantum state $|\psi(t)\rangle$, we need to use the *Schrödinger equation*

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = \hat{H}|\psi(t)\rangle, \quad (2.8)$$

where \hbar is the *Planck constant* and \hat{H} is a fixed Hermitian operator called *Hamiltonian* of the system. In the case where the Hamiltonian does not depend itself on time, which is the most commonly considered scenario, we can see the connection between the continuous and discrete evolution. In fact, solving explicitly the Schrödinger equation for times t_0 and t_1 yields the result

$$|\psi(t_1)\rangle = e^{-\frac{i(t_1-t_0)\hat{H}}{\hbar}}|\psi(t_0)\rangle, \quad (2.9)$$

which is simply Eq. (2.7) with $U(t_1, t_0) := e^{-\frac{i(t_1-t_0)\hat{H}}{\hbar}}$. To conclude, we remark that it can be shown that any operator in the form $\hat{U} = e^{i\hat{K}}$, with \hat{K} Hermitian, is unitary, thus ensuring that $U(t_1, t_0)$ is unitary, recovering the description of the discrete evolution of a quantum state.

2.1.3 Third postulate: quantum measurement

Lastly, we need to characterize the measurement process in quantum mechanics, i.e., the act of extracting information from a system and how it changes the system itself. Clearly, since the measurement operation requires interaction with the system, its evolution cannot be unitary, as described in the previous section. Let us first

introduce some important concepts of linear algebra that will be crucial to describe the measurement process.

Let us first introduce an important class of operators called *projectors*. A linear Hermitian operator \hat{P} is called a *projector* if, given an orthonormal basis $\{|a_i\rangle\}_{i=1}^d$, it can be written as

$$\hat{P} = \sum_{i \in \mathcal{S}} |a_i\rangle\langle a_i|, \quad (2.10)$$

where the index i runs over a subset \mathcal{S} of cardinality k of the d indices. An operator in this form is called a projector because it projects any vector of the Hilbert space onto the k -dimensional subspace of \mathcal{H} spanned by the vectors $\{|a_i\rangle\}_{i \in \mathcal{S}}$. Since any operator $|a_i\rangle\langle a_i|$ is Hermitian also \hat{P} is Hermitian. Moreover, it can be seen that $\hat{P}^2 = \hat{P}$.

Finally, we define a crucial quantity that we will use throughout the whole thesis. We define the *trace* of an operator \hat{A} as

$$\text{Tr}[\hat{A}] = \sum_{i=1}^d \langle a_i | \hat{A} | a_i \rangle, \quad (2.11)$$

where, again, $\{|a_i\rangle\}_{i=1}^d$ is an orthonormal basis of \mathcal{H} . Since changing bases is achieved with unitary transformations, we can write the following:

$$\begin{aligned} \text{Tr}[\hat{A}] &= \sum_{i=1}^d \langle a_i | \hat{A} | a_i \rangle = \sum_{i=1}^d \langle b_i | \hat{U}^\dagger \hat{A} \hat{U} | b_i \rangle \\ &= \text{Tr}[\hat{U}^\dagger \hat{A} \hat{U}] = \text{Tr}[\hat{A} \hat{U}^\dagger \hat{U}] = \text{Tr}[\hat{A}], \end{aligned} \quad (2.12)$$

where we used the fact that the trace of product of operators is invariant under cyclic permutations and that, from the definition of unitary operator, $\hat{U} \hat{U}^\dagger = \hat{U}^\dagger \hat{U} = \mathbf{1}_{\mathcal{H}}$. Eq. (2.12) tells us that the trace is independent on the basis chosen to calculate it.

We are now ready to provide the mathematical description of quantum measurements. A measurement on a quantum system, whose states are described by vectors of the Hilbert space \mathcal{H} , is, in fact, described by a collection $\{\hat{M}_i\}_{i=1}^m$ of linear operators on the Hilbert space, called *measurement operators*. Each operator \hat{M}_i is associated with the i -th outcome of the measurement. We remark that no assumption is made on the quantity of available outcomes m . In quantum mechanics, since the outcomes of the measurements are not deterministic, the most important quantity is the probability of obtaining a certain outcome i , when performing the measurement described by the operators $\{\hat{M}_i\}_{i=1}^m$ on a state $|\psi\rangle$. This quantity is given by the so-called *Born rule*, i.e.,

$$p(i) = \langle \psi | \hat{M}_i^\dagger \hat{M}_i | \psi \rangle. \quad (2.13)$$

The state of the system is also changed by the measurement process. We describe the state of the system after the measurement as

$$|\psi_i\rangle = \frac{\hat{M}_i|\psi\rangle}{\sqrt{p(i)}}, \quad (2.14)$$

where the denominator serves as normalization. Finally, since each $p(i)$ is a probability, it must be positive, which in turn implies

$$\hat{M}_i^\dagger \hat{M}_i \geq 0 \quad \forall i, \quad (2.15)$$

where we define an operator \hat{A} to be positive if $\langle\psi|\hat{A}|\psi\rangle \geq 0 \quad \forall |\psi\rangle \in \mathcal{H}$. Moreover, since all $p(i)$ form a probability distribution, it must hold $\sum_i p(i) = 1$, which, in turn, implies

$$\sum_{i=1}^m \hat{M}_i^\dagger \hat{M}_i = \mathbf{1}_{\mathcal{H}}, \quad (2.16)$$

which is an equivalent formulation of the completeness relation.

2.2 Density operator formalism

The postulates presented in the previous section provide an exhaustive description of a quantum system, as well as its interactions and readout, provided that we possess full knowledge of the vector state $|\psi\rangle$ describing the system. However, sometimes our knowledge on the state of a quantum system restricts to an ensemble of vector states with different occurring probability. In this case, to describe the state of a quantum system, we resort to the *density operator* formalism.

Suppose that the state of a quantum system is described by an ensemble of vector states $\{|\psi_i\rangle\}_{i=1}^k$, each occurring with probability p_i . The state of the system is then said to be a *mixed state* and is described by the *density operator*

$$\rho = \sum_{i=1}^k p_i |\psi_i\rangle\langle\psi_i|. \quad (2.17)$$

We note that the matrix representation of the operator ρ is called *density matrix*. From Eq. (2.17), due to the normalization and positivity of the probability distribution p_i , we straightforwardly have that any density operator must be positive and $\text{Tr}[\rho] = 1$.

If the state of the system is described by a single state vector $|\psi\rangle$ we call it a *pure state* and its density operator is the projector $\rho = |\psi\rangle\langle\psi|$. We finally note that for pure states, we have $\rho^2 = \rho$ and thus $\text{Tr}[\rho^2] = \text{Tr}[\rho] = 1$. It is straightforward to see that

for mixed states $\text{Tr}[\rho^2] < 1$, giving us a simple criterion to determine whether a state is pure or mixed just from the density operator: if the quantity $\text{Tr}[\rho^2]$, called *purity*, is less than one, then the state is straightforwardly mixed. Moreover, it is possible to show that, given a Hilbert space of dimension d , the minimal purity achievable by any density operator on the Hilbert space is $\text{Tr}[\rho^2] = \frac{1}{d}$ and it is achieved by the so-called *maximally mixed state* $\rho = \frac{1}{d}\mathbf{1}$.

To provide a full description of a quantum system in a mixed state it is now necessary to reformulate all postulates of quantum mechanics in the density operator formalism. The three postulates given in the previous section for pure states are then reformulated as following:

Postulate 2.2.1. *The state of a quantum system is described by a positive operator with unit trace ρ , called density operator, acting on a Hilbert space \mathcal{H} .*

Postulate 2.2.2. *The time evolution of a closed quantum system is described by a unitary operator $\hat{U}(t)$, which evolves any initial state ρ_0 according to*

$$\rho_t = \hat{U}(t)\rho_0\hat{U}^\dagger(t). \quad (2.18)$$

Postulate 2.2.3. *The measurement on a quantum system is described by a collection of measurement operators $\{\hat{M}_i\}_{i=1}^m$, that satisfy $\sum_{i=1}^m \hat{M}_i^\dagger \hat{M}_i = \mathbf{1}$ and $\hat{M}_i^\dagger \hat{M}_i \geq 0 \forall i$, each corresponding to one of the m possible outcomes of the measurement. The measurement statistics is determined by the so-called Born rule*

$$p(i) = \text{Tr} \left[\hat{M}_i^\dagger \hat{M}_i \rho \right], \quad (2.19)$$

and the state after the measurement is given by

$$\rho_i = \frac{\hat{M}_i \rho \hat{M}_i^\dagger}{\sqrt{p(i)}}. \quad (2.20)$$

Finally, we will introduce an alternative formalism for quantum measurements that can be adopted when we are interested only in the measurement statistic and not in the post-measurement state. We start by defining a Positive Operator-Valued Measure (POVM) as a collection of positive operators $\{\hat{E}_i\}_{i=1}^m$, with $\sum_{i=1}^m \hat{E}_i = \mathbf{1}_{\mathcal{H}}$, called *POVM effects*. Once again each POVM effect represents one of the possible outcomes of the measurement, which occur with probability

$$p(i) = \text{Tr} \left[\hat{E}_i \rho \right]. \quad (2.21)$$

It is immediate to see that a POVM alone does not allow for a unique definition of the measurement operators of Postulate 2.2.3. In fact, we can define $\hat{M}_i = \sqrt{\hat{E}_i}$ but

this definition is not unique as also $\hat{M}'_i = \hat{U} \sqrt{\hat{E}_i}$, with \hat{U} being any unitary operator, also give rise to the same POVM effect. As a consequence, the POVM effects do not give us any information about the post-measurement state.

An interesting special case of POVMs is given by *projective measurements*, where the POVM is composed by projectors satisfying the completeness relation. In this case, as we have $\sqrt{\hat{E}_i} = \hat{M}_i = \hat{P}_i$, with all the operators being Hermitian, the description of the quantum measurement is significantly simplified. Finally, if all projectors are rank-one, meaning that $\hat{P}_i = |a_i\rangle\langle a_i| \forall i$, we call the measurement a *von Neumann measurement*.

2.3 Composite systems

So far the postulates we introduced provide an exhaustive description of single systems. However, the mathematical structure of Hilbert spaces allows for a natural extension of this description when dealing with multiple systems, giving rise to one of the most striking features of quantum mechanics, that is *entanglement*. This section is based on [GT09; Hor+09]

2.3.1 Bipartite systems

We start with the simplest case of two different systems, labelled by A and B , whose vector states belong to two Hilbert spaces \mathcal{H}_A and \mathcal{H}_B . We now postulate that the vector space of the composite system is $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, where \otimes indicates the *tensor product* of Hilbert spaces. This tensor product structure allows us to define one of the most important properties of states in quantum mechanics, that is *entanglement*.

We start by considering pure states. We will, from now on, imagine that the systems are controlled by two parties, namely Alice and Bob. A pure state $|\psi_{AB}\rangle \in \mathcal{H}_{AB}$ is called a *product state* if it can be written as $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, where $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$ and, again, \otimes represents the tensor product of vectors. Physically, a product state represents the situation where the states of the two subsystems are prepared by the parties independently from one another, without any type of classical or non-classical interaction between the two systems. The definition extends to mixed states straightforwardly: a mixed state ρ_{AB} , where ρ_{AB} is a density operator acting on \mathcal{H}_{AB} , is in a product state if $\rho_{AB} = \rho_A \otimes \rho_B$, where ρ_A and ρ_B are density operators acting on \mathcal{H}_A and \mathcal{H}_B , respectively.

We could, however, allow Alice and Bob to use classical communication to agree on preparing locally certain sets of (possibly mixed) states $\{\rho_A^{(i)}\}_{i=1}^m$ and $\{\rho_B^{(i)}\}_{i=1}^m$,

respectively, according to a shared probability distribution p_i . In this scenario the state of the composite system is defined as following:

Definition 2.3.1 (Separable state). *A quantum state ρ_{AB} on \mathcal{H}_{AB} is called separable if it is in the form*

$$\rho_{AB} = \sum_{i=1}^m p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad (2.22)$$

where $\rho_A^{(i)}$ and $\rho_B^{(i)}$ are density operators acting on \mathcal{H}_A and \mathcal{H}_B , respectively.

A separable state still exhibit local behavior, since the two subsystems are independent from one another apart from the shared probability distribution p_i . As a final note, we remark that the set of separable states is a convex set, meaning that convex combinations of separable states are still separable.

However, not all states on \mathcal{H}_{AB} are separable states. We can thus define the following important property of a quantum bipartite state:

Definition 2.3.2 (Entangled state). *A state ρ_{AB} on \mathcal{H}_{AB} is called entangled if it is not separable, i.e., if it cannot be prepared locally with classical communication.*

Entangled states are the key ingredient in many quantum information applications, since, as we will see, entangled state exhibit a strong non-local behavior. We note that identifying entanglement is not an easy task: given a generic mixed quantum state ρ_{AB} , it is not immediate to tell whether it is entangled or separable. Among the many techniques developed [GT09], we will present one of the most relevant ones, that exploits the convexity of the set of separable states. Let us start with the following definition:

Definition 2.3.3 (Entanglement witness). *Given an entangled state ρ_{AB} , an entanglement witness is a Hermitian operator \hat{W} such that*

$$\text{Tr}[\hat{W}\sigma] \geq 0, \quad (2.23)$$

for all separable states σ and

$$\text{Tr}[\hat{W}\rho_{AB}] < 0. \quad (2.24)$$

The definition is based on the fact that a convex set can be separated from its complement with an hyperplane, represented in this case by the equation $\text{Tr}[\hat{W}\rho] = 0$. The operator \hat{W} thus separates the convex set of separable states from a subset of entangled states, which, by definition, must contain at least one state. Although the idea is quite simple and elegant, in practice finding a proper entanglement witness is not a trivial task and usually entanglement witnesses are tailored for specific states.

2.3.2 Partial trace and purification

In the previous section we presented a description of how composite systems are treated in quantum mechanics. However, one important tool is missing from the description of composite systems, i.e., a way to treat the states of the subsystems of a composite state. We start by introducing the concept of *partial trace*.

Given the composite state ρ_{AB} on \mathcal{H}_{AB} , it can be written, in its matrix representation, as

$$\rho_{AB} = \sum_{i,j,m,n} p_{i,j,m,n} |a_i\rangle\langle a_j| \otimes |b_m\rangle\langle b_n|, \quad (2.25)$$

where $\{|a_i\rangle\}_{i=1}^{d_A}$ and $\{|b_m\rangle\}_{m=1}^{d_B}$ are orthonormal bases for \mathcal{H}_A and \mathcal{H}_B , respectively, and where $p_{i,j,m,n}$ is the matrix element $\langle a_i| \otimes \langle b_m| \rho_{AB} |b_n\rangle \otimes |a_j\rangle$. We define the *partial trace* of ρ_{AB} on subsystem B as the linear map

$$\text{Tr}_B[\rho_{AB}] = \sum_{i,j,m,n} p_{i,j,m,n} |a_i\rangle\langle a_j| \cdot \text{Tr}[|b_m\rangle\langle b_n|] = \sum_{i,j,m,n} p_{i,j,m,n} \langle b_m|b_n\rangle |a_i\rangle\langle a_j|, \quad (2.26)$$

where Tr indicates the usual trace defined in Eq. (2.11). A similar definition can be given for the partial trace on subsystem A. The partial trace provides a natural tool to deal with subsystem of a composite system. In fact, we can give the following definition:

Definition 2.3.4 (Reduced density operator). *Let us consider the state ρ_{AB} on \mathcal{H}_{AB} . The description of the state of the system of Alice is given by the reduced density operator*

$$\rho_A = \text{Tr}_B[\rho_{AB}], \quad (2.27)$$

where Tr_B indicates the partial trace over Bob's subsystem.

The use of the partial trace to treat subsystems of composite systems is justified by the fact that it is the unique operation that gives rise to the correct measurement statistics when making measurements on a subsystem.

Related to the partial trace, we introduce another important procedure that we will extensively use throughout the whole thesis called *purification* procedure. Let us consider a mixed state ρ_A of Alice's subsystem. It is always possible to introduce a second system, labelled by E, and define a pure state $|\psi_{AE}\rangle \in \mathcal{H}_{AE}$ with $\mathcal{H}_{AE} = \mathcal{H}_A \otimes \mathcal{H}_E$, such that

$$\rho_A = \text{Tr}_E[|\psi_{AE}\rangle\langle\psi_{AE}|]. \quad (2.28)$$

This purification procedure can be done for any mixed state ρ_A , and we will show it by explicitly constructing the purifying state. We can, in fact, write the state ρ_A

in its spectral decomposition as $\rho_A = \sum_{i=1}^d p_i |\psi_A^{(i)}\rangle\langle\psi_A^{(i)}|$. We now fix the second system to have the same vector space as A , and define the following pure state of the composite system

$$|\psi_{AE}\rangle = \sum_{i=1}^d \sqrt{p_i} |\psi_A^{(i)}\rangle \otimes |\psi_E^{(i)}\rangle. \quad (2.29)$$

We remark that no assumption has been made for the state ρ_A . Now it is straightforward to see that

$$\begin{aligned} \text{Tr}_E [|\psi_{AE}\rangle\langle\psi_{AE}|] &= \sum_{i,j=1}^d \sqrt{p_i p_j} |\psi_A^{(i)}\rangle\langle\psi_A^{(j)}| \cdot \text{Tr} [|\psi_E^{(i)}\rangle\langle\psi_E^{(j)}|] \\ &= \sum_{i,j=1}^d \sqrt{p_i p_j} |\psi_A^{(i)}\rangle\langle\psi_A^{(j)}| \delta_{i,j} = \sum_{i=1}^d p_i |\psi_A^{(i)}\rangle\langle\psi_A^{(i)}| \\ &= \rho_A, \end{aligned} \quad (2.30)$$

meaning that $|\psi_{AE}\rangle$ is a purification of ρ_A .

2.3.3 Multipartite systems

So far we have considered only bipartite composite systems, but the tensor product structure allows for a straightforward generalization to any number of subsystems, or, in other words, parties. However, the structure of multipartite entanglement is much richer and more intricate than the bipartite one and it is therefore worth presenting in detail.

Let us now consider the scenario of a system composed of N subsystem, each controlled by a different party labelled B_1, \dots, B_N and named Bob₁, ..., Bob_N. As anticipated, the tensor product structure of the vector space of the composite system directly generalizes from the bipartite scenario: the vector space of the composite system will thus be $\mathcal{H}_{B_1, \dots, B_N} = \mathcal{H}_{B_1} \otimes \dots \otimes \mathcal{H}_{B_N}$. As for bipartite separable states, we can define a class of states that can be prepared locally by the parties with, at most, shared randomness and classical communication:

Definition 2.3.5 (Fully separable states). *Consider a state ρ_{B_1, \dots, B_N} on $\mathcal{H}_{B_1, \dots, B_N}$. The state is called fully separable if it can be written as*

$$\rho_{B_1, \dots, B_N} = \sum_i p_i \rho_{B_1}^{(i)} \otimes \rho_{B_2}^{(i)} \otimes \dots \otimes \rho_{B_N}^{(i)}, \quad (2.31)$$

where $\rho_{B_k}^{(i)}$ are states on $\mathcal{H}_{B_k} \forall k$.

As we already pointed out, fully separable states are the equivalent of separable states in the bipartite scenario, as they can be prepared locally by the parties with,

at most, classical communication between the parties. However, when introducing multipartite entanglement a richer structure than the simple entangled/separable structure of the bipartite scenario arises. Let us define \mathcal{S} to be a subset of the parties and $\bar{\mathcal{S}}$ the complement. A state can be *separable with respect to the fixed partition* $\mathcal{S}\setminus\bar{\mathcal{S}}$ if it is in the form

$$\rho_{B_1, \dots, B_N} = \sum_i p_i \rho_{\mathcal{S}}^{(i)} \otimes \rho_{\bar{\mathcal{S}}}^{(i)}, \quad (2.32)$$

where $\rho_{\mathcal{S}}^{(i)}$ and $\rho_{\bar{\mathcal{S}}}^{(i)}$ are states shared by the parties in \mathcal{S} and $\bar{\mathcal{S}}$, respectively. However, we can still imagine a scenario where the parties can prepare different states which are separable with respect to different partitions, according to a shared probability distribution. In this scenario, we define the following class of multipartite states:

Definition 2.3.6 (Biseparable states). *Consider a state $\rho_{B_1 \dots B_N}$ on $\mathcal{H}_{B_1, \dots, B_N}$. The state is called biseparable if it is in the form*

$$\rho_{B_1, \dots, B_N} = \sum_{\mathcal{S}_\alpha} \sum_i p_{\mathcal{S}_\alpha}^{(i)} \rho_{\mathcal{S}_\alpha}^{(i)} \otimes \rho_{\bar{\mathcal{S}}_\alpha}^{(i)}, \quad (2.33)$$

where the first sum runs over all possible partitions of the parties.

Biseparable states are convex combinations of states that are separable with respect to (possibly) different partitions of the parties. This implies that there exist states that are biseparable yet not separable with respect to any fixed partition of the parties. We can now define the class of most strongly entangled states, that are the *Genuinely Multipartite Entangled (GME) states*.

Definition 2.3.7 (GME states). *Consider a state $\rho_{B_1 \dots B_N}$ on $\mathcal{H}_{B_1, \dots, B_N}$. The state is called Genuinely Multipartite Entangled (GME) if it is not biseparable.*

GME states are of the utmost importance, as, since they contain the strongest form of entanglement, they are the most commonly used in multipartite quantum information tasks. One example is the so-called *GHZ state* [GHZ07], defined as

$$|GHZ\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes N} + |1\rangle^{\otimes N} \right), \quad (2.34)$$

and whose strong correlations are exploited in many quantum information tasks. The intricate entanglement structure of multipartite states still allows for entanglement detection with linear witnesses, as shown in section 2.3.1: it is possible, e.g., to rule out fully separable states or states that are separable with respect to a fixed partition with entanglement witnesses, as they are convex sets. To better illustrate our point, in Figure 2.1, taken from [Car+21], we give a schematic representation of the set of tripartite states. An important remark is that the red set in Figure 2.1, i.e., the set of

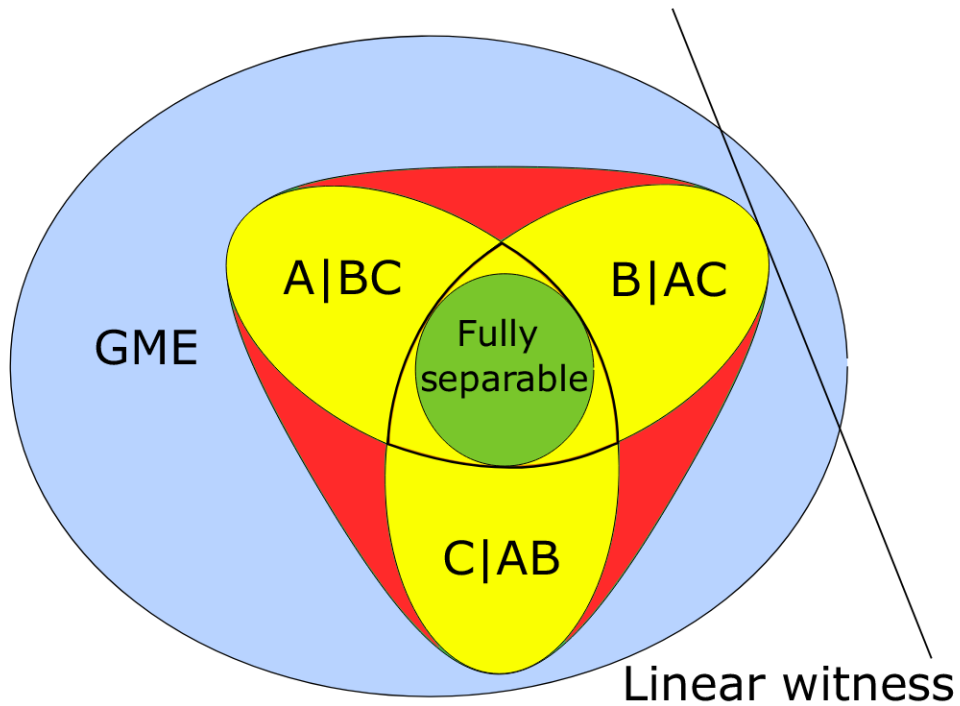


Fig. 2.1.: Schematic representation of the set of tripartite states. In light blue (outer set) is represented the set of GME states. In red (dark grey area) is highlighted the set of biseparable states that are not separable with respect to any fixed partition, whereas in yellow (light grey) are represented the sets of states that are separable with respect to a fixed partition. In the middle, in green, is represented the set of fully separable states. A linear witness defines a hyperplane in the space of states.

states that are biseparable but not separable with respect to any fixed partition, is not convex, thus such states are not detectable with linear entanglement witnesses.

2.4 Quantum Operations

In this section we introduce an alternative formalism to describe operations on quantum states, which also encompasses the description of both Postulate 2.2.2 and Postulate 2.2.3, providing useful tools for the description of many quantum information processes.

We start by introducing the concept of a *quantum operation*, that is a map \mathcal{E} that transforms a quantum state ρ acting on a Hilbert space \mathcal{H}_A in another quantum state $\mathcal{E}(\rho)$ acting on a possibly different Hilbert space \mathcal{H}'_A . In order for this operation to be physically meaningful, we need require the following properties:

Property 2.4.1. The map \mathcal{E} must preserve the hermiticity and positivity of ρ , i.e., $\mathcal{E}(\rho)$ must be Hermitian and positive $\forall \rho$ acting on \mathcal{H} . Moreover, it must be trace non-increasing, i.e., $0 \leq \text{Tr}[\mathcal{E}(\rho)] \leq 1$.

Property 2.4.2. The map \mathcal{E} must be convex-linear, i.e.,

$$\mathcal{E}\left(\sum_i p_i \rho^{(i)}\right) = \sum_i p_i \mathcal{E}\left(\rho^{(i)}\right), \quad (2.35)$$

for any probability distribution p_i , with $p_i \geq 0 \forall i$ and $\sum_i p_i = 1$.

Property 2.4.3. The map \mathcal{E} must be completely positive, i.e., the map must be positive also on subsystems of composite systems. In other terms, given the original Hilbert space \mathcal{H}_A , if we define any other Hilbert space \mathcal{H}_E it must hold

$$\mathcal{E} \otimes \mathbf{1}_E(\rho_{AE}) \geq 0, \quad (2.36)$$

for any auxiliary Hilbert space \mathcal{H}_E and any composite state ρ_{AE} acting on $\mathcal{H}_A \otimes \mathcal{H}_E$.

We note that the trace non-increasing property is a relaxation with respect to the natural choice of the map to be trace preserving, i.e., $\text{Tr}[\mathcal{E}(\rho)] = 1$. This relaxation however allows us to include the measurement operations in this framework. In particular, the quantum operations that are trace preserving are called *quantum channels*. The final property, that is complete positivity, is the least trivial property to be verified since there are even simple examples of maps that are positive but not completely positive.

One such example is the *transposition* map. In general, the transposition can be defined for any operator \hat{A} as the conjugate of the adjoint of \hat{A} , i.e., $\hat{A}^T = (\hat{A}^\dagger)^*$. If we write the matrix representation of our operator in some basis, i.e., $\hat{A} = \sum_{i,j} A_{i,j} |a_i\rangle\langle a_j|$ the transpose of \hat{A} is written as

$$\hat{A}^T = \sum_{i,j} A_{i,j} |a_j\rangle\langle a_i| = \sum_{i,j} A_{j,i} |a_i\rangle\langle a_j|. \quad (2.37)$$

It is straightforward to see that the transpose does not change the diagonal elements of an operator nor its eigenvalues, and thus it is trace preserving and positive. However, it is also possible to show that the transposition map is not a quantum operation as it can be shown that is not completely positive.

An important and elegant characterization of quantum operations is given in the following Theorem:

Theorem 1. A map \mathcal{E} is a quantum operation, i.e., it satisfies Properties 2.4.1, 2.4.2 and 2.4.3, **if and only if** there exists a set of operators $\{\hat{K}_i\}$, with $\sum_i \hat{K}_i^\dagger \hat{K}_i \leq \mathbf{1}$, called *Kraus operators*, such that

$$\mathcal{E}(\rho) = \sum_i \hat{K}_i \rho \hat{K}_i^\dagger. \quad (2.38)$$

Moreover, the number of Kraus operators \hat{K}_i is upper bounded by d^2 , with d being the dimension of the Hilbert space of the initial state ρ .

We will omit the proof of the Theorem, which can be found in [NC00]. The Theorem elegantly generalizes the unitary description of the evolution of a quantum state to any quantum operation.

2.5 Qubit systems

In this section, and throughout most of this thesis, we will focus on a specific type of quantum systems called quantum bits or *qubits*. A qubit system is any two-level system, including, for example, the polarization state of a photon or the state of spin- $\frac{1}{2}$ particles. The vector space of a qubit system is represented by a two-dimensional Hilbert space \mathcal{H}_2 spanned by the two possible states of the system that we will call $\{|0\rangle, |1\rangle\}$, and that form the so-called *computational basis*. Therefore, any pure state of the qubit system can be written, in the computational basis, as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$.

2.5.1 Pauli operators and the Bloch sphere

We now introduce a set of operators that are crucial in the description of qubits, called *Pauli operators*. Pauli operators, indicated by $\hat{\sigma}_X$, $\hat{\sigma}_Z$ and $\hat{\sigma}_Y$, or alternatively by \hat{X} , \hat{Z} and \hat{Y} , are defined, in their matrix representation in the computational basis, as

$$\hat{\sigma}_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \hat{\sigma}_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (2.39)$$

It is straightforward to see that the Pauli operators are Hermitian, traceless, have eigenvalues $+1$ and -1 and square to the identity. Pauli operators transform the computational basis according to

$$\hat{X}|a\rangle = |\bar{a}\rangle, \quad \hat{Z}|a\rangle = (-1)^a|a\rangle, \quad \hat{Y}|a\rangle = i(-1)^a|\bar{a}\rangle, \quad (2.40)$$

where $a = \{0, 1\}$ and \bar{a} indicates the bit flip of a . It is thus clear that the eigenvectors of the Pauli \hat{Z} operator are the elements of the computational basis, thus also sometimes called the Z -basis. Furthermore, the eigenvectors of \hat{X} and \hat{Y} , are

$$\left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}, \quad \left\{ \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\}. \quad (2.41)$$

Both sets of eigenstates form a basis for \mathcal{H}_2 , called X -basis and Y -basis, also denoted as $\{|+\rangle, |-\rangle\}$ and $\{|R\rangle, |L\rangle\}$, respectively.

Pauli operators have a fundamental role in the characterization of mixed states of qubits. As a matter of fact, one can write any density operator on \mathcal{H}_2 as

$$\rho = \frac{\mathbf{1}_{\mathcal{H}_2} + \vec{r} \cdot \vec{\sigma}}{2}, \quad (2.42)$$

where we defined $\vec{\sigma} = (\hat{\sigma}_X, \hat{\sigma}_Z, \hat{\sigma}_Y)^T$ and where \vec{r} is a real, 3-dimensional vector with $\|\vec{r}\| \leq 1$. Since any state ρ is uniquely determined by the vector \vec{r} , we can identify the set of qubit states with the unit sphere in the 3-dimensional real vector space, which is called the *Bloch sphere*. Most properties of the state ρ can be directly inferred from the vector \vec{r} : for example, the purity of ρ can be written as

$$\text{Tr}[\rho^2] = \frac{1 + \|\vec{r}\|^2}{2}. \quad (2.43)$$

Therefore, all pure states lie on the surface of the Bloch sphere, since the state is pure if and only if $\|\vec{r}\| = 1$. The points inside the Bloch sphere represent mixed states and the maximally mixed state is the center point of the sphere, with $\|\vec{r}\| = 0$.

2.5.2 The depolarizing channel

The Pauli operators also play an important role in one of the most common characterization of noise in quantum information protocols: the *depolarizing noise*. Depolarizing noise is an useful tool to benchmark the robustness of any quantum information protocol against detrimental noise. It is described by the so-called *depolarizing channel*, defined in its Kraus representation as

$$\mathcal{D}(\rho) = (1 - q)\rho + \frac{q}{3} \sum_{i=1}^3 \hat{\sigma}_i \rho \hat{\sigma}_i, \quad (2.44)$$

where $\hat{\sigma}_1 = \hat{\sigma}_X$, $\hat{\sigma}_2 = \hat{\sigma}_Z$ and $\hat{\sigma}_3 = \hat{\sigma}_Y$. The Kraus operators are thus

$$\hat{K}_0 = \sqrt{1 - q} \mathbf{1}_{\mathcal{H}_2}, \quad \hat{K}_i = \sqrt{\frac{q}{3}} \sigma_i \quad \text{for } i = 1, 2, 3, \quad (2.45)$$

as, we recall, the Pauli operators are Hermitian. To understand more deeply the action of the depolarizing channel we use the fact that, due to the properties of Pauli operators, it holds

$$\rho + \sum_{i=1}^3 \hat{\sigma}_i \rho \hat{\sigma}_i = 2\mathbf{1}_{\mathcal{H}_2}, \quad (2.46)$$

to write the action of the depolarizing channel as

$$\mathcal{D}(\rho) = (1 - p)\rho + p\frac{\mathbf{1}_{\mathcal{H}_2}}{2}, \quad (2.47)$$

with $p = \frac{3}{4}q$. The physical meaning of the depolarizing channel is therefore clear: with probability $1 - p$ it leaves the state unchanged whereas with probability p it replaces it with the maximally mixed state.

We conclude the description of the depolarizing channel by generalizing it to systems of N qubits, with vector space $\mathcal{H}_N := \mathcal{H}_2^{\otimes N}$. The first straightforward generalization is called *global depolarizing channel* and is defined as

$$\mathcal{D}_{gd}(\rho) = (1 - p)\rho + p\frac{\mathbf{1}_{\mathcal{H}_N}}{2^N}. \quad (2.48)$$

Again, it represents the channel that replaces, with probability p , the multipartite state ρ with the maximally mixed state of N qubits. However, a more interesting and realistic channel model is given by the *local depolarizing channel*, where a depolarizing channel is applied to each subsystem of the multipartite state ρ , as

$$\mathcal{D}_{ld}(\rho) = \mathcal{D}^{\otimes N}(\rho). \quad (2.49)$$

The local depolarizing channel better represents realistic noise in multipartite communication protocols, where the parties are space-like separated and each subsystem of the composite system ρ is sent to the specific party through a different channel.

2.5.3 Bell states

We conclude the description of qubit systems by introducing a class of relevant states of composite qubit systems that are particularly useful in quantum information tasks: *Bell states* and their multipartite generalization, *GHZ states*.

We start by considering a bipartite qubit system with vector space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, where both \mathcal{H}_A and \mathcal{H}_B are two-dimensional Hilbert spaces. We define the set of *Bell states* as the states

$$\begin{aligned} |\psi_+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\psi_-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\phi_+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), & |\phi_-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \end{aligned} \quad (2.50)$$

where we used the short-hand notation $|\psi\rangle \otimes |\phi\rangle = |\psi, \phi\rangle$ for product states. The Bell states are entangled and form a basis for \mathcal{H}_{AB} . Furthermore, it is possible to show that the Bell states are *maximally entangled*, i.e., they contain the most amount of entanglement among all bipartite states and thus are particularly fit for quantum information applications.

Moving to the multipartite scenario, where the vector space of the composite system is $\mathcal{H}_{B_1, \dots, B_N} = \mathcal{H}_{B_1} \otimes \dots \otimes \mathcal{H}_{B_N}$, with each \mathcal{H}_{B_i} being two-dimensional, we can define the set of *GHZ states* as

$$|\psi_{i, \vec{j}}\rangle = \frac{1}{\sqrt{2}} \left(|0\vec{j}\rangle + (-1)^i |1\vec{j}\rangle \right), \quad (2.51)$$

where \vec{j} is a binary vector of length $N - 1$ and $\vec{\bar{j}}$ is the vector that has all entries flipped with respect to \vec{j} . Similarly to the bipartite case, the GHZ states are all GME, even though there not exists a notion of "maximally entangled" for multipartite states. Moreover, for $N = 2$ they reduce to the Bell states. We will show in future sections the relevance of both Bell states and GHZ states for quantum information tasks, in particular in quantum cryptography.

Introduction to Quantum Key Distribution

This chapter is dedicated to the introduction of the quantum information task that we are going to explore in the rest of the thesis: the task called *Quantum Key Distribution (QKD)*. QKD allows two parties, traditionally denoted as Alice and Bob, to share a secret string of bits, called *key*, utilizable afterwards for cryptographic purposes, whose security against possible eavesdroppers stems from the unique features of the quantum mechanical systems employed in the protocol. The first QKD protocol was proposed in 1984 by Bennett and Brassard [BB84], whose information-theoretical security was shown at a later time [SP00; May01; Bih+06]. Other protocols soon followed [Eke91; Ben92; Bru98], employing different quantum resources. An extensive review about the most common QKD protocols can be found in [Pir+20].

The chapter is structured as following: in section 3.1 we introduce one more theoretical tool, namely entropy, and give examples of both classical and quantum entropy. We will then move on, in section 3.2, to provide a general description of common QKD protocols, showing how to prove security in section 3.2.1 and finally showing the first and most simple protocol in section 3.2.2. The chapter is mainly based on [Gra21; Wol21], with the section 3.1 being based on [Tom16].

3.1 Measures of uncertainty: entropies

In this section we introduce one more crucial tool required to prove security of any cryptographic protocol, i.e., a measure of the amount of uncertainty about the state of a system, starting from classical random variables, all the way to quantum mechanical systems. The most studied measure of uncertainty is *entropy*, which has been utilized in many different fields to quantify the information (or lack thereof) about a system. An exhaustive compendium of all relevant classical and especially quantum entropies and their properties can be found in [Tom16].

3.1.1 Classical entropy

We start with the description of classical entropy, traditionally used in classical information theory to quantify the uncertainty of random variables. We will not go

into detail about all the properties and nuances of classical entropy, but an extensive description can be found in [CT05]. In 1948 Claude Shannon [Sha48] tried to give an answer to one simple, yet fundamental question: how do we quantify the information of a random variable? To answer this question we define the so-called *Shannon entropy*:

Definition 3.1.1 (Shannon entropy). *Given a random variable X whose outcome x is drawn from an alphabet \mathcal{X} with probability p_x , the Shannon entropy of X is given by*

$$S(X) = - \sum_{x \in \mathcal{X}} p_x \log(p_x), \quad (3.1)$$

where \log will indicate, for the rest of the thesis, the base-2 logarithm. Moreover, we will assume for convention that $0 \cdot \log_2(0) = 0^1$.

The Shannon entropy has many desirable properties, but the main reason why this quantity is well suited to measure the amount of information of X is due to the so-called *Shannon's noiseless coding theorem* [Sha48]. We will not go into detail about the theorem, but it states that, given an infinite string of independent outcomes of the random variable X , there exists a compression scheme that allows to encode uniquely each outcome of the string using $S(X)$ bits. As a final remark, we consider the special case in which the alphabet \mathcal{X} is composed of only two symbols: in this case the Shannon entropy is called *binary entropy*, and is in the form

$$h(p) = -p \log(p) - (1 - p) \log(1 - p), \quad (3.2)$$

where p is the outcome probability of one of the two symbols.

The definition of the Shannon entropy can be extended to describe the joint information of two random variables X and Y . We thus define the *joint Shannon entropy* as

$$S(X, Y) = - \sum_{x,y} p_{x,y} \log(p_{x,y}), \quad (3.3)$$

where $p_{x,y}$ is the joint probability distribution of the random variables X and Y . One property of the joint Shannon entropy that is worth mentioning is *subadditivity*, i.e., $S(X, Y) \leq S(X) + S(Y)$, where the equality holds if X and Y are independent variables. Furthermore, given the two random variables X and Y , we can define the *conditional Shannon entropy* of X conditioned on Y as

$$S(X|Y) = S(X, Y) - S(Y). \quad (3.4)$$

¹This choice is supported by the intuition that an impossible event does not contribute to the information about the variable X .

Similarly we can define $S(Y|X)$. The quantity $S(X|Y)$ represents the amount of uncertainty we have about X given that we possess information about Y . An important property of the conditional Shannon entropy is that it is always non-negative, as, intuitively, the joint uncertainty about X and Y is always greater than the uncertainty about Y . As we will see, this property is not conserved when we move to quantum systems.

3.1.2 The von Neumann entropy

In a similar way as for classical information, it is possible to quantify the uncertainty about a quantum state using entropic measures. Quantum entropy has been the subject of extensive research in the last years and many different definitions have been proposed [Tom16]. The first and most natural way to quantify the information contained in a quantum state is using the so-called *von Neumann entropy*, defined as follows:

Definition 3.1.2 (von Neumann entropy). *Given a quantum state ρ on a Hilbert space \mathcal{H} , the von Neumann entropy of ρ is defined as*

$$H(\rho) = -\text{Tr}[\rho \log \rho]. \quad (3.5)$$

It can be easily shown that the von Neumann entropy can also be written as the Shannon entropy of the eigenvalues of ρ , and has the following properties:

1. The von Neumann entropy is bounded as $0 \leq H(\rho) \leq \log d$, with $H(\rho) = 0$ if and only if ρ is pure and $H(\rho) = \log d$ if and only if ρ is maximally mixed.
2. The von Neumann entropy is concave, meaning

$$H\left(\sum_i p_i \rho_i\right) \geq \sum_i p_i H(\rho_i) \quad (3.6)$$

3. The von Neumann entropy is invariant under unitary evolution, i.e.,

$$H(\hat{U}\rho\hat{U}^\dagger) = H(\rho), \quad (3.7)$$

since unitary evolution does not change the eigenvalues of a quantum state.

These properties justify the role of the von Neumann entropy as an uncertainty quantifier: a pure state has no uncertainty whereas the maximally mixed state is the most uncertain one. Moreover, the uncertainty of a quantum state does not change under unitary evolution and can only increase with mixing.

Finally, as for the classical entropy, we can define both a joint and a conditional quantum entropy. Given a bipartite state ρ_{AB} , the *joint von Neumann entropy* of ρ_{AB} is simply defined as

$$H(\rho_{AB}) = H(AB) = -\text{Tr}[\rho_{AB} \log \rho_{AB}]. \quad (3.8)$$

The joint von Neumann entropy is still subadditive, i.e., $H(A, B) \leq H(A) + H(B)$, where the equality holds if ρ_{AB} is a product state. Furthermore, given two subsystems A and B belonging to Alice and Bob, respectively, we can define the *conditional von Neumann entropy* of the state of Alice conditioned on the state of Bob as

$$H(A|B) = H(AB) - H(B), \quad (3.9)$$

where $H(B) = H(\rho_B)$ is the von Neumann entropy of the reduced state of Bob. The conditional von Neumann entropy has several properties, but here we will show three important ones, that we will use in subsequent chapters. As a direct consequence of the additivity of the joint von Neumann entropy for product states, the conditional von Neumann entropy satisfies

$$H(A|B) = H(A), \quad (3.10)$$

if ρ_{AB} is a product state. Another relevant property is the so-called *data-processing inequality*, that states that adding conditioning cannot increase the conditional von Neumann entropy. More precisely, given a tripartite state ρ_{ABC} , it holds

$$H(A|BC) \leq H(A|B) \quad (3.11)$$

where $H(A|B)$ is evaluated on the marginal $\rho_{AB} = \text{Tr}_C[\rho_{ABC}]$. Finally, let us define a *classical-quantum (c.q.) state*:

Definition 3.1.3. Given a random variable X , with M possible outcomes and a set of M orthogonal states $\{|x_i\rangle\}_{i=1}^M$, we define a classical-quantum (c.q.) state as a state in the form

$$\rho_{XQ} = \sum_{i=1}^M p_{x_i} |x_i\rangle_X \langle x_i| \otimes \rho_Q^{(i)}, \quad (3.12)$$

where the system Q is a quantum system of any dimension and p_{x_i} is the probability of obtaining outcome x_i from the random variable X .

A c.q. state represents a state where a quantum system is paired with a classical system, represented by the orthogonal states $\{|x_i\rangle\}$, reproducing the outcomes of a classical random variable. Let us then consider a particular c.q. state in the form of

Eq. 3.12, where Q is a bipartite quantum system composed by subsystems A and B . It is possible to show that the following holds:

$$H(A|BX) = \sum_{i=1}^M p_{x_i} H(A|BX = x_i), \quad (3.13)$$

where $H(A|BX)$ is evaluated on the state ρ_{ABX} and $H(A|BX = x_i)$ on the state $\rho_{AB}^{(i)}$.

As a final remark, we note that the conditional von Neumann entropy, unlike the conditional Shannon entropy, can be negative. For example, if we consider one of the Bell states given in Eq. (2.50), its joint entropy is $H(AB) = 0$ since it is a pure state. However, it can easily be seen that $H(A) = H(B) = 1$, and thus $H(A|B) = -1$. This substantial difference with the classical entropy can be seen from another point of view: it is no longer true that $H(AB) \geq H(A), H(B)$, like with classical entropy or, in other words, it is possible to have less knowledge about the reduced systems than the global system. This interesting feature, unique to quantum systems, gives us an important characterization of entangled states: as a matter of fact, if $H(A|B) < 0$ we know that ρ_{AB} must be entangled, reinforcing the idea that entanglement is an important and unique feature of quantum theory.

3.1.3 Conditional min- and max-entropy

In this section we will introduce two more entropy measures that are of pivotal importance in many quantum information tasks: the *conditional min-entropy* and *max-entropy* [KRS09]. We start by defining the min-entropy as follows:

Definition 3.1.4 (Conditional min-entropy). *Given a bipartite quantum state ρ_{AB} the conditional min-entropy of A conditioned on B is defined as*

$$H_{min}(A|B) = -\log \min_{\sigma_B} \{ \text{Tr}[\sigma_B] \text{ s.t. } \sigma_B \geq 0, (\mathbf{1}_A \otimes \sigma_B) - \rho_{AB} \geq 0 \}, \quad (3.14)$$

where the minimization is over all quantum states σ_B .

The *conditional max-entropy* is defined as follows

Definition 3.1.5 (Conditional max-entropy). *Given a bipartite state ρ_{AB} the conditional max-entropy of A conditioned on B is defined as*

$$H_{max}(A|B) = \max_{\sigma_B} \log \left\| \sqrt{\rho_{AB}} \sqrt{\mathbf{1} \otimes \sigma_B} \right\|_1^2, \quad (3.15)$$

where $\|\cdot\|_1$ is the trace norm of an operator, defined as $\|\hat{A}\| = \text{Tr} \left[\sqrt{\hat{A}\hat{A}^\dagger} \right]$ and where the maximisation is over all quantum states σ_B .

An alternative definition of the conditional max-entropy can be given in terms of the conditional min-entropy:

Definition 3.1.6. Given a bipartite state ρ_{AB} and its purification ρ_{ABC} , such that $\text{Tr}_C[\rho_{ABC}] = \rho_{AB}$, we define the conditional max-entropy of A conditioned on B as

$$H_{max}(A|B) = -H_{min}(A|C). \quad (3.16)$$

Given a bipartite state ρ_{AB} the conditional min- and max-entropy are related to the conditional von Neumann entropy as follows [TCR09]

$$H_{min}(A|B) \leq H(A|B) \leq H_{max}(A|B). \quad (3.17)$$

The importance of the conditional min-entropy is due to its operational meaning. Let us consider the following scenario: one party, Alice, holds a key k , i.e., a string of bits. Alice's subsystem is indicated by K . A malicious party, traditionally called Eve, wants to acquire knowledge about Alice's key and, to do so, she correlates Alice's key with a quantum state. The global quantum state describing Alice's key together with Eve's system is thus a c.q. state in the form

$$\rho_{KE} = \sum_{k \in \mathcal{K}} p_k |k\rangle\langle k| \otimes \rho_E^{(k)}, \quad (3.18)$$

where the different possible keys are encoded in the orthogonal states $\{|k\rangle\}_{k \in \mathcal{K}}$, where \mathcal{K} is the space of all possible keys, each occurring with probability p_k and $\rho_E^{(k)}$ is Eve's quantum state. In order to gain knowledge about Alice's subsystem, Eve performs a measurement, with POVM elements E_k , on her subsystem and the probability of Eve correctly guessing the key is given by the so-called *guessing probability*

$$p_{guess}(K|E) = \max_{E_k} \sum_{k \in \mathcal{K}} p_k \text{Tr} [E_k \rho_E^{(k)}]. \quad (3.19)$$

It turns out that the guessing probability is closely related to the conditional min-entropy, as

$$H_{min}(K|E) = -\log p_{guess}(K|E). \quad (3.20)$$

The conditional min-entropy, therefore, plays a crucial role in another quantum information task closely related to QKD, namely *randomness extraction*. In fact, the min-entropy can be also seen, in its operational meaning, as the amount of uniform randomness that Alice can extract from its random variable, in this case K with probability distribution p_k : if the key is completely random, in fact, Eve has no way of guessing it and thus the conditional min-entropy is maximal, whereas in the

opposite case, where the key is completely deterministic, Eve can perfectly guess the key and thus the conditional min-entropy is zero.

3.1.4 Entropic uncertainty relation

Finally, we introduce an important tool related to entropy that is the *entropic uncertainty relation*. In the standard formulation of quantum mechanics, the famous Heisenberg uncertainty principle tells us that due to the inherent non-commutativity of certain observables, like position and momentum, these observables cannot be measured jointly with arbitrary precision. A similar situation presents itself with the quantum von Neumann entropy and this uncertainty relation proves to be extremely useful in quantum cryptography.

We consider the following scenario: two parties, Alice and Bob, hold a bipartite state ρ_{AB} . Furthermore, Alice has at her disposal two quantum measurements, defined by POVM elements $\{\hat{M}_x^{(A)}\}$ and $\{\hat{N}_y^{(A)}\}$, respectively. If Alice performs the first measurement, the resulting state will be the c.q. state

$$\rho_{XB} = \sum_x |x\rangle_X \langle x| \otimes \text{Tr}_A[(\hat{M}_x^{(A)} \otimes \mathbf{1}_B)\rho_{AB}], \quad (3.21)$$

where Alice's subsystem has been replaced with the classical subsystem X in which she records the outcomes x of the measurement in the orthogonal states $\{|x\rangle\}$. A similar state can be defined for the second measurement

$$\sigma_{YB} = \sum_y |y\rangle_Y \langle y| \otimes \text{Tr}_A[(\hat{N}_y^{(A)} \otimes \mathbf{1}_B)\rho_{AB}]. \quad (3.22)$$

Using the conditional von Neumann entropy, we can define the uncertainty that Bob has about the outcome of the measurement with $H(X|B)$ and $H(Y|B)$ for the first and second measurement, respectively. We remark that $H(X|B)$ is evaluated on the state ρ_{XB} of Eq. (3.21) and $H(Y|B)$ on the state σ_{YB} of Eq. (3.22). If Bob doesn't know which measurement is performed, the total uncertainty of Bob about the outcome is $H(X|B) + H(Y|B)$. The following theorem, formulated in [Ber+10], gives a lower bound on this uncertainty.

Theorem 2. *Given a bipartite state ρ_{AB} and given two measurements on Alice's side with POVM elements $\{\hat{M}_x^{(A)}\}$ and $\{\hat{N}_y^{(A)}\}$ the total uncertainty of Bob about Alice's measurements is lower bounded by*

$$H(X|B) + H(Y|B) \geq \log \frac{1}{c} + H(A|B), \quad (3.23)$$

where $H(A|B)$ is the conditional von Neumann entropy of ρ_{AB} . The quantity c is a measure of incompatibility of the two measurements, defined as

$$c := \max_{x,y} \left\| \sqrt{M_x^{(A)}} \sqrt{N_y^{(A)}} \right\|_{\infty}^2, \quad (3.24)$$

with $\|\cdot\|_{\infty}$ being the infinity norm of an operator, defined as its largest singular value (in the finite-dimensional case).

The first term on the right-hand side of Eq. (3.23) depends on the measurements of Alice and intuitively is higher for more incompatible measurement and the second term depends only on the state. It is worth noting that since the conditional von Neumann entropy can be negative, even for highly incompatible measurements Bob can know Alice's outcome with certainty by choosing the right state. This uncertainty relation serves, as we will see in detail later, as a foundational tool for modern security proofs of many quantum cryptographic protocols.

3.2 Quantum Key Distribution protocols

We are now ready to introduce and discuss the main topic of this thesis, i.e., the fundamental quantum information task known as *Quantum Key Distribution* (QKD). The main goal of QKD is to allow two parties², called as usual Alice and Bob, to share a common key, i.e., a string of bits, secure against possible tampering of a malicious party called Eve. The security in particular is guaranteed by the unique properties of quantum mechanics. A generic QKD protocol is described as following:

1. **Quantum transmission:** the parties share, each round of the protocol, a quantum resource which is vulnerable to attacks by the eavesdropper Eve. Eve can correlate the quantum resource with its own system and perform measurements on her own subsystem. The quantum transmission can be done mainly in two different ways: Alice can encode the information about the key into quantum states and send them to Bob through an insecure quantum channel, which can be attacked by Eve. In this case we say that the protocol is *Prepare and Measure (PM)*. Alternatively, Alice and Bob can receive each a subsystem of a bipartite quantum state from a source which can be in the hands of Eve. In this case we say that the protocol is *entanglement based (EB)*.
2. **Quantum measurements:** the parties (or, for PM protocols, just Bob) perform, each round of the protocol, specific measurements on the resource they shared

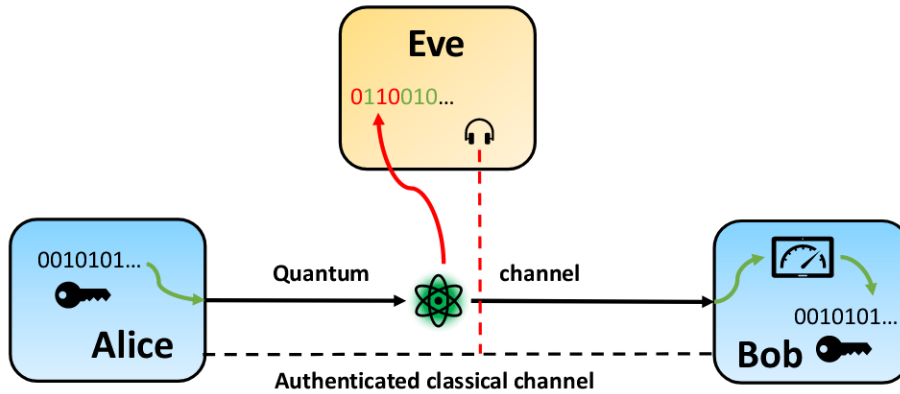
²The generalization to more parties will be considered in the next chapter. In this chapter we will focus uniquely on the two-party scenario.

to extract the encoded information. After M rounds of the protocol, they share a *raw key* of length M , obtained with the measurement outcomes. We remark that at this point the raw key contains errors and information leaked to Eve.

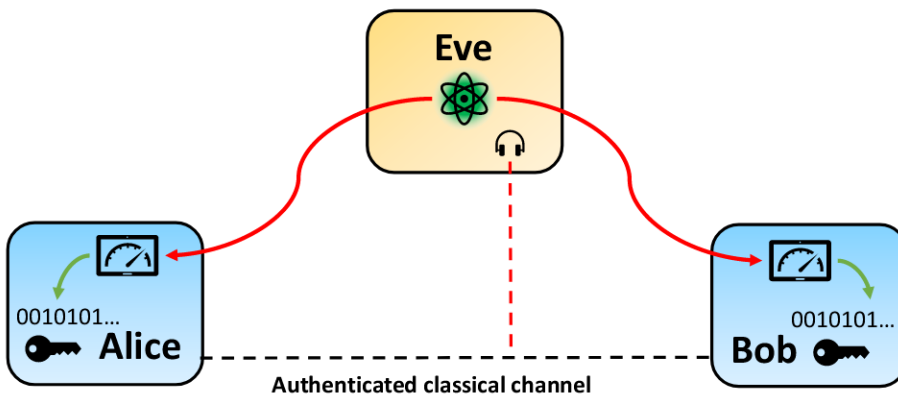
3. **Classical parameter estimation:** the parties use an authenticated classical channel to share a small part of the raw key in order to estimate the information gained by Eve in the protocol. If they detect that Eve has gained enough information to reconstruct the key, they abort the protocol.
4. **Classical error correction:** the parties use the same authenticated classical channel to share information about the raw keys in order to use error correction algorithms to obtain a matching key. From now on we will consider the case where Alice and Bob use *one-way error correction* algorithms, meaning that Alice sends information to Bob, which corrects his raw key according to Alice's one.
5. **Classical privacy amplification:** the parties use the same authenticated classical channel to compress the error-corrected keys into shorter keys, in order to erase the information that Eve gained. This is done, e.g., with *two-universal hashing*. They thus obtain matching, secure keys.

In Figure 3.1 we show a schematic representation of both a PM- and an EB-QKD protocol. As we can see any QKD protocol is divided into two parts: a first, quantum part, where the parties share quantum systems and perform quantum measurements to effectively extract the key, followed by a second, classical, part where they employ classical post-processing to guarantee the correctness and security of said key. We note that the classical part of the protocol requires an authenticated classical channel between Alice and Bob, meaning that when they share classical information they are sure to communicate with each other and Eve has not replaced one of the parties. However, Eve can have access to the classical information shared. In this thesis we will focus mainly on the quantum part of the protocols. A variety of error correction algorithms can be found in [MS83] and more details about privacy amplification can be found in [Wol21]. Finally, we remark that, for different reasons, it is useful to consider the so-called *asymptotic scenario*, i.e., to consider $M \rightarrow \infty$, corresponding to an infinite key length. One of the main reasons to restrict to the asymptotic scenario is that it is usually easier to prove information-theoretical security of the protocol. However in a realistic scenario Alice and Bob will not be capable of performing the protocol for an infinite amount of rounds and therefore the security analysis must be extended for finite-size keys.

In the protocol description we outlined the difference between PM and EB protocols. While the two descriptions are different for practical applications, it is



(a)



(b)

Fig. 3.1.: Schematic representation of PM- and EB-QKD protocols, as described in this Section. In Figures 3.1a and 3.1b we show a sketched version of a PM-QKD protocol and an EB-QKD protocol, respectively. It is interesting to note that many QKD protocols have equivalent PM and EB formulations. Usually, PM-QKD protocols are more easily implemented in practical scenarios, whereas EB-QKD protocols have more straightforward security proofs.

possible to show the theoretical equivalence between some PM protocols and some EB ones. Let us consider a PM protocol: let us assume that Alice holds a string of bits x_1, \dots, x_M , i.e., the raw key, where each bit is generated from a random variable with probability p_x . In the i -th round of the protocol Alice encodes the information

of the i -th bit in a quantum state $|\phi_i\rangle$ and sends it to Bob. The *global state* sent by Alice to Bob is described by

$$|\phi_{gl}\rangle = |\phi_1\rangle \otimes \dots \otimes |\phi_M\rangle. \quad (3.25)$$

Bob, each round of the protocol, performs a measurement on the received state and extract the information about Alice's key. Let us now imagine that Alice and Bob share, each round of the protocol, the following entangled state

$$|\psi\rangle_{AB} = \sum_x \sqrt{p_x} |x\rangle_A |\psi_x\rangle_B, \quad (3.26)$$

where the states $\{|x\rangle_A\}$ are an orthonormal basis of Alice's subsystem. If Alice measures on this orthonormal basis, she obtains outcome x with probability p_x , thus reproducing, if she measures M times, the generation of the key from a random variable with probability distribution p_x in the PM scenario. Moreover, if we consider the reduced state after the measurement we obtain $|\psi\rangle_{X_i B} = |x_i\rangle_A |\psi_{x_i}\rangle_B$, which simulates the transmission of the state $|\psi_{x_i}\rangle$ to Bob. This is therefore the equivalent EB formulation for the corresponding PM protocol.

In general, it is more convenient to show security in the EB scenario, where one does not have to deal with quantum channels but just with the bipartite entangled state shared by the parties, assuming that Eve has full control on the source of the state. Therefore, although PM protocols are more practical to implement, it is common in security proofs to find the equivalent EB formulation of the protocol and show security for the latter.

3.2.1 Security of QKD

As already pointed out, the crucial advantage that QKD protocols provide over classical protocols is the ability to guarantee information-theoretical security, meaning that we are able to guarantee security independently on the power given to the eavesdropper. In this section we will go into detail about the security of QKD protocols. Further details can be found in [Sca+09; PR22], where the countless techniques that have been developed are analyzed thoroughly. We will present one of the most modern and universal techniques, due originally to Devetak and Winter [DW05] and then further refined [SR08], that we will extensively use throughout the thesis.

Let us start with some basic assumptions that are required to prove security in any QKD scheme. Breaking these assumptions will result in a possible leakage of information to Eve not accounted for in the model. A complete treatment

of the assumptions of quantum cryptography and possible loopholes in practical implementations can be found in [Bea14; SK14].

1. **Quantum mechanics is correct and complete.** This basic underlying assumption ensures that the theory we use correctly predicts measurement outcomes and provides a description for all phenomena we observe. Without quantum theory it is clearly impossible to formulate a QKD scheme.
2. **The parties' laboratories are isolated.** We assume that Alice's and Bob's laboratory, where they make measurements and prepare states, are isolated and inaccessible to Eve.
3. **Trusted devices.** We assume that the state preparation (in PM protocols) and the measurement devices are trusted and produce the exact state or measurement outcome they are supposed to. Additionally, Eve has not tampered in advance with the devices, which could give her additional information. This assumption can be relaxed in *Device-Independent QKD* schemes, which will be outlined in chapter 6.
4. **Authenticated channel and trusted classical post-processing.** Finally, we already pointed out that the parties need to have an authenticated classical communication channel in order to perform classical post-processing. Moreover, the parties need to trust that all parts of the classical post-processing function the way they are supposed to and there are no deviations from the theoretical model.

Under these basic assumptions, Eve is able to attack the quantum channel connecting the parties and access the classical information exchanged. However, we have not specified how much power can be given to Eve in tampering with the quantum resource. Eve's attacks can be grouped into three classes, which we will outline in the order of power given to Eve: *individual attacks*, *collective attacks* and *coherent attacks*.

Let us start by describing the scenario: let us for now consider a PM-QKD scheme, where Alice prepares M states $\rho_A^{(1)} \dots \rho_A^{(M)}$, in which she encodes the information about the key. Each round she sends one of the states through an insecure quantum channel to Bob. The way Eve extracts information about the states sent by Alice is to attach an ancilla state $|E\rangle_E \langle E|$, which can be chosen to be pure without loss of generality³ and apply an unitary evolution on the composite state. Afterwards, she

³This assumption is due to the fact that, in order to give Eve the maximum amount of power, we do not give any assumption on the dimension of the Hilbert space of Eve's subsystem. Therefore, even if the state is mixed, she can always purify it by enlarging the dimension of the Hilbert space of her subsystem.

performs some measurement on her part of the state, which is usually called *Eve's quantum side-information*, to retrieve some knowledge about Alice's initial state.

In the weakest class of attacks, i.e., *individual attacks*, Eve does this procedure each round independently: in the i -th round she attaches the ancilla state to the state $\rho_A^{(i)}$, applies the same unitary \hat{U} each round and obtains the state

$$\rho_E^{(i)} = \text{Tr}_A \left[\hat{U}^\dagger \rho_A^{(i)} \otimes |E\rangle_E \langle E| \hat{U} \right]. \quad (3.27)$$

She then proceeds to perform the same measurement, with POVM elements $\{\hat{E}_i\}$ on each individual $\rho_E^{(i)}$. Eve, however, could be able to exploit not only the information contained in each individual state but also the one contained in the global state sent by Alice, i.e., $\rho_A^{(1)} \otimes \dots \otimes \rho_A^{(M)}$. This is accounted for with collective and coherent attacks. In fact, in *collective attacks*, Eve can attach the ancilla and evolve the state individually, like in individual attacks, obtaining the same state $\rho_E^{(i)}$ as Eq. (3.27). However, in collective attacks, she is able to perform a global measurement on the global ancilla state $\rho_E^{(1)} \otimes \dots \otimes \rho_E^{(M)}$. Finally, with *coherent attacks* Eve is able to act directly on the global state sent by Alice. Her ancilla state is, in this scenario

$$\rho_E = \text{Tr} \left[\hat{U}_{gl}^\dagger (\rho_A^{(1)} \otimes \dots \otimes \rho_A^{(M)}) \otimes |E\rangle_E \langle E| \hat{U}_{gl} \right], \quad (3.28)$$

where \hat{U}_{gl}^\dagger is a global unitary on the composite system. She then can perform a global measurement on the state ρ_E . Coherent attacks are the most general attacks, that give Eve the maximum amount of power.

As a final remark, we note that in EB protocols a similar description about Eve's attacks can be given. Eve, instead of attaching an ancilla and unitarily evolving the composite state, is in control of the source of entangled states and thus is assumed, to give her the most amount of power, to hold a purification of the state shared by Alice and Bob together with her quantum side-information, on which she can perform any measurement or operation. For individual and collective attacks she holds a purification of the state shared each round and she can perform measurements on her part of the purification independently each round and globally, respectively. For coherent attacks Eve is assumed to hold a purification of the global state shared by the parties.

In order to assess the performances and limitations of any QKD protocol, we need to introduce a measure of how many bits of secret key can be generated per round in the protocol. This fundamental quantity is called the *key rate*, defined as the fraction of secret bits of key extracted each round by the parties. Crucially, the key rate can

be lower bounded, in any asymptotic QKD protocol against collective attacks, by the following quantity [DW05; SR08],

$$r_\infty \geq H(A|E) - S(A|B), \quad (3.29)$$

where $H(A|E)$ is the quantum conditional entropy of Alice's random variable representing the secret key A conditioned on Eve's quantum side-information and $S(A|B)$ is the classical conditional entropy of A given the random variable representing Bob's key, B . Intuitively the first term represents how much information about the key is leaked to Eve during the protocol and the second term accounts for the errors that Bob has to correct in order to obtain a matching key with Alice. The security of the protocol is itself contained in the key rate: if the key rate is positive, Alice and Bob can extract a shared key, secure against Eve, whereas if the key rate is zero ⁴ the protocol fails, either due to leakage of information to Eve or to too many errors in the raw keys. We finally remark that restricting to collective attacks does not imply loss of generality in the asymptotic regime, as security against coherent attacks can be inferred from security against collective attacks with the *post-selection technique* [CKR09]. Therefore, in many protocols and in asymptotic regimes, it is sufficient to restrict to collective attacks to prove unconditional security.

3.2.2 The BB84 protocol

In this final section we review the first and most important QKD protocol, designed by Bennett and Brassard in 1984 [BB84], thus called BB84 protocol. Let us start with the original PM protocol and then give the equivalent EB description. The protocol is described as following:

1. **Quantum transmission:** each round of the protocol Alice randomly picks either the Z- or the X-basis. She then randomly picks one of the two states of the chosen basis, i.e., $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ and sends it to Bob through an insecure quantum channel, subject to attacks by Eve. The parties agree to encode the key bit value 0 with states $|0\rangle$ and $|+\rangle$ and bit value 1 with states $|1\rangle$ and $|-\rangle$.
2. **Quantum measurements:** each round Bob measures randomly in the Z- or X-basis the state he receives. If he measures in the same basis Alice prepared her system in, he will extract the encoded information, i.e., he will obtain exactly the bit Alice intended to encode. Otherwise, he will get a random bit.

⁴The key rate can be negative, which does not make physical sense, as already $r_\infty = 0$ implies that the protocol fails. Usually one considers the key rate to be $\max\{r_\infty, 0\}$ to avoid such confusion.

3. **Classical sifting:** after M rounds the parties publicly share the information about which basis Alice used for state preparation and in which basis Bob measured each round. We note that this information can be overheard by Eve as it does not give her any information about the key bits. Then, they discard all rounds in which Bob measured in a different basis than the one Alice prepared her state in. They are then left, in case of no noise or tampering of Eve, with a perfectly correlated key string of approximately $\frac{M}{2}$ bits.
4. **Classical parameter estimation:** the parties publicly disclose a small fraction of the key to estimate the *quantum bit error rate (QBER)* in each basis, namely Q_Z and Q_X . We note that in realistic implementations errors can be caused by any source of noise, even outside the control of Eve. However, to show information-theoretical security we have to consider the worst-case scenario, where all the errors and noise are caused by Eve.
5. **Classical post-processing:** as shown in Section 3.2, the parties perform classical error correction and privacy amplification to obtain a secure shared key.

This protocol's formulation follows directly the original work and it is the most useful from the point of view of the practical applications. However, its equivalent EB formulation is more useful in security proofs and thus it is worth to be considered. The equivalent EB formulation requires the parties to share the bipartite Bell state, given in Eq. (2.50),

$$|\psi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (3.30)$$

where $|0\rangle$ and $|1\rangle$ are the element of the computational basis. It is straightforward to show that the Bell state has the same form if we change to the X-basis, namely $|\psi_+\rangle_{AB} = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$. Therefore, if Alice and Bob measure in the Z- and X-basis, they will obtain perfectly correlated outcomes if they measure in the same basis and random outcomes otherwise, equivalently to the PM formulation. It is worth also noting that all Bell states of Eq. (2.50) are equivalent up to local operations and thus all Bell states can be used in the EB formulation of the BB84 protocol.

We can show security of the BB84 protocol in its EB formulation by exploiting the entropic uncertainty relation. This is not the only nor the original method used to prove security for the BB84 protocol, but besides being elegant and simple it is close to the security proofs we will employ in the works we will present in the next chapters. The full original security proof, that we will omit here, was rigorously given in [SP00; May01; Bih+06], some years after the original work by Bennett and Brassard.

In order to proof security of the BB84 protocol, we need to allow the parties to estimate Eve's knowledge and errors in the protocol with the quantities that they can estimate in the protocol, i.e., the QBERs Q_Z and Q_X . We thus recast the key rate in Eq. (3.29) as a function of these quantities. In the asymptotic scenario and for collective attacks, Eve has access to a purification ρ_{ABE} of the state shared by the parties ρ_{AB} . Let us start with the following Corollary, derived directly from the entropic uncertainty relation shown in Section 3.1.4.

Corollary 3.2.1. *Given the purification ρ_{ABE} and given that Alice performs either Z- or X-basis measurements on her part of the system, it holds*

$$H(Z|E) + H(X|B) \geq 1, \quad (3.31)$$

where the first entropy is evaluated on the post Z-basis measurement state ρ_{ZBE} and the second on the post X-basis measurement state ρ_{XBE} .

Proof. To show this expression we start with Eq. (3.23), which we can write in our case as

$$H(Z|B) + H(X|B) \geq 1 + H(A|B) \quad (3.32)$$

where we used that $\log_2 \frac{1}{c} = 1$ for Z- and X-basis measurements, since they are maximally incompatible. We can thus write, using the expression of the conditional von Neumann entropy in Eq. (3.9)

$$H(ZB) - H(B) + H(XB) - H(B) \geq 1 + H(AB) - H(B) \quad (3.33)$$

Moreover, it is possible to show that if a multipartite state is pure, the entropies of any of its marginals are equal [Tom16]. Therefore, since ρ_{ABE} is pure by definition we have $H(AB) = H(E)$ and $H(ZB) = H(ZE)$. We can thus write

$$H(ZE) + H(XB) \geq 1 + H(E) + H(B), \quad (3.34)$$

which can finally be recast as $H(Z|E) + H(X|B) \geq 1$, concluding the proof. \square

Using this expression, the asymptotic key rate of Eq. (3.29) becomes

$$r_\infty \geq H(Z|E) - H(Z|B) \geq 1 - H(Z|B) - H(X|B), \quad (3.35)$$

where we note that both $H(Z|B)$ and $H(X|B)$ are quantum conditional entropies of Alice's measurements outcomes given Bob's quantum subsystem. We now use the fact that the entropy does not increase with measurement operation [Tom16] to write

$$r_\infty \geq 1 - S(Z_A|Z_B) - S(X_A|X_B) \quad (3.36)$$

where Z_A and Z_B are the random variables representing Alice's and Bob's outcomes in the Z-basis, respectively, and X_A and X_B are the random variables representing Alice's and Bob's outcomes in the X-basis, respectively. We note that this expression only contains classical conditional entropies of the parties' outcomes and can be recast in terms of the QBERs as

$$r_\infty \geq 1 - h(Q_Z) - h(Q_X). \quad (3.37)$$

This security analysis holds only for the asymptotic scenario. If we consider the finite-size key scenario, this expression must be corrected with additional terms depending on the size of the key. These additional terms are called *finite-key effects* and vanish for $M \rightarrow \infty$. We will not go into details about finite-key effects for the BB84 protocol in this work, but more details can be found in [Tom+12].

Conference Key Agreement

In the last chapter we introduced the main ideas behind the concept of exploiting quantum mechanics to allow the sharing of a secure key. We mainly focused on bipartite protocols, where the parties that want to perform the protocol are two, namely Alice and Bob. However, all modern communication tasks involve intricate networks, where many users establish communication channels with each other. In this scenario, it is required to extend the secure communication protocols from the standard two-party formulation to multipartite protocols. The extension of QKD to many parties is often called *Conference Key Agreement (CKA)*, and it is the main focus of our work. Due to the imminent application of quantum cryptography in networks, CKA has received a lot of attention in the past years, both from a theoretical [CL07; Epp+17; GKB18; GKB19; Ott+19; ZSG18; Zha+20; HJP20; Gra+22] and experimental point of view [Pic+22; Rüc+22]. This first chapter is dedicated to showing the rudiments of CKA and investigating the fundamental requirements of the quantum resource exploited in the protocol, following mainly our work done in [Car+21].

The chapter is structured as following: in section 4.1 we introduce the task of CKA and restrict our analysis to a specific class of protocols. From this class, we present two simple CKA protocols, one of which being a direct generalization to many parties of the BB84 protocol presented in section 3.2.2, the other, shown in section 4.1.2, exploiting another class of GME states. Then, in section 4.2 we explore in detail the results we obtained in [Car+21], investigating the necessary and sufficient requirements of the state shared in each round of the protocol to successfully perform CKA. In section 4.2.2 we present an interesting insight connecting the key rate of a CKA protocol with the concept of entanglement witnesses. Finally, in section 4.2.3, we restrict to a specific type of network, namely the *triangle network*, where the parties cannot perform classical communication, and investigate the properties of the states that can be generated in this network, with the use for CKA in mind.

4.1 Basics of Conference Key Agreement

Let us start with introducing the task of CKA. In a quantum CKA protocol, N parties, named Alice and Bob₁,...,Bob _{$N-1$} , labelled A and B_1, \dots, B_{N-1} , exploit a quantum resource in order to extract a common conference key, secure against the attacks

of an eavesdropper, Eve. A general CKA protocol is described in an almost identical way as a QKD protocol, as in Section 3.2, the only difference being that N parties instead of two are involved in the protocol. However, from now on, we will restrict to a specific class of protocols, described as following:

1. **Quantum transmission:** each round of the protocol N parties, namely Alice and $\text{Bob}_1, \dots, \text{Bob}_{N-1}$, receive, from a source possibly controlled by an eavesdropper, Eve, a multipartite entangled state $\rho_{AB_1 \dots B_{N-1}}$. Eve, in the most adversarial scenario, holds a purification $|\psi\rangle_{AB_1 \dots B_{N-1}E}$, where E represents Eve's subsystem, of the state $\rho_{AB_1 \dots B_{N-1}}$ and can manipulate E freely, e.g., by performing measurements.
2. **Quantum measurements:** the N parties perform, each round of the protocol, one of two measurement on the state they shared: a first set of measurements, called *Key Generation (KG)* measurements, chosen with probability p , whose outcomes are used to generate the secret key and a second set of measurements, called *Parameter Estimation (PE)* measurements, chosen with probability $1 - p$, used to obtain information about the eavesdropper's knowledge of the key. After M rounds of the protocol, where $M \rightarrow \infty$, the parties share a *raw key* of length $L = Mp$, obtained with the KG measurement outcomes. We remark that at this point the raw key contains errors and information leaked to Eve.
3. **Classical parameter estimation:** the N parties disclose, through an authenticated classical channel, part of the outcomes of the KG rounds to estimate the error correction information required to obtain matching keys. Then, they disclose the outcomes of the PE rounds to estimate the information about the key leaked to Eve.
4. **Classical post-processing:** the N parties use the same authenticated classical channel to perform the usual post-processing, i.e., error correction and privacy amplification. We still consider one-way error correction, where each Bob corrects his key according to Alice's one.

We thus restrict the analysis to EB asymptotic protocols, where the parties perform two different sets of measurements each. We give a schematic representation of such protocols in Figure 4.1. The EB formulation of the BB84 protocol is the most simple and studied example, for two parties, of such protocols. We also remark that we implicitly restricted to collective attacks, by allowing Eve to have a purification of the individual states shared by the parties. As already discussed, however, in the asymptotic scenario, security against general attacks can be inferred from security against collective attacks.

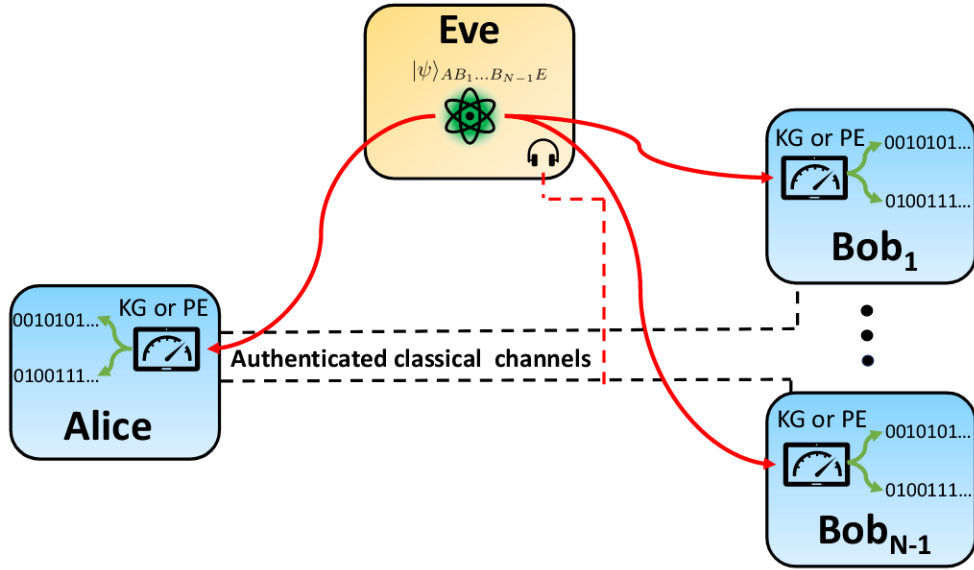


Fig. 4.1.: Schematic representation of the considered class of CKA protocols. We restrict to EB-CKA protocols where the parties share a multipartite quantum state generated by Eve and perform two types of measurements, labelled as KG or PE measurements. The most commonly considered and most simple protocols fall in this class, as we will show in future sections.

Once again, the crucial quantity of a CKA protocol is the key rate, i.e., the fraction of key bits of conference key extracted each round. The Devetak-Winter rate of Eq. (3.29) can be generalized for N parties as follows [Epp+17]

$$r_\infty \geq H(A|E) - \max_i S(A|B_i), \quad (4.1)$$

where $H(A|E)$ is the quantum conditional entropy of Alice's outcomes conditioned on Eve's quantum side-information and $S(A|B_i)$ is the classical conditional entropy of Alice's KG outcomes given Bob B_i 's KG outcomes. The second term accounts for error correction of the most discordant key among the Bobs' with the maximization over the Bobs, as all the Bobs correct their keys according to Alice's one. Let us now show two examples of simple CKA protocols, both exploiting the correlations of different classes of GME states.

4.1.1 The N-BB84 protocol

We start with the most intuitive idea for a CKA protocol, i.e., the generalization of the BB84 protocol to many parties, proposed in [GKB18], where the authors provide a complete description of the protocol including finite-key effects. Here, we only focus on the asymptotic scenario. The protocol is described as following:

1. **Quantum transmission:** each round of the protocol N parties, Alice and $\text{Bob}_1, \dots, \text{Bob}_{N-1}$ ideally receive from an untrusted quantum source a *GHZ state*¹,

$$|\psi\rangle_{AB_1, \dots, B_{N-1}} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \quad (4.2)$$

2. **Quantum measurements:** the N parties perform, each round of the protocol, one of two measurements, e.g., choosing according to a pre-shared key, on the state they shared: in KG rounds they measure on the Z-basis and in PE rounds they measure on the X-basis.
3. **Classical parameter estimation:** the N parties disclose, through an authenticated classical channel, part of the outcomes of the KG rounds to estimate the error correction information required to obtain a matching key. They evaluate the Z-basis pair-wise QBER, that is, the probability that the outcome of the measurement in the Z-basis of Bob B_i differs from Alice's one, defined as

$$Q_{AB_i} = \frac{1 - \langle \hat{Z}_A \otimes \hat{Z}_{B_i} \rangle}{2}, \quad (4.3)$$

where \hat{Z} is the Pauli Z operator of Eq. (2.39). We note that in the ideal scenario, where the parties receive the noiseless GHZ state and Eve does not tamper with the state, $Q_{AB_i} = 0 \ \forall i$. Then, they disclose the outcomes of the PE rounds and calculate the X-basis QBER defined as

$$Q_X = \frac{1 - \langle \hat{X}_A \otimes \hat{X}_{B_1} \otimes \dots \otimes \hat{X}_{B_{N-1}} \rangle}{2}, \quad (4.4)$$

where \hat{X} is the Pauli X operator of Eq. (2.39). Again, in the ideal scenario $Q_X = 0$.

4. **Classical post-processing:** the N parties use the same authenticated classical channel to perform the usual post-processing, in the form of error correction and privacy amplification. We still consider one-way error correction, where each Bob corrects his key according to Alice's one.

The protocol exploits the entanglement of the GHZ state, whose outcomes in the Z basis are clearly perfectly correlated, similarly to the BB84 protocol which, in its EB formulation, exploits the correlations of the maximally entangled Bell states, as seen in section 3.2.2

¹We note that the parties do not know exactly which state they receive from the source, as it is untrusted and could be in the hands of Eve. If the source does not behave as expected and sends different states, they will notice in the parameter estimation phase and abort the protocol.

Following the same procedure as for the bipartite BB84, shown in section 3.2.2, we can recast, for the N-BB84 protocol, the key rate of Eq. (4.1) as

$$r_\infty \geq 1 - h(Q_X) - \max_i h(Q_{AB_i}), \quad (4.5)$$

where the QBERs Q_{AB_i} and Q_X are defined in the "Classical parameter estimation" step of the protocol. As a final remark, we note that, without noise and Eve's intervention, the protocol achieves the optimal key rate $r_\infty = 1$. However, besides the technical difficulties of generating GHZ states, this protocol is also not suited for long distance communication, due to the GHZ state lacking noise resistance. One way to overcome this limitation is, as we will see in detail in chapter 5, to exploit the correlations of a different GME states, e.g., the *W-state*.

4.1.2 CKA with the W state

Although the GHZ state appears to be the most natural state to exploit for CKA due to its perfect correlations in the Z-basis, it is natural to ask whether other multipartite states are suited for quantum cryptographic tasks. A first, simple answer was given in [GKB19], where the authors show that another GME state can be used in a cryptographic protocol, that is the *W-state*

$$|W\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^N |\vec{b}_i\rangle, \quad (4.6)$$

where the vector \vec{b}_i is a binary vector with zeros in all positions except for position i , where it has a one. In [GKB19], the authors show the possibility to employ this state in a simple CKA protocol, described as following:

1. **Quantum transmission:** each round of the protocol N parties, Alice and Bob₁,...,Bob_{N-1} ideally receive, from an untrusted quantum source, a *W state*,

$$|W\rangle_{AB_1, \dots, B_{N-1}} = \sum_{i=1}^N |\vec{b}_i\rangle_{AB_1, \dots, B_{N-1}}. \quad (4.7)$$

2. **Quantum measurements:** the N parties perform, each round of the protocol, one of two measurements, e.g., choosing according to a pre-shared key, on the state they shared: in KG rounds they measure on the X-basis and in PE rounds they measure on the Z-basis.
3. **Classical parameter estimation:** the N parties disclose, through an authenticated classical channel, part of the outcomes of the KG rounds to estimate the

error correction information required to obtain a matching key. They evaluate the X-basis pair-wise QBER, that is, the probability that the outcome of the measurement in the X-basis of Bob B_i differs from Alice's one, defined as

$$Q_{AB_i} = \frac{1 - \langle \hat{X}_A \otimes \hat{X}_{B_i} \rangle}{2}, \quad (4.8)$$

where \hat{X} is the Pauli X operator of Eq. (2.39). Then, they disclose the outcomes of the PE rounds and calculate the Z-basis QBER, defined as

$$Q_Z = \frac{1 + \langle \hat{Z}_A \otimes \hat{Z}_{B_1} \otimes \dots \otimes \hat{Z}_{B_{N-1}} \rangle}{2}, \quad (4.9)$$

where \hat{Z} is the Pauli Z operator of Eq. (2.39). In the ideal scenario, where the parties receive the noiseless W-state and Eve does not tamper with the state, $Q_Z = 0$.

4. **Classical post-processing:** the N parties use the same authenticated classical channel to perform the usual post-processing, in the form of error correction and privacy amplification. We still consider one-way error correction, where each Bob corrects his key according to Alice's one.

The protocol is similar to the N-BB84 protocol, where the role of KG and PE measurements are switched. Therefore, the key rate of Eq. (4.1) can be written, similarly as for the N-BB84 protocol shown in section 4.1.1, as

$$r_\infty \geq 1 - h(Q_Z) - \max_i h(Q_{AB_i}), \quad (4.10)$$

where Q_Z and Q_{AB_i} are given in Eq. (4.9) and (4.8), respectively. It is worth noting that using the W state for CKA has a major disadvantage with respect to the N-BB84 protocol, in which the parties share a GHZ state: if we consider the perfect scenario, where the shared state is the noiseless W state and Eve does not have any information, the key rate reduces to

$$r_\infty = 1 - h\left(\frac{1}{2} - \frac{1}{N}\right). \quad (4.11)$$

The second term on the right-hand side of the equation is due to the fact that the outcomes of the X-basis measurements on the W state are not perfectly correlated, thus lowering the key rate due to necessary error correction even in the perfect scenario. Moreover, the key rate drops with the number of parties, making this scheme sub-optimal with respect to the N-BB84 protocol, which we have shown to provide perfect key rate in the noiseless scenario.

On the other hand, using W state-based CKA has other major advantages, mainly in terms of practical applications: CKA protocols based on the W state are proven to

be more noise tolerant and easier to implement in near-term applications [Mur+20]. We will discuss these advantages more in detail in chapter 5, where we will also provide concrete examples of practical protocols based on W-state correlations.

4.2 Requirements for Conference Key Agreement

In this section, as an attempt to further investigate the entanglement requirements for CKA protocols, we will finally outline the main results obtained in [Car+21], regarding the resources required to successfully perform a CKA protocol of the class given in section 4.1. The full work can be found in appendix B.

The work takes inspiration from [CLL04], where the authors show that, in the bipartite scenario, entanglement is a necessary resource to successfully perform a QKD protocol. The examples of CKA protocol provided in sections 4.1.1 and 4.1.2 require the parties to share, each round of the protocol, a GME state, where GME is defined in Definition 2.3.7. However, GME states are the most strongly entangled multipartite states and therefore can be challenging to generate. In this scenario, a natural question rises: is it possible to perform a CKA protocol exploiting less strongly entangled states, such as biseparable states defined in Definition 2.3.6? The answer to this question is not trivial, as the structure of multipartite entanglement, outlined in section 2.3.3, is far richer than bipartite entanglement, where a state is either separable (and thus useless for quantum information tasks) or entangled and thus resourceful.

The first result obtained in [Car+21] is a no-go theorem, that tells us that states that are separable with respect to a fixed partition cannot be used in CKA protocols:

Theorem 3. *Given a CKA protocol of the form given in Section 4.1, if the state $\rho_{AB_1, \dots, B_{N-1}}$ shared by the N parties each round of the protocol is separable with respect to a fixed partition $S \setminus \bar{S}$, then $r_\infty = 0$, where r_∞ is defined in Eq. (4.1).*

The proof of the Theorem can be found in [Car+21]. Theorem 3 allows us to exclude states that are separable with respect to a fixed partition from the possible candidates of biseparable states exploitable for CKA. With this limitation in mind, it is possible to design a family of biseparable states that can be employed in CKA protocols. Finally, we note that Theorem 3 is valid for a larger class of protocols than the one considered, that is any protocol with key rate in the form of Eq. (4.1).

4.2.1 Conference Key Agreement with biseparable states

Having excluded a particular class of states, we now focus on finding a family of biseparable states that can be used for CKA. Due to Theorem 3, we know that the

desired states must be entangled across all partitions of the parties. We therefore define the following family of mixed N-partite states:

$$\rho_{AB_1, \dots, B_{N-1}}^{(N,k)} = \sum_{S_\alpha \in \mathcal{S}^{(k)}} \frac{1}{\mathcal{N}} |GHZ\rangle\langle GHZ|_{S_\alpha} \bigotimes_{B_m \in \bar{S}_\alpha} |+\rangle\langle +|_{B_m}, \quad (4.12)$$

where $\mathcal{S}^{(k)}$ is the set of subsets of k parties, for $2 \leq k \leq N-1$, that contain Alice and $k-1$ Bobs, $|GHZ\rangle_{S_\alpha}$ is the GHZ state shared by the k parties of the subset $S_\alpha \in \mathcal{S}^{(k)}$, and \mathcal{N} is a normalization factor, equal to $\mathcal{N} = \binom{N-1}{k-1}$, i.e., the number of subsets of cardinality $k-1$ within the $N-1$ Bobs. We can exclude the trivial cases $k=1$ and $k=N$, since the state would be fully separable and the GHZ state, respectively. Each term of the mixture is composed by the projector on the GHZ state for a subset of k parties and a fully separable state for all the others, summing over all possible subsets of parties.

To better illustrate the shape of the family of states, let us write explicitly the state for $N=3$ and $k=2$:

$$\rho_{AB_1 B_2}^{(3,2)} = \frac{1}{2} (|\psi_+\rangle\langle \psi_+|_{AB_1} \otimes |+\rangle\langle +|_{B_2} + |\psi_+\rangle\langle \psi_+|_{AB_2} \otimes |+\rangle\langle +|_{B_1}), \quad (4.13)$$

where $k=2$ is the only non-trivial value of k for $N=3$ and where we note that the GHZ state for two parties is simply the Bell state $|\psi_+\rangle$ of Eq. (2.50). As a final remark, we note that all states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, with $N \geq 3$ and $2 \leq k \leq N-1$ are biseparable by construction.

Let us now employ this family of states in the N-BB84 protocol, presented in section 4.1.1, to verify whether any of these (biseparable) states lead to a positive key rate, implying the possibility of using them for CKA. Let us then consider the N-BB84 protocol of section 4.1.1, with the "Quantum transmission" step replaced by

- 1a **Quantum transmission:** each round of the protocol N parties, Alice and $\text{Bob}_1, \dots, \text{Bob}_{N-1}$ receive, from an untrusted quantum source the state of Eq. (4.12) for some fixed k .

The rest of the protocol remains unchanged.

It is possible to analytically evaluate the key rate of the protocol, by evaluating the QBERs of Eq. (4.3) and Eq. (4.4) and plugging them in Eq. (4.5). The resulting obtainable key rate is, as a function of N and k , in the following form

$$r_\infty(N, k) = \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \quad (4.14)$$

For completeness we show, in Figure 4.2 (adapted from [Car+21]), a plot of the key rate of the protocol as a function of the number of parties N for different k . Surprisingly, the obtained key rate is positive for all values of N and k , showing that,

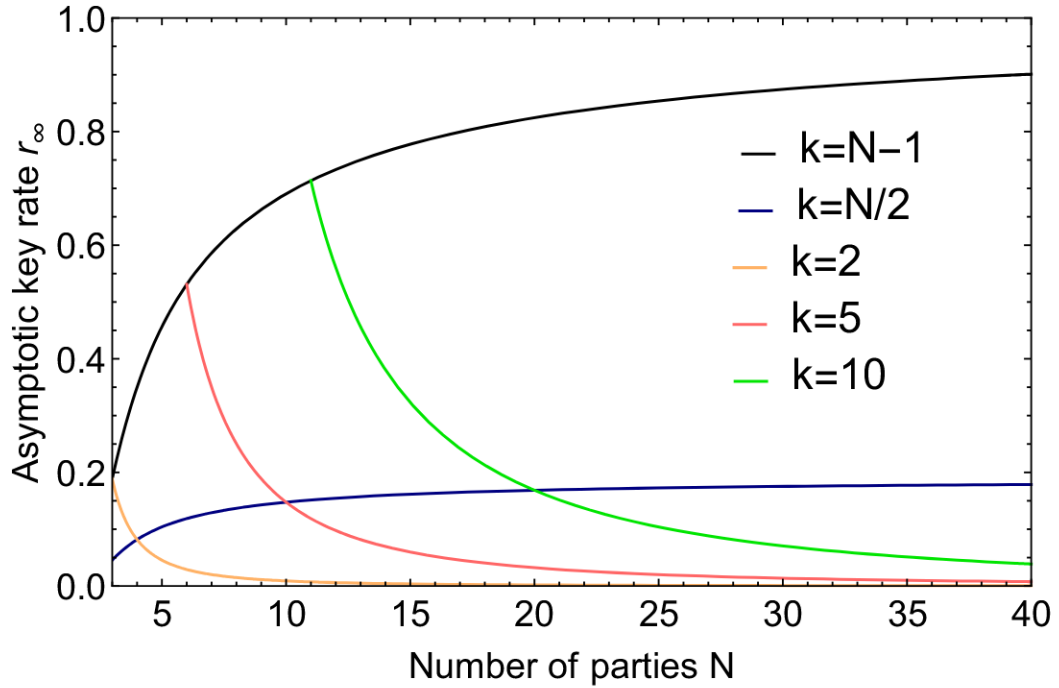


Fig. 4.2.: Asymptotic key rate of the N-BB84 protocol when employing the family of states in Eq. (4.13). The plot is given as a function of the number of parties N for different k . It is interesting to note that for fixed k the key rate decays with the number of parties, whereas if k scales with N the key rate reaches a fixed value for $N \rightarrow \infty$. In the extremal case of $k = N - 1$, meaning that each term of the mixture only one party is not entangled with the others, the key rate $r_\infty \rightarrow 1$ for $N \rightarrow \infty$.

since the states are biseparable by construction, it is not required that a GME state is shared each round of the protocol to successfully establish a secret key with a quantum CKA protocol. Moreover, in [Car+21] it is shown that the N-BB84 protocol is the optimal protocol among the ones described in section 4.1 when using the class of states of Eq. (4.13) and Z-basis measurements for key generation. This is shown by explicitly calculating the key rate of Eq. (4.1), which is much more complicated to evaluate analytically than the key rate of the N-BB84 protocol. Moreover, in [Car+21] a detailed noise analysis is performed together with a discussion on the performance of the protocol compared to a concatenation of bipartite QKD protocols, both of which we will omit here.

The question whether biseparable states can be used in CKA is closely related to another important question about the structure of quantum states, that is whether a set of states is *tensor stable*, or, in other words, whether tensor products of states in the set will still belong to the set. In the bipartite scenario the answer to this question is trivial, since both the sets of entangled and separable states are tensor stable. In the multipartite scenario, where the entanglement structure is more rich

and complicated, the question is not trivial and has been investigated in [Yam+22; PV22].

It is straightforward to show that the set of states that are separable with respect to a fixed partition (and thus also fully separable states) is tensor stable. Moreover, also the set of GME states is tensor stable. However, the interesting part regards the set of biseparable states that are not separable with respect to a fixed partition, which is precisely the set of states investigated in [Car+21]: it turns out that these states are not tensor stable. Furthermore, it is shown that any such state becomes GME, if we consider the tensor product of enough copies of it [PV22]. This result is useful to clarify an apparent contradiction of the results of this section with the results in [Das+21], where the authors show that GME is necessary for CKA. In fact, in [Car+21] we consider the entanglement properties of the single copy of the state shared each round, whereas in [Das+21] the authors consider the properties of the *global state*, resulting from the tensor product of the copies of the state shared each round, which is necessarily GME due to the results in [PV22].

In the same context, a question remains open, that is what are the sufficient conditions on the entanglement properties of the state shared by the parties in order to successfully perform a CKA protocol. Answering this question could lead to bounds on the key rate as a function of the entanglement class the state belongs to, e.g., as a function of the number of entangled parties in each term of the mixture, posing fundamental limitations on the achievable key rate in practical scenarios. Moreover, all results presented concern the asymptotic scenario, which is, as we already discussed, unrealistic for practical applications. An interesting question is thus how these resource play a role in a finite-key analysis, taking into account the effects stemming from dropping the asymptotic key assumption.

4.2.2 Conference key rate as an entanglement witness

The presented results also allow us to gain insight about the detection of multipartite entanglement. As already shown in section 2.3.3, some entangled multipartite states can be detected with *entanglement witnesses*, i.e., hyperplanes separating convex sets from their complements. However, the states we are interested in, i.e., states that are not separable with respect to any partition, do not form a convex set and thus are not detectable in this way.

Nevertheless, following [CLL04], we can construct, using the measurement of the parties in a CKA protocol, a collection of entanglement witnesses detecting entanglement across a specific partition. Moreover, we can consider the key rate of a CKA protocol itself as an entanglement witness, as the quantum state employed in

the CKA protocol must be entangled across all partition for the protocol to succeed. The following Theorem, adapted from [Car+21], better illustrates the claim.

Theorem 4. *Given a CKA protocol in which the parties perform local measurements, for the PE and KG rounds, which are represented by the POVMs $\{G_x^a\}, \{G_{y_1}^{b_1}\}, \dots, \{G_{y_{N-1}}^{b_{N-1}}\}$, where a, b_1, \dots, b_{N-1} indicate the outputs of the measurements labeled by x, y_1, \dots, y_{N-1} , then one can obtain a non-zero asymptotic conference key rate $r_\infty > 0$ only if the presence of entanglement can be proved across any partition of the parties into two subsets.*

Moreover, the presence of entanglement across each bi-partition can be verified through a set of entanglement witnesses of the form

$$W_\alpha = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}, a, b_1, \dots, b_{N-1}}^{(\alpha)} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}} \quad (4.15)$$

where α labels the partition $S_\alpha | \bar{S}_\alpha$, with S_α being a proper subset of the parties and \bar{S}_α is its complement, and where $c_{x, y_1, \dots, y_{N-1}, a, b_1, \dots, b_{N-1}}^{(\alpha)}$ are real coefficients.

We will omit the proof, which can be found in [Car+21]. This Theorem, combined with the insight of section 4.2.1, allows us to formulate the following Corollary.

Corollary 4.2.1. *The figure of merit $r_\infty > 0$ is a non-linear entanglement witness, detecting the presence of entanglement across any bi-partition of the parties.*

This Corollary is due to the following observations: due to Theorem 4, if CKA protocol is performed and a non-zero key rate is obtained, the state shared by the parties each round of the protocol must be entangled across all partitions of the parties. Moreover, since the set of biseparable states entangled across all partitions, i.e., the red set in Figure 2.1, is not convex, a linear witness cannot detect such states. Thus a non-zero key rate is a non-linear witness, capable of detecting states that are biseparable but not separable with respect to any fixed partition.

4.2.3 Biseparable states in the triangle network

Going beyond the work of [Car+21] we now focus on the question of state generation in practical scenarios. Recently a lot of effort [Nav+20; Han+22; WXG22] has been put in investigating a particular class of quantum states, that is states that can be produced in realistic networks where only bipartite sources and shared randomness are available to the parties. Although already many interesting insights were proposed, one further line of research is to analyze the capabilities of such states in quantum cryptographic protocols. In this final section we will briefly outline

this particular class of states and show an interesting result connecting this class of states with the traditional notion of biseparability, relating to the work presented in this section and paving the way for future quantum cryptographic tasks in networks.

Let us first introduce the scenario. Let us restrict to the case of a network, called *triangle network*, comprised of 3 users, called *Alice*, *Bob* and *Charlie*, where each pair of parties receives a quantum bipartite state from a shared source. Moreover, the parties can perform local operations on their systems and have access to a shared random variable λ , which dictates the local operation performed on the source state. We remark that the parties do not have the possibility to perform classical communication.

States that can be generated in the triangle network have the form

$$\rho_{LOSR} = \sum_{\lambda} p_{\lambda} \mathcal{E}_{AA'}^{(\lambda)} \otimes \mathcal{E}_{BB'}^{(\lambda)} \otimes \mathcal{E}_{CC'}^{(\lambda)} [\rho_{AB} \otimes \sigma_{A'C} \otimes \tau_{B'C'}], \quad (4.16)$$

where p_{λ} is a probability distribution associated with the random variable λ , $\mathcal{E}_{AA'}^{(\lambda)}$, $\mathcal{E}_{BB'}^{(\lambda)}$ and $\mathcal{E}_{CC'}^{(\lambda)}$ are the maps representing the quantum local operations of Alice, Bob and Charlie, respectively, and $\rho_{AB} \otimes \sigma_{A'C} \otimes \tau_{B'C'}$ is the source state, which is the tensor product of the 3 bipartite source states between Alice and Bob, Alice and Charlie and Charlie and Bob, respectively. We remark that no assumption has been given about the dimension of the source state or of the final shared state. The scenario is depicted in Figure 4.3.

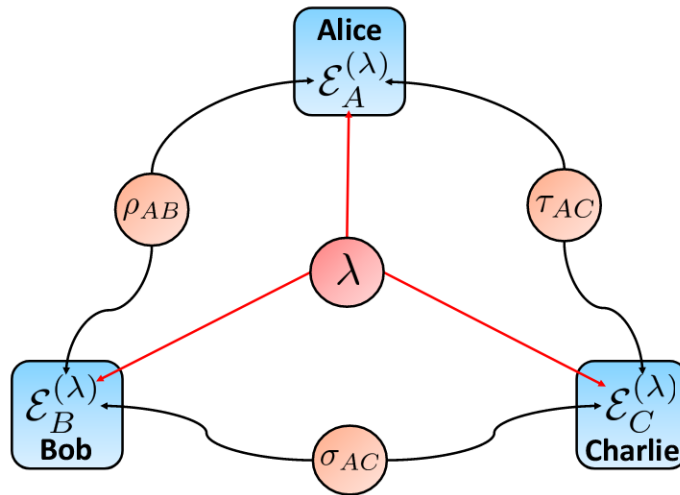


Fig. 4.3.: Depiction of the triangle network scenario. The three parties, Alice, Bob and Charlie, share pairwise independent source states and are then able to perform local operations, coordinated by a shared random variable λ .

Recent works have focused specifically on identifying which quantum states *cannot* be prepared in the triangle network, resulting in no-go theorems ruling out, e.g., the GHZ state, the W state and even a large class of graph states [Han+22; WXG22]. However, it proved to be more challenging to characterize the set of states that *can* be prepared in the triangle network [Nav+20]. In this section we present a preliminary result that could pave the way to characterize the capabilities of triangle network states in particular quantum information tasks. The result is given in the following Theorem.

Theorem 5. *Let us consider a source state $\rho_{source} = \rho_{AB} \otimes \sigma_{A'C} \otimes \tau_{B'C'}$. Then, there exists a biseparable state ρ_{bs} such that*

$$\rho_{source} = \lim_{n \rightarrow \infty} \mathcal{M}_A \otimes \mathcal{M}_B \otimes \mathcal{M}_C \left[\rho_{bs}^{\otimes n} \right], \quad (4.17)$$

where \mathcal{M}_A , \mathcal{M}_B and \mathcal{M}_C are local quantum operations on Alice's, Bob's and Charlie's subsystems, respectively.

The proof of the Theorem can be found in appendix A. The proof also provides an alternative formulation for Theorem 5: the source state can be generated from n copies of ρ_{bs} with a local procedure that fails with a certain probability, with the failure probability exponentially decaying with the number of copies n . Finally, since the states that can be prepared in the triangle network are generated from bipartite source states with local operations coordinated by shared randomness, we have the following Corollary.

Corollary 4.2.2. *The states that can be generated in the triangle network are equivalent to states that can be generated with local operations and shared randomness starting from multiple copies of biseparable states.*

These results could provide some interesting insights on the capabilities of network states in quantum information processes where multiple copies of the same state are required. One example is clearly CKA: as already pointed out, in a CKA protocol, one can consider the global state shared by the parties, described as a tensor product of all the states shared each round of the protocol, which we recall is required to be GME [Das+21]. In considering the global state, Theorem 5 could prove to be an useful tool to compare the capabilities of triangle network states and biseparable states in CKA protocols. Our result thus pave the way for further investigation on the capabilities of network states in quantum cryptographic protocols.

Measurement-Device-Independent protocols

In section 3.2.1 we outlined four fundamental assumptions necessary for QKD and CKA protocols to be secure. The third assumption, namely that the measurement devices are trusted and work precisely as intended, turns out to be the most problematic to meet from a practical point of view. In a realistic implementation, in fact, imperfections in the measurement devices are common, hard to prevent, and have been shown to open the way for powerful eavesdropping attacks [Zha+08; Lyd+10; Ger+11], called *detector side channels*. This chapter is dedicated to presenting a new QKD scheme, namely *Measurement-Device-Independent (MDI) QKD*, which removes the need for this assumption, thus preventing such attacks. We also show how MDI-QKD schemes can be generalized to N-party MDI-CKA schemes and show how such multipartite protocols provide practical solutions for near-term implementations of quantum cryptography.

The chapter is structured as following: section 5.1 is dedicated to introducing MDI protocols. After a brief introduction about quantum optics in section 5.1.1, we show, in section 5.1.2 a basic MDI-QKD protocol and present, in section 5.1.3 one of the main advantages of such scheme, i.e., the capability of beating fundamental bounds on the communication rate. Furthermore, in section 5.1.4 we introduce a multipartite generalization of the protocol of section 5.1.2. Then, in section 5.2, we present some practical MDI-QKD protocols: in section 5.2.1 we introduce a first, simple, MDI bipartite scheme, called *Twin-Field QKD (TF-QKD)*, which is easily implementable with state-of-the-art technology and show its security in section 5.2.2, using the *decoy-state method*. Finally, in section 5.2.3, we analyze in detail our original work, consisting in the design of a multipartite, practical, MDI protocol and show, in section 5.2.4 its capabilities of beating fundamental bounds on communication rates in networks.

5.1 Introduction to MDI protocols

In this section we introduce a new scheme for QKD, and afterwards CKA, protocols, which allows us to drop the assumption of trusted measurement devices, while keeping the need for trusted sources. These protocols are called *Measurement-*

Device-Independent (MDI). MDI schemes require the parties to prepare and send specific states, usually quantum optical states generated with attenuated lasers, to a measurement relay, which, in principle, can be fully controlled by the eavesdropper. The relay announces the outcome of the measurements and the parties are able to extract a shared secret key based on the announcement of the relay, detecting any possible tampering during the classical post-processing phase, as in regular QKD schemes. Since most MDI-QKD protocols are based on quantum optical systems, let us first introduce the rudiments of quantum optics.

5.1.1 Introduction to quantum optics

Quantum optical systems are widely used in quantum information applications, as the technological platforms to generate and control quantum optical states are among the most advanced. In this section we will outline the fundamentals of quantum optics and introduce the states needed for the most common MDI-QKD and -CKA protocols. For a more detailed analysis of quantum optical systems, we refer the reader to [BR97; Leo10].

Quantum optical systems are described, due to the quantization of the electromagnetic field, by an infinite-dimensional Hilbert space \mathcal{H}_F for each quantum optical mode of the system. Each Hilbert space is equipped with a discrete orthonormal basis, called the *Fock basis*, whose states, $\{|n\rangle\}_{n=0}^{+\infty}$, are called *Fock states*. In practice, the Fock state $|n\rangle$ represents a state of n indistinguishable photons in the mode. In particular, The Fock state $|0\rangle$ is called *vacuum state*, as it represents an optical system with no photons. On this Hilbert space, we define a crucial operator called *annihilation operator* \hat{a} , which acts on the Fock states as follows

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle. \quad (5.1)$$

It is thus clear the meaning of the terminology "annihilation operator": acting on an n -photon Fock state, it removes one photon from the state, resulting in the state $|n-1\rangle$. Similarly the Hermitian conjugate of the annihilation operator is called *creation operator* as it adds one photon to any mode, that is

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \quad (5.2)$$

The operator \hat{a} admits a continuous set of eigenstates, indicated by $|\alpha\rangle$ and called *coherent states*. Coherent states can be written in the Fock basis as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \quad (5.3)$$

being an infinite superposition of Fock states. Coherent states are especially relevant from a practical point of view, as they closely approximate the output state of a laser system. Therefore, they are better suited for near-term applications than, e.g., Fock states, which need more complicated devices to be generated.

Quantum optical states can be manipulated with linear optical devices. One important example is a simple passive optical device called *Beam-Splitter (BS)*, that admits two input systems, described by the optical modes \hat{a} and \hat{b} and two output systems, described by optical modes \hat{d} and \hat{c} . The action of a BS is described by the unitary operator

$$\hat{U}_{BS}(\xi) = e^{\xi\hat{a}^\dagger\hat{b} - \xi^*\hat{b}^\dagger\hat{a}}, \quad (5.4)$$

where $\xi = r e^{i\phi}$, which transforms the input modes into the output modes according to

$$\begin{aligned} \hat{c} &= \hat{U}_{BS}^\dagger(\xi)\hat{a}\hat{U}_{BS}(\xi) = \hat{a} \cos(r) + \hat{b} \sin(r)e^{i\phi} \\ \hat{d} &= \hat{U}_{BS}^\dagger(\xi)\hat{b}\hat{U}_{BS}(\xi) = \hat{b} \cos(r) - \hat{a} \sin(r)e^{-i\phi}. \end{aligned} \quad (5.5)$$

A specific instance of a BS is the so-called *Balanced Beam-Splitter (BBS)*, with $\phi = 0$ and $r = \frac{\pi}{4}$, such that the transformation of the modes, determined in this case by the unitary evolution \hat{U}_{BBS} reads

$$\begin{aligned} \hat{c} &= \hat{U}_{BBS}^\dagger\hat{a}\hat{U}_{BBS} = \frac{\hat{a} + \hat{b}}{\sqrt{2}} \\ \hat{d} &= \hat{U}_{BBS}^\dagger\hat{b}\hat{U}_{BBS} = \frac{\hat{b} - \hat{a}}{\sqrt{2}}. \end{aligned} \quad (5.6)$$

To close this section, we present one example of how a BBS acts on a quantum optical system. Let us consider, as input states of a BBS, one coherent state $|\alpha\rangle_{\hat{a}_1}$, representing the state of a laser beam of intensity $|\alpha|^2$, and the vacuum state $|0\rangle_{\hat{a}_2}$, representing the fact that the second input port is left untouched. It is possible to show that the output state is $\left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\hat{b}_1} \left|\frac{\alpha}{\sqrt{2}}\right\rangle_{\hat{b}_2}$ which has a clear operational interpretation: the laser beam is split into two laser beams of intensity $\frac{|\alpha|^2}{2}$ each. Moreover, one can easily calculate the output state of the BBS when two coherent states $|\alpha\rangle_{\hat{a}_1}$ and $|\beta\rangle_{\hat{a}_2}$ are sent into the input ports of a BBS, which reads

$$|\psi_{out}\rangle = \left|\frac{\alpha + \beta}{\sqrt{2}}\right\rangle_{\hat{b}_1} \left|\frac{\beta - \alpha}{\sqrt{2}}\right\rangle_{\hat{b}_2}, \quad (5.7)$$

meaning that the amplitudes of the coherent states are mixed in the same way as the modes.

5.1.2 Ideal MDI-QKD protocol

We now have all the tools to present one of the most commonly employed MDI-QKD protocols, which is particularly relevant due to the scaling properties of its key rate with the communication distance, as we will see in section 5.1.3. We mainly follow the work of [CAL19], where this protocol serves as an idealized base to build a more practical and easily implementable scheme, which we will present in section 5.2.1. The MDI-QKD protocol is described as following:

1. **Quantum transmission:** both Alice and Bob prepare, each round of the protocol, an entangled state between an optical mode and a qubit system of the form

$$|\psi\rangle_{\hat{a}_i Q_i} = \sqrt{q}|0\rangle_{\hat{a}_i}|0\rangle_{Q_i} + \sqrt{1-q}|1\rangle_{\hat{a}_i}|1\rangle_{Q_i}, \quad (5.8)$$

where \hat{a}_i labels the optical mode, with the states $|n\rangle_{\hat{a}_i}$ being Fock states of that mode, and Q_i labels the qubit system for each party, with $i \in \{A, B\}$. Both parties then send the optical mode through a lossy quantum channel, with transmittance $\sqrt{\eta}$, to a central, untrusted relay. The lossy channel is modelled as mixing the signal in a BS, described in section 5.1.1, with $\sqrt{\eta} = \cos(r)$ in Eq. (5.5), with a second input mode in the vacuum state. Moreover, the second output mode of the BS is not measured, representing the part of the signal that is lost. The qubit system is stored by the parties by means of a quantum memory.

2. **Relay operations:** in the relay the two input modes, namely \hat{a}_A and \hat{a}_B , coming from Alice and Bob, respectively, are mixed in a BBS, described in section 5.1.1. The two output modes, namely \hat{c} and \hat{d} are then measured with *threshold detectors* D_c and D_d , which detect the presence of one or more photons in the mode, but are not able to resolve the photon number. The relay finally announces the outcomes of the measurements, by publicly disclosing the values $k_c = 1$ or $k_d = 1$ if the respective detector clicked or $k_c = 0$ or $k_d = 0$ if the respective detector did not click.
3. **Quantum measurement:** Alice and Bob perform, each round of the protocol, one of two measurement on the stored qubit system. In KG rounds they measure on the X-basis and in PE rounds they measure on the Z-basis.
4. **Classical post-selection and parameter estimation:** Alice and Bob only keep the rounds where they measured in the same basis and only keep rounds where $k_c \oplus k_d = 1$, i.e., where only one detector clicked and discard the rest. We call this phase of the protocol *post-selection phase*. They then disclose, through an authenticated classical channel, part of the measurements outcomes in both

bases. They use the disclosed data in the Z-basis to evaluate the *phase-error rate* Q_Z defined as

$$Q_Z = p_Z(Z_A = Z_B | k_c \oplus k_d = 1), \quad (5.9)$$

that is, the probability that the outcomes in the Z-basis are the same, conditioned on the event that only one detector clicked. Similarly, they use the disclosed data in the X-basis to evaluate the *quantum bit error rate (QBER)* Q_{AB} defined as

$$Q_{AB} = p_X(X_A \neq X_B \oplus k_d | k_c \oplus k_d = 1), \quad (5.10)$$

that is, the probability that the simulated outcomes of the X-basis measurement are different (taking into account a correction due to the BS evolution) conditioned on the event that only one detector clicked.

5. **Classical post-processing:** Alice and Bob use the same authenticated classical channel to perform the usual post-processing, in the form of error correction and privacy amplification.

Let us now explain the basic idea behind the protocol. Let us imagine that the parties prepare their states with $1 - q \approx 0$, i.e., a state preparation heavily biased towards the vacuum. In this case, the one-click events happen, with high probability, due to single-photon transmission, meaning that only one photon was sent, either by Alice or by Bob. However, due to the BBS in the relay, the parties lose the information about which party effectively sent the photon. Therefore, since the photons are entangled with the qubit system, the resulting state of the qubit conditioned on the one-click event is

$$|\phi_{k_d}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + (-1)^{k_d}|10\rangle), \quad (5.11)$$

which coincides with one of two Bell states in Eq. (2.50), depending on k_d . Therefore, the protocol, after the post-selection, reduces to a simple EB-BB84 protocol, shown in section 3.2.2, whose key rate can be written as

$$r_\infty \geq 2p_{click} [1 - h(Q_{AB}) - h(Q_Z)], \quad (5.12)$$

where p_{click} is the probability that Alice and Bob chose the same basis and only one detector clicks and accounts for the discarded rounds in the post-selection phase. We note that, in a general protocol, we should consider two different key rates $r_\infty^{(k_c=1)}$ and $r_\infty^{(k_d=1)}$ depending on which detector clicks and the total key rate would be the sum of the two, that is $r_\infty = r_\infty^{(k_c=1)} + r_\infty^{(k_d=1)}$. However in the proposed protocol,

due to its symmetries, the key rate does not depend on which detector clicks, thus the form of the key rate of Eq. (5.12).

The protocol is EB, as Alice and Bob are required to generate entangled states between an optical mode and a qubit system. This requirement can be a substantial challenge from a practical point of view and thus an equivalent PM formulation would be desirable. Indeed, we can note that the measurement on the qubit system commutes with all the operations of the relay: the parties could therefore measure the qubit system independently from the announcement of the measurement outcome from the relay, and use the information disclosed by the relay only in the (classical) post-selection phase. The parties can therefore simulate the quantum measurement on the qubit system with an appropriate random variable and send an appropriate state of the optical mode, making the protocol PM. The equivalent PM protocol is identical to the one presented above, where the "Quantum transmission" and "Quantum measurement" phases are replaced by the following:

- 1a. **Quantum transmission:** Alice and Bob label each round, e.g. according to a pre-shared key, as a KG or PE round. In PE rounds Alice and Bob prepare an optical mode in the state $|0\rangle_{\hat{a}_i}$ with probability q , corresponding to the Z-basis measurement outcome $Z_i = +1$ and $|1\rangle_{\hat{a}_i}$ with probability $1 - q$, corresponding to the Z-basis measurement outcome $Z_i = -1$. The states $|n\rangle_{\hat{a}_i}$ are Fock states of the corresponding mode and $i = \{A, B\}$. In KG rounds Alice and Bob prepare an optical mode in the state $|+_q\rangle_{\hat{a}_i} = \sqrt{q}|0\rangle_{\hat{a}_i} + \sqrt{1-q}|1\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = +1$ and $|-_q\rangle_{\hat{a}_i} = \sqrt{q}|0\rangle_{\hat{a}_i} - \sqrt{1-q}|1\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = -1$. Both parties then send the optical mode through a lossy quantum channel, with transmittance $\sqrt{\eta}$, to a central, untrusted, relay.

The rest of the protocol is left unchanged. This equivalent PM formulation of the protocol has the same performance of the original protocol but with much more limited practical requirements. However, the parties are still required to generate single-photon optical states, which can be a challenging practical requirement. We will see, in section 5.2.1, how to lift this requirement, by looking at a similar protocol which requires only laser pulses.

5.1.3 Overcoming fundamental limitation on the communication rate

The protocol introduced in the previous section takes into account the most relevant source of noise in practical application, i.e., transmission loss. In fact, in realistic implementations that rely on optical sources, photon loss is the main obstacle

for long-distance communication. As already pointed out, photon loss can be modelled as a channel with transmittance η , where η is the probability that a photon is successfully transmitted. One example is given by telecom fibers, where the transmittance is given by $\eta = 10^{-\frac{\alpha_f L}{10}}$, where L represents the length of the fiber and α_f is an optical attenuation parameter, which is equal to $\alpha_f = 0.2 \text{ dB km}^{-1}$ for modern fibers. We remark that this behavior can severely limit the communication distance, as the transmittance decays exponentially with the distance. For long distance communication it is thus crucial to analyze how the protocol, and therefore the key rate, behave as a function of the losses.

Interestingly, there exists some limitations on the achievable key rate of any protocol performed by Alice and Bob, if they are connected by a lossy channel with transmittance η [Pir+17; TGW14]. Particularly interesting is the result of [Pir+17], where the authors show an upper bound on the achievable key rate of any QKD protocol, which reads

$$r_\infty \leq -\log_2(1 - \eta) := r_{PLOB}, \quad (5.13)$$

usually referred to as Pirandola-Ottaviani-Bianchi-Laurenza (PLOB) bound. For $\eta \ll 1$, the PLOB bound scales linearly with η and thus exponentially with the distance, severely limiting the communication capabilities of any protocol. This bound however, can be overcome by employing intermediate stations in the quantum channel, leading to a possibly better scaling of the key rate with the distance.

In particular, in the MDI-QKD protocol presented in section 5.1.2, each party is connected to the untrusted relay with a channel of transmittance $\sqrt{\eta}$ making the total channel connecting Alice and Bob having transmittance η . In other words, the intermediate measuring station "breaks" the total channel of transmittance η into two channels of transmittance $\sqrt{\eta}$. Thus, the aforementioned protocol has the striking feature of being able to overcome the PLOB bound in the high loss regime, making it extremely appealing for long-distance communication.

More in detail, the key rate of Eq. (5.12), in the limit of highly biased preparation $1 - q \approx 0$, reduces to $r_\infty \approx 2(1 - q)q\sqrt{\eta}$, thus showing an improved scaling on $\sqrt{\eta}$ with respect to the linear scaling of the PLOB bound. The protocol is thus able to overcome the PLOB bound in high loss regimes, as shown, e.g., in Figure 1 of [CAL19]. The intuitive reason for this behavior is the following: since the protocol is based on single-photon transmission, it is sufficient that only one photon, either from Alice or from Bob is successfully transmitted each round of the protocol. This happens with probability $\sqrt{\eta}$, as the channel connecting each party with the relay has transmittance $\sqrt{\eta}$, with the total channel connecting Alice and Bob having transmittance η . Therefore, the key rate scales only with $\sqrt{\eta}$, allowing for high-distance communication even beyond the PLOB bound.

5.1.4 Ideal MDI-CKA protocol

Due to the advantages provided by the scheme presented in section 5.1.2 over usual QKD schemes in terms of scaling of the key rate with channel losses, it is natural to ask whether it is possible to generalize such scheme to many parties. This section is thus devoted to presenting a MDI-CKA scheme based on single photon interference, which retains the main advantage of the protocol of section 5.1.2, i.e., the scaling of the key rate with $\sqrt{\eta}$. One of the most relevant attempts was given in [GKB19]. The first part of our work of [CMG23] was to reformulate the protocol of [GKB19] to allow for a practical implementation, which we will show in section 5.2.3. In the following we will present directly our formulation of the protocol, that is the ideal protocol of [CMG23].

The protocol, performed by N parties labelled as A_0, \dots, A_{N-1} , is described as following:

1. **Quantum transmission:** each party A_i prepares, each round of the protocol, an entangled state between an optical mode and a qubit system of the form

$$|\psi\rangle_{\hat{a}_i Q_i} = \sqrt{q}|0\rangle_{\hat{a}_i}|0\rangle_{Q_i} + \sqrt{1-q}|1\rangle_{\hat{a}_i}|1\rangle_{Q_i}, \quad (5.14)$$

where \hat{a}_i labels the optical mode, with the states $|n\rangle_{\hat{a}_i}$ being Fock states of that mode, and Q_i labels the qubit system for each party. All parties then send the optical mode through a lossy quantum channel, with transmittance $\sqrt{\eta}$, to a central, untrusted relay.

2. **Relay operations:** in the relay, the incoming optical modes go through a BBS network of $M = 2^s$ inputs and outputs, with $M \geq N$. The BBS network is sketched in Figure 5.2 for $N = 4$ and described in detail in Appendix A of [CMG23]. The BBS network transforms the input modes, described by the respective creation operators $\hat{a}_0^\dagger, \dots, \hat{a}_{M-1}^\dagger$ into the output modes $\hat{d}_0^\dagger, \dots, \hat{d}_{M-1}^\dagger$, according to

$$\hat{a}_i^\dagger \rightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} (-1)^{\vec{k} \cdot \vec{i}} \hat{d}_k^\dagger, \quad (5.15)$$

where \vec{i} and \vec{k} are the binary representation of the integers i and k , respectively. We note that, since in principle $N \leq M$, the M modes $\hat{a}_0^\dagger, \dots, \hat{a}_{M-1}^\dagger$ represent the N signals coming from the parties paired with additional $M - N$ modes in the vacuum state. The output modes are then measured with threshold detectors D_0, \dots, D_{M-1} , to certify the arrival of one (or more) photon at the detector. The relay finally announces the outcomes of the measurements of each detector $D_j \forall 0 \leq j \leq M - 1$, by publicly disclosing the values $k_j = 1$ if the respective detector clicked or $k_j = 0$ if the detector did not click.

3. **Quantum measurement:** the parties perform, each round of the protocol, one of two measurement on the stored qubit system. In KG rounds they measure on the X-basis and in PE rounds they measure on the Z-basis.
4. **Classical post-selection and parameter estimation:** the parties only keep rounds where they all measured in the same basis. Moreover, they keep only rounds where one detector, e.g. D_j , clicked and discard the rest. We call this phase of the protocol *post-selection phase*. Each party A_i also flips the outcome of their X-basis measurements if $(-1)^{\vec{i}\cdot\vec{j}} = -1$. They then disclose, through an authenticated classical channel, part of the measurements outcomes in both bases. They use the disclosed data in the Z-basis to evaluate the *phase-error rate* defined as

$$Q_Z^j = \Pr\left(\prod_{i=0}^{N-1} Z_i = 1 \mid k_j = 1\right), \quad (5.16)$$

that is, the probability that the outcomes in the Z-basis are all the same, conditioned on the event that only detector D_j clicked. Similarly, they use the disclosed data in the X-basis to evaluate the *pair-wise quantum bit error rate (QBER)* Q_{X_0, X_i}^j defined as

$$Q_{X_0, X_i}^j = \Pr\left(X_0 \neq (-1)^{\vec{i}\cdot\vec{j}} X_i \mid k_j = 1\right), \quad (5.17)$$

that is, the probability that the outcomes of the X-basis of parties A_0 and A_i are different, conditioned on the event that only detector D_j clicked. These error rates are estimated for each detector D_j .

5. **Classical post-processing:** the parties use the same authenticated classical channel to perform the usual post-processing, in the form of pair-wise error correction, where all the parties correct their keys according to party A_0 's one (hence the definition of the QBER in Eq. (5.17)) and privacy amplification.

This protocol, being analogous to the one shown in section 5.2.1, is still based on single-photon interference. In fact, if the state preparation is heavily biased, i.e., $1 - q \approx 0$, the events where only one detector clicks happen in rounds where only one party sends a photon and all the others send the vacuum. However the BBS network, mixing all modes in a balanced way, erases the information about which party sent the photon and therefore which party's qubit state is $|1\rangle$. Therefore, the post-selected state of the qubits when detector D_j clicks can be described as

$$|W_j\rangle_{Q_0, \dots, Q_{N-1}} := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{i}\cdot\vec{j}} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}}, \quad (5.18)$$

where \vec{b}_i is a binary vector with zeros in all positions except for position i , where it has a one. The state is analogous to a W state, defined in Eq. (4.6), where some terms have a -1 sign. However, the protocol is designed to correct for this sign, such that in the end the parties hold a proper W state. In fact, the parties flip their outcome in the X-basis if $(-1)^{\vec{i} \cdot \vec{j}} = -1$, which is equivalent to applying, before the measurement, for each qubit system Q_i , the operator $\hat{Z}^{\vec{i} \cdot \vec{j}}$, where \hat{Z} is the Pauli Z operator of Eq. (2.39). The resulting state is therefore

$$\begin{aligned}
|W_j\rangle_{Q_0, \dots, Q_{N-1}} &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{i} \cdot \vec{j}} \bigotimes_{k=0}^{N-1} Z^{\vec{k} \cdot \vec{j}} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}} \\
&= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{i} \cdot \vec{j}} (-1)^{\vec{i} \cdot \vec{j}} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}} \\
&= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}}, \tag{5.19}
\end{aligned}$$

which corresponds to the W state of Eq. (4.6).

The rest of the protocol thus is analogous to the one in section 4.1.2. It is worth noting that the protocol is designed to also keep the same scaling properties of the protocol of section 5.1.2, i.e., the scaling of the key rate with $\sqrt{\eta}$, since it is similarly based on single-photon events and thus the key rate scales with the probability that only one photon is transmitted. As we will see in section 5.2.3 for the practical version of this protocol, this feature allows this scheme to overcome fundamental bounds on communication rates in networks, similar to the PLOB bound. The key rate of the protocol can be calculated as

$$r_\infty \geq \sum_{j=1}^M p_j (1 - h(Q_Z^j) - \max_i h(Q_{X_0, X_i}^j)), \tag{5.20}$$

where p_j is the probability that detector D_j clicks and Q_Z^j and Q_{X_0, X_i}^j are the error rates defined in Eqs. (5.16) and (5.17). In this expression we take into account the post-selection by including the probability that each detector clicks and generalize the key rate to include multipartite post-processing, where all parties perform error correction to match the first party's key.

Finally, following the same arguments of section 5.1.2, we can give a PM formulation of this protocol. We can replace the "Quantum transmission" and "Quantum measurement" phases with the following

- 1a. **Quantum transmission:** each party A_i labels each round, e.g. according to a pre-shared key, as a KG or PM round. In PE rounds each party A_i prepares an optical mode in the state $|0\rangle_{\hat{a}_i}$ with probability q , corresponding to the

Z-basis measurement outcome $Z_i = +1$ and $|1\rangle_{\hat{a}_i}$ with probability $1 - q$, corresponding to the Z-basis measurement outcome $Z_i = -1$. The states $|n\rangle_{\hat{a}_i}$ are Fock states of the corresponding mode. In KG rounds each party A_i prepares an optical mode in the state $|+q\rangle_{\hat{a}_i} = \sqrt{q}|0\rangle_{\hat{a}_i} + \sqrt{1-q}|1\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = +1$ and $|-q\rangle_{\hat{a}_i} = \sqrt{q}|0\rangle_{\hat{a}_i} - \sqrt{1-q}|1\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = -1$. All parties then send their respective optical mode through the same lossy quantum channel, with transmittance $\sqrt{\eta}$, to a central, untrusted, relay.

The rest of the protocol remains unchanged. This PM formulation is equivalent to the EB one, achieving the same performances and key rate. Once again, this formulation also allows for further practical simplifications of the protocol, as we will see in section 5.2.3.

5.2 Practical protocols

The protocols presented in section 5.1 have several desirable features, the most important of which being the ability to achieve long-distance communication, but also drawbacks that limit their applicability in practice. In fact, the protocols, in their PM formulation, require the parties to generate single-photon states, which could represent a substantial challenge with the currently available technology. In this section we will show how to overcome this practical challenge, by modifying the protocol of section 5.1.2 to be implemented with more accessible states than single-photon states, i.e., coherent states.

Many bipartite protocols of such nature, usually referred to as *Twin-Field QKD (TF-QKD)* protocols, have already been proposed [Luc+18; CAL19; WYH18; Cui+19] and experimentally implemented [Min+19; Liu+19; Wan+19; Fan+20; Che+20; Pit+21; Liu+21a; Che+21; Cli+22; Wan+22; Che+22], but only few multipartite generalizations have been proposed [Cao+21b; Cao+21a; Bai+22], and they are limited in the number of parties as well as not being MDI. In this section, after analyzing one of the most relevant TF-QKD protocol, i.e., the practical version of the protocol shown in section 5.1.2, we illustrate the practical version of the CKA protocol in section 5.1.4 that we introduced in [CMG23].

5.2.1 Twin-Field QKD

In this section we will present the TF-QKD protocol of [CAL19], which is a practical version of the PM formulation of the protocol of section 5.1.2. We focus on this

particular TF-QKD protocol, which is not the first one to be proposed (the first one being the one in [Luc+18]), because of its elegant security proof and remarkable performance at high losses. The protocol, given in its PM formulation, is described as following:

1. **Quantum transmission:** Alice and Bob label each round, e.g. according to a pre-shared key, as a KG or PM round. In KG rounds Alice and Bob each prepare an optical mode in the state $|\alpha\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = +1$, or $|-\alpha\rangle_{\hat{a}_i}$, corresponding to the X-basis measurement outcome $X_i = -1$. The states $|\alpha\rangle$ are coherent states, described in section 5.1.1, and $i = \{A, B\}$. In PE rounds Alice and Bob each prepare an optical mode in the state

$$\rho_{\beta_i} = \frac{1}{2\pi} \int_0^{2\pi} d\phi |e^{i\phi}\beta_i\rangle \langle e^{i\phi}\beta_i|, \quad (5.21)$$

where the amplitude β_i is chosen at random from a finite set \mathcal{S} . The state is called *phase-randomized coherent state (PRCS)*, as it represents a coherent state with a random, unknown phase. Both parties then send the optical mode through a lossy quantum channel, with transmittance $\sqrt{\eta}$, to a central, untrusted, relay.

2. **Relay operations:** in the relay, the two input modes, namely \hat{a}_A and \hat{a}_B , coming from Alice and Bob, respectively, are mixed in a BBS, described in Section 5.1.1. The two output modes, namely \hat{c} and \hat{d} are then measured with *threshold detectors* D_c and D_d , which detect the presence of one or more photons in the mode, but are not able to resolve the photon number. The relay finally announces the outcomes of the measurements, by publicly disclosing the values $k_c = 1$ or $k_d = 1$ if the respective detector clicked or $k_c = 0$ or $k_d = 0$ if the respective detector did not click.
3. **Classical post-selection and parameter estimation:** Alice and Bob only keep rounds where they chose the same basis and where $k_c \oplus k_d = 1$, i.e., where only one detector clicked, and discard the rest. We call this phase of the protocol *post-selection phase*. They then disclose, through an authenticated classical channel, part of the simulated X-basis measurement outcomes. They use the disclosed data in the X-basis to evaluate the *quantum bit error rate (QBER)* Q_{AB} , defined as

$$Q_{AB} = \Pr(X_A \neq X_B \oplus k_d | k_c \oplus k_d = 1), \quad (5.22)$$

that is, the probability that the simulated outcomes of the X-basis measurement are different (taking into account a correction due to the BS evolution) conditioned on the event that only one detector clicked. Similarly, for PE rounds, they disclose the choices of intensities (β_A, β_B) and estimate the so-called *gains* defined as

$$G_{\beta_A, \beta_B}^{k_c, k_d} := \Pr(k_c, k_d | \beta_A, \beta_B), \quad (5.23)$$

that is, the probability to obtain the detection pattern (k_c, k_d) given the choice of intensities (β_A, β_B) , where $\beta_A, \beta_B \in \mathcal{S}$.

4. **Classical post-processing:** Alice and Bob use the same authenticated classical channel to perform the usual post-processing, error correction and privacy amplification.

In Figure 5.1 we show a schematic representation of the protocol.

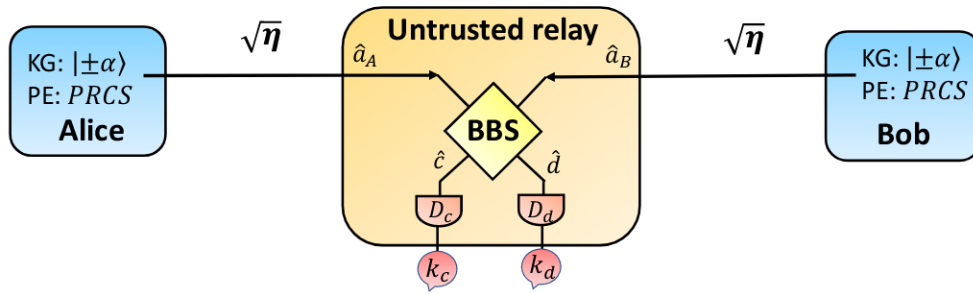


Fig. 5.1.: Schematic representation of the TF-QKD protocol. The protocol is PM and MDI, as Alice and Bob communicate with an untrusted relay and use the public announcement of the relay to establish a secret shared key. The main feature of the protocol is that it has extremely limited practical requirements: Alice and Bob only need to generate coherent states and PRCS and, in an honest implementation, the relay only needs a single BBS, described in section 5.1.1.

The basic idea behind the protocol is the following. If we consider the PM formulation of the ideal protocol in section 5.1.2, the parties prepare, in the KG rounds, the optical states $|\pm_q\rangle = \sqrt{q}|0\rangle \pm \sqrt{1-q}|1\rangle$, where $|0\rangle$ and $|1\rangle$ are single-photon states. From Eq. (5.3), it is straightforward to see that, for $|\alpha|^2 \ll 1$, a coherent state is well approximated by

$$|\pm\alpha\rangle \approx e^{-\frac{|\alpha|^2}{2}} |0\rangle \pm \alpha e^{-\frac{|\alpha|^2}{2}} |1\rangle, \quad (5.24)$$

which coincides with the states required in the protocol for an appropriate choice of α . We can thus replace, in KG rounds, with good approximation, the states $|\pm_q\rangle$ with

$|\pm\alpha\rangle$, the latter being much simpler to generate. As for PE rounds, the states sent by Alice and Bob are the Fock states $|0\rangle$ or $|1\rangle$. In the ideal protocol the phase-error rate Q_Z is thus related to the probability of the parties sending no photons or more than one photon and still obtaining a click in the detector. We will see in the next section how the PRCS used in the practical protocol can be used to estimate the phase-error rate efficiently.

5.2.2 Security proof and decoy-state method

In this section we will outline the security proof of the practical TF-QKD protocol presented in the previous section and show how the key rate of the protocol is estimated. The key rate obtained in the practical protocol is identical to the one given in Eq. (5.12). The main difference from the ideal MDI-QKD protocol of section 5.1.2 is how the parties estimate the error rates. As briefly outlined in the previous section, the parties are able to estimate the QBER simply from the results of their simulated measurement in the X-basis. In fact, the QBER is defined as in Eq. (5.10) and the parties, in the protocol, are able to estimate the probability of a certain detection pattern given their simulated outcomes in the X basis, i.e., $\Pr(k_c, k_d|X_A, X_B)$. Using Bayes' rule, one can straightforwardly estimate Q_{AB} of Eq. (5.10) using the aforementioned probabilities. The estimation of the phase-error rate of Eq. (5.12), however, is more involved and requires the introduction of a well-known technique used in such scenarios, called *decoy-state method*.

To estimate the phase-error rate, let us consider the equivalent EB version of the TF-QKD protocol of section 5.2.1. In KG rounds, the parties can equivalently prepare the following entangled state:

$$|\psi\rangle_{\hat{a}_i, Q_i} = \frac{1}{\sqrt{2}}(|+\rangle_{Q_i}|\alpha\rangle_{\hat{a}_i} + |-\rangle_{Q_i}|-\alpha\rangle_{\hat{a}_i}), \quad (5.25)$$

where Q_i is a qubit system, \hat{a}_i an optical mode and $i = \{A, B\}$. Furthermore, they equivalently measure the qubit system in the X-basis, while sending the optical mode to the relay, as in the EB formulation of the ideal protocol of section 5.1.2. Therefore, the state after the operations and announcements of the outcomes of the relay is described as

$$|\chi_{k_c, k_d}\rangle_{Q_A Q_B E} = \frac{\hat{K}_{k_c, k_d}(|\psi\rangle_{\hat{a}_A, Q_A} \otimes |\psi\rangle_{\hat{a}_B, Q_B})}{\sqrt{p(k_c, k_d)}}, \quad (5.26)$$

where the operator \hat{K}_{k_c, k_d} represents the operations and measurements of the relay which could be, we recall, controlled by Eve (hence Eve's system on the left-hand side of the equation) and $p(k_c, k_d)$ is the probability that the detection pattern

(k_c, k_d) occurs. In this formulation, we can write the phase-error rate, affecting Z-basis measurements on this state, as

$$Q_Z = \sum_{i=0}^1 \|\langle ii | \chi_{k_c, k_d} \rangle_{Q_A Q_B E}\|^2. \quad (5.27)$$

The main point of the security proof performed in [CAL19] is thus to find an upper bound on this quantity which can be estimated in the protocol. The derived expression for the upper bound reads

$$\bar{Q}_Z = \frac{1}{p(k_c, k_d)} \left[\left(\sum_{n,m=0}^{\infty} c_{2n} c_{2m} \sqrt{\Pr(k_c, k_d | 2n, 2m)} \right)^2 + \left(\sum_{n,m=0}^{\infty} c_{2n+1} c_{2m+1} \sqrt{\Pr(k_c, k_d | 2n+1, 2m+1)} \right)^2 \right], \quad (5.28)$$

where $\Pr(k_c, k_d | n, m)$ is the probability of obtaining the detection pattern (k_c, k_d) given that the parties sent Fock states $|n\rangle$ and $|m\rangle$ to the relay and where $c_n = e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}}$. The probabilities $\Pr(k_c, k_d | n, m)$ are usually referred to as *yields* and indicated by $Y_{n,m}^{k_c, k_d}$.

It is important to note that the parties are not able to estimate the yields directly in the protocol, as Fock states are hard to generate and manipulate. However, the parties can estimate the yields from the gains of Eq. (5.23) using the so-called *decoy-state method*. This technique was firstly proposed in [Hwa03; Wan05; LMC05] for generic MDI-QKD protocols and employed for TF-QKD in [CAL19; GC19; GNC19]. Let us consider the state that the parties generate in PE rounds, i.e., the PRCS of Eq. (5.21). The state can be equivalently written, as a mixture of Fock states, as

$$\rho_{\beta_i} = e^{-|\beta_i|^2} \sum_{n=0}^{\infty} \frac{|\beta_i|^{2n}}{n!} |n\rangle \langle n|_{\hat{a}_i}. \quad (5.29)$$

Using this expression for PRCSs, we can write the gains as

$$G_{\beta_A, \beta_B}^{k_c, k_d} = e^{-|\beta_A|^2 - |\beta_B|^2} \sum_{n,m=0}^{\infty} \frac{|\beta_A|^{2n} |\beta_B|^{2m}}{n! m!} Y_{n,m}^{k_c, k_d}, \quad (5.30)$$

where, we recall, each β_i is chosen from a discrete set of intensities \mathcal{S} . The latter expression corresponds to a different equation for each choice of intensities with the same unknown variables, that is, the yields.

We then obtain a system of equations, where the unknowns are the (infinite) yields and the known variables are the gains. The system can be solved exactly

if we consider the unrealistic scenario where the parties can choose from a set of infinite decoys. However, even with a finite amount of decoy amplitudes, we can still derive an upper bound on a finite amount of yields and bound the remaining ones trivially with 1, since they are probability distributions. Therefore the parties are able to estimate the yields, and consequently the phase-error rate, using the statistics obtained in the protocol, thus obtaining an estimation of the information leaked to Eve, leading to a secure protocol. As a final remark we note that, even in its practical implementation, the protocol retains the most desirable property of the original MDI-QKD protocol presented in section 5.1.2, i.e, the scaling of the key rate with $\sqrt{\eta}$ and therefore the possibility of beating the PLOB bound as shown in section 5.1.3 (see [CAL19] for further details).

5.2.3 Practical MDI-CKA protocol

In this final section we present our work from [CMG23], where one of the first practical multipartite protocols based on single-photon interference was proposed. The protocol is a practical version of the MDI-CKA protocol presented in section 5.1.4, in the same way as TF-QKD is a practical version of the protocol in section 5.1.2. Let us start with the description of the protocol, performed by N parties labelled as A_0, \dots, A_{N-1} .

1. **Quantum transmission:** each party labels each round, e.g. according to a pre-shared key, as a KG or PM round. In KG rounds each party A_i prepares an optical mode in the state $|\alpha\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = +1$, or $|-\alpha\rangle_{\hat{a}_i}$ with probability $\frac{1}{2}$, corresponding to the X-basis measurement outcome $X_i = -1$. The state $|\alpha\rangle$ is a coherent state, defined in Eq. (5.3). In PE rounds each party A_i prepares an optical mode in the state

$$\rho_{\beta_i} = \frac{1}{2\pi} \int_0^{2\pi} d\phi |e^{i\phi}\beta_i\rangle \langle e^{i\phi}\beta_i|, \quad (5.31)$$

where the amplitude β_i is chosen at random from a finite set \mathcal{S} . All parties then send the optical mode through a lossy quantum channel, with transmittance $\sqrt{\eta}$, to a central, untrusted, relay.

2. **Relay operations:** in the relay, the incoming optical modes go through a BBS network of $M = 2^s$ inputs and outputs, with $M \geq N$. The BBS network is sketched in Figure 5.2 for $N = 4$ and described in detail in Appendix A of [CMG23]. The BBS network transforms the input modes, described by the

respective creation operators $\hat{a}_0^\dagger, \dots, \hat{a}_{M-1}^\dagger$ into the output modes $\hat{d}_0^\dagger, \dots, \hat{d}_{M-1}^\dagger$ according to

$$\hat{a}_i^\dagger \rightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} (-1)^{\vec{k} \cdot \vec{i}} \hat{d}_k^\dagger, \quad (5.32)$$

where \vec{i} and \vec{j} are the binary representation of the integers i and j , respectively. We note that, since in principle $N \leq M$, the M modes $\hat{a}_0, \dots, \hat{a}_{M-1}$ represent the N signals coming from the parties paired with additional $M - N$ modes in the vacuum state. The output modes are then measured with threshold detectors D_0, \dots, D_{M-1} , to certify the arrival of one (or more) photon detector. The relay finally announces the outcomes of the measurements of each detector D_j , by publicly disclosing the values $k_j = 1$ if the detector clicked or $k_j = 0$ if the detector did not click.

3. **Classical post-selection and parameter estimation:** the parties only keep rounds where they chose the same basis and where only one detector, e.g. detector D_j , clicked and discard the rest. We call this phase of the protocol *post-selection phase*. They then disclose, through an authenticated classical channel, part of the simulated measurements outcomes in the X-basis of the KG rounds to evaluate the *pair-wise QBER* $Q_{AB_i}^j$ defined, again, as

$$Q_{X_0, X_i}^j = \Pr \left(X_0 \neq (-1)^{\vec{i} \cdot \vec{j}} X_i \mid k_j = 1 \right), \quad (5.33)$$

Similarly, for PE rounds, they disclose the choices of amplitudes $(\beta_0, \dots, \beta_{N-1})$ and estimate the gains

$$G_{\beta_0, \dots, \beta_{N-1}}^j := \Pr(k_j = 1 \mid \beta_0, \dots, \beta_{N-1}), \quad (5.34)$$

that is, the probabilities that detector D_j clicks given the choice of intensities $(\beta_0, \dots, \beta_{N-1})$, where we recall $\beta_0, \dots, \beta_{N-1} \in \mathcal{S}$.

4. **Classical post-processing:** the parties use the same authenticated classical channel to perform the usual post-processing, in the form of error correction and privacy amplification.

In Figure 5.2 we show a sketch of the protocol, implemented for $N = 4$.

The protocol reduces to the TF-QKD protocol of section 5.2.1 for $N=2$. In particular, a novel multipartite decoy-state method is employed in PE rounds to estimate the phase-error rate. The key rate of the protocol reads

$$r_\infty \geq \sum_{j=1}^M p_j (1 - h(\bar{Q}_Z^j) - \max_i h(Q_{X_0, X_i}^j)), \quad (5.35)$$

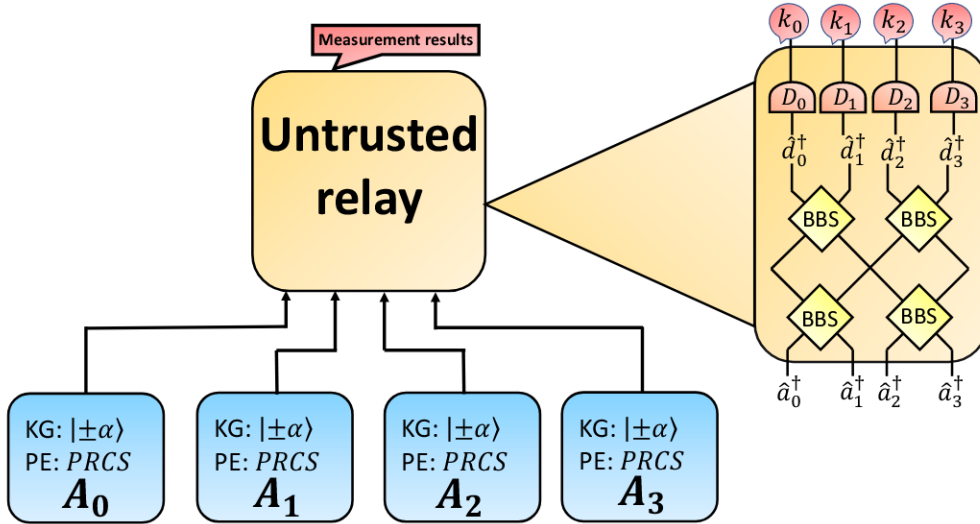


Fig. 5.2.: Schematic representation of the practical CKA protocol for $N = 4$. The MDI practical CKA protocol presented in this section takes inspiration from standard TF-QKD to allow a secure communication between many users. All desirable properties of TF-QKD are retained in the generalization, namely the practical implementation and, as we will see in the next section, the communication capabilities at high distance.

where Q_{X_0, X_i}^j is the pair-wise QBER estimated in KG rounds and \bar{Q}_Z^j is an upper bound on the phase-error rate of Eq. (5.16). To prove security, in fact, we derive the upper bound on the phase-error rate, given as

$$\bar{Q}_Z^j = \sum_{\substack{g(\vec{f})=3 \\ |\vec{f}| \text{ even}}}^{2^N-1} \left(\sum_{n_1, \dots, n_N=0}^{\infty} \prod_{i=1}^N c_{n_i}^{(f_i)} \sqrt{Y_{n_1, \dots, n_N}^j} \right)^2, \quad (5.36)$$

where p_j is the probability that detector D_j clicks and $c_{n_i}^{(f_i)} = \frac{\alpha^{2n_i+f_i}}{\sqrt{(2n_i+f_i)!}}$. Furthermore, we defined, as in section 5.2.1 the *multipartite yields* Y_{n_1, \dots, n_N}^j as the probabilities that detector D_j clicks given that the parties sent Fock states $|n_1\rangle, \dots, |n_N\rangle$ to the relay. To estimate the multipartite yields, and thus the upper bound on the phase-error rate, it is possible to write the gains of Eq. (5.34) as

$$G_{\beta_1, \dots, \beta_N}^j = \sum_{n_1, \dots, n_N=0}^{\infty} \prod_{i=1}^{N-1} e^{-|\beta_i|^2} \frac{\beta_i^{2n_i}}{n_i!} Y_{n_1, \dots, n_N}^j, \quad (5.37)$$

and use a (multipartite) decoy-state method to upper bound non-trivially a finite amount of yields as a function of the gains. This multipartite decoy-state method is a novel result of [CMG23], where it is used for the first time for an arbitrary number

of users. In the next, final, section, we examine in detail the performances of the protocol, compared to fundamental bounds on communication rate in networks.

5.2.4 Overcoming fundamental limitations in networks

Since the proposed multipartite scheme is, like TF-QKD, based on single-photon interference, the key rate is also expected to retain the $\sqrt{\eta}$ scaling, giving advantageous performances in the high-loss regime. Also, similarly to the bipartite case, we can compare the performances of the protocol with fundamental limitations on the communication rate in network scenarios, proposed in [Pir20] to generalize the results of section 5.1.3 to network scenarios. This fundamental limitation is called *single-message multicast bound* and it strongly depends on the architecture of the network. Therefore, when comparing the performances, we need to choose the architecture of the network arising from removing the relay in the practical MDI-CKA scheme.

We consider firstly the simplest scenario, where the network resulting from the removal of the relay is a star network, with the party A_0 connected with a pure photon-loss channel with transmittivity η with all the other parties. We remark that, as already discussed for the bipartite case, each party is connected to the relay with the same pure photon-loss channel with transmittance $\sqrt{\eta}$, hence the η transmittance of the channel connecting each party with any other. In this star network configuration, the single-message multicast bound reads

$$r_\infty \leq -\log_2(1 - \eta) := R_1. \quad (5.38)$$

We note that the expression of Eq. (5.38) coincides with the PLOB bound of Eq. (5.13) and does not depend on the number of parties. The other configuration considered is a fully connected network, where each party is connected with any other party with a pure photon-loss channel with transmittance η . The resulting single-message multicast bound is

$$r_\infty \leq -(N - 1) \log_2(1 - \eta) := R_2(N). \quad (5.39)$$

We note that with the second configuration the parties have more communication power, since they have more channels, and thus the single-message multicast bound is higher.

As we can see in Fig. 5.3, taken from [CMG23], the practical scheme presented in section 5.2.3 is capable of beating both multicast bounds of Eqs. (5.38) and 5.39 in the high-loss regime, making this protocol suitable for long-distance communication. We remark that in Figure 5.3 we performed the decoy-state analysis considering

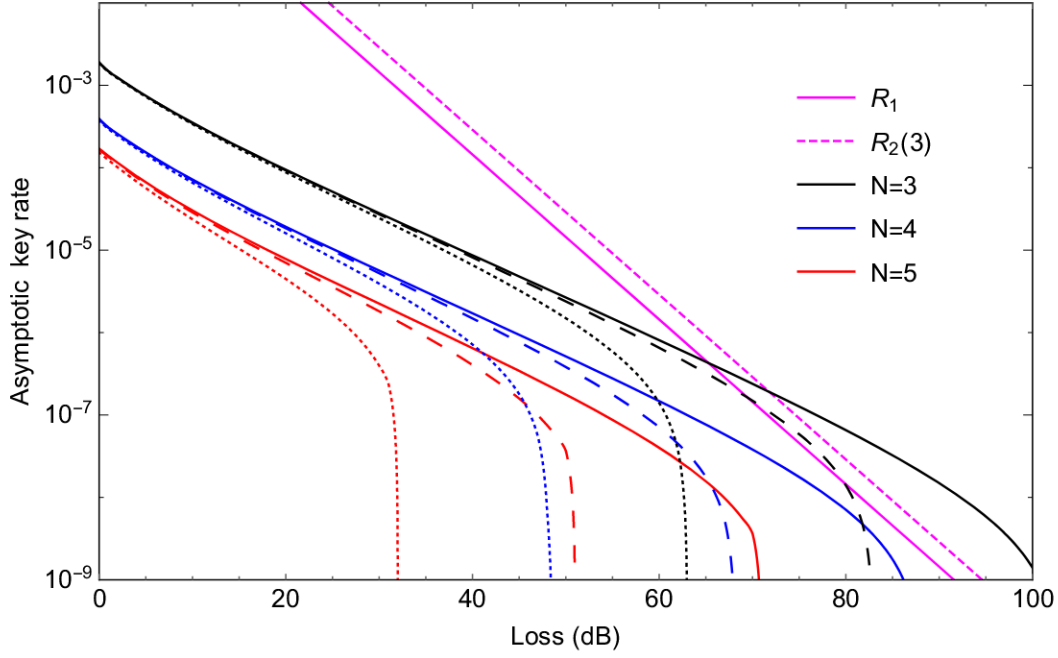


Fig. 5.3.: Asymptotic conference key rate of the practical CKA protocol as a function of the loss, compared with the single-message multicast bound. We plot the key rate for different dark count probabilities: $p_d = 10^{-10}$ (solid lines), $p_d = 10^{-9}$ (dashed lines) and $p_d = 10^{-8}$ (dotted lines) and different number of parties N , while we fix the polarization and phase misalignment to 2%. We employed the multipartite decoy-state method with two decoy settings $\beta_0 = 0$ and $\beta_1 = 0.5$. We report the single-message multicast bound R_1 (Eq. (5.38), solid magenta line) for the star network and the bound $R_2(3)$ (Eq. (5.39), dashed magenta line) for the fully connected network. For sufficiently high loss, our protocol with two decoys can overcome the multicast bounds for both configurations when $N = 3$.

only two decoy amplitudes, limiting the achievable key rate. In [CMG23] we also performed the analysis in the unrealistic scenario of infinite decoys, which we omit here, showing better overall performances and thus hinting at the possibility of improving the performance of the protocol by employing more decoy amplitudes.

It is worth noting that, since the protocol is based on W state-CKA, the key rate of the protocol unavoidably drops with the number of parties, due to the intrinsic QBER of such schemes, as shown in section 4.1.2. The protocol is therefore particularly efficient for low numbers of parties, being able, as shown, to beat the single-message multicast bound. A similar scheme based on GHZ-state correlations was recently proposed [Li+23] to improve the scaling with the number of parties. The protocol is suited for high-distance communication, being able to beat fundamental bounds on communication rate in network similar to the single-message multicast bound, but has substantial practical requirements, i.e., the parties need to send each round of the protocol a high number of single-photon states and the relay needs to perform a

quantum non-demolition measurement on all incoming signals, making the protocol much less appealing for near-term implementations than the one we proposed.

Nevertheless, the protocol presented in section 5.2.3 represents a substantial step for practical implementations of MDI-CKA protocols. In fact, besides having minimal requirements, only needing laser sources and passive optical devices to be implemented, it allows for long-distance communication, paving the way for the vision of a real quantum communication network.

Device-Independent randomness expansion

In chapter 5 we introduced a new quantum cryptographic paradigm, namely MDI-QKD, that allows to relax one of the fundamental assumptions for security, outlined in 3.2.1, that is the assumption of trusted devices. However, MDI-QKD schemes do not allow to fully relax the assumption, as the parties do not need to trust the measurement devices but still need to trust the state preparation. In this chapter we will introduce a simple task, called *Device-Independent randomness expansion (DIRE)* [Pir+10; CK11; PM13; FGS13; MS16; WBA18; VV12; CR12; Gal+13], where the assumption of trusted devices is fully lifted. In DIRE two or more parties try to obtain uniformly random outcomes from an untrusted device, with which they can interact only by giving it inputs and receiving outputs. The task is then for the parties to certify that the outputs of the device are truly random and unknown to possible eavsdroppers that may have tampered with the device.

As uniform randomness is one of the basic requirements for a cryptographic key, DIRE can be seen as a primitive to Device-Independent (DI) quantum cryptographic protocols where the assumption of trusted devices is fully lifted. Different DI cryptographic protocols, both bipartite [Ací+07; Pir+09; MPA11; VV14; Arn+18a] and multipartite [SG01a; SG01b; RMW19; HKB20a; Gra+21; Gra+23], with a few experimental implementations [Liu+22; Nad+22; Zha+22; Sha+21; Liu+21b], have been developed. In this thesis we will focus specifically on DIRE.

The chapter is structured as following: in the first section, namely section 6.1, we introduce the Device-Independent scenario for two parties and define Bell inequalities in section 6.1.1. Furthermore, in section 6.1.2 we generalize the concepts to adapt for multiple parties and introduce the multipartite Bell inequality of interest for the subsequent work. In section 6.2 we then introduce the task of DIRE and show, in section 6.2.1, interesting results about DIRE with partially entangled states.

6.1 Device-Independent scenario

Let us first introduce the so-called *Device-Independent scenario*, starting from the bipartite case. As already anticipated, the parties, in this case Alice and Bob, have some untrusted devices which give them outputs when they provide them with

inputs. These devices are represented as black boxes and they are fully characterized by the conditional probability distribution $p(a, b | x, y)$, where a and b are the possible outputs and x and y the possible outputs of Alice's and Bob's devices, respectively. The DI scenario is sketched in Figure 6.1 The crucial intuition behind any DI protocol

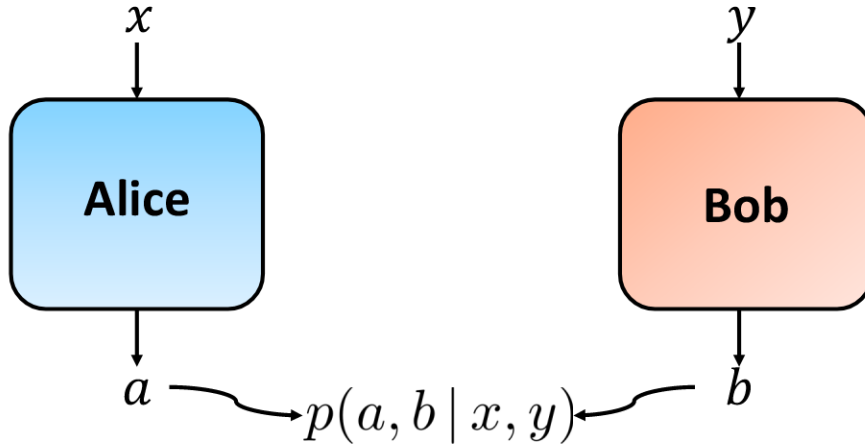


Fig. 6.1.: Sketch of the DI scenario. Two parties, Alice and Bob, possess two untrusted devices which return outputs a and b when given inputs x and y . The devices are characterized by the conditional probability distribution $p(a, b | x, y)$.

is the following, which was firstly formulated by Bell [Bel64]: the properties of the underlying system of the devices determine the properties of the probability distribution $p(a, b | x, y)$. In particular, if the device contains a classical system, the probability distribution $p(a, b | x, y)$ is in the form

$$p(a, b | x, y) = \int d\lambda p_\lambda p(a | x, \lambda) p(b | y, \lambda), \quad (6.1)$$

where λ is a hidden variable with probability distribution p_λ which is responsible for the observed correlations and $p(a | x, \lambda)$ and $p(b | y, \lambda)$ are local conditional probability distributions of Alice's and Bob's outcomes a and b , given the inputs x and y and the hidden variable λ , respectively. In other words, since classical systems are local, if the underlying system in the device is classical, the observed correlations must be explained with a shared hidden variable, namely λ in Eq. (6.1), which is responsible for the seemingly non-local behavior. We call the set of classical correlations the *local set* and indicate it by \mathcal{L} .

Quantum theory, on the other hand, is intrinsically non-local, giving rise to a larger set of possible correlations. In fact, if the underlying system is a quantum system, the probability distribution $p(a, b | x, y)$ can be written as

$$p(a, b | x, y) = \text{Tr} \left[\hat{M}_{a,x}^{(A)} \otimes \hat{M}_{b,y}^{(B)} \rho_{AB} \right], \quad (6.2)$$

where ρ_{AB} is a quantum state shared by Alice and Bob and $\{\hat{M}_{a,x}^{(A)}\}$ and $\{\hat{M}_{b,y}^{(B)}\}$ are the POVM elements of the measurement devices of Alice and Bob, respectively. We indicate the set of quantum correlations with \mathcal{Q} . Since the set of quantum and classical correlations are not the same, with $\mathcal{L} \subset \mathcal{Q}$, the main idea behind any DI protocol is to rule out the possibility of the device being classical by only looking at the correlations. The parties, once they certified that their devices are quantum devices, can then exploit the unique properties of quantum mechanics to, e.g., certify the randomness of the outcomes of the device or extract a secure secret key from them.

Before diving into the details on how to distinguish classical and quantum correlations, we introduce another set of correlations, motivated by physical reasons. We could indeed ask whether there exist other theories that describe the underlying system of our devices besides quantum and classical theory. If we do not assume any specific theory describing the device's systems, we could observe any normalized probability distribution $p(a, b|x, y)$. However, physically, the outcomes of each party must be independent from the choice of input of the other party. This requirement is necessary to avoid instantaneous communication between Alice and Bob, which would violate relativity. Mathematically, this requirement translates to the following set of constraints

$$\begin{aligned} \sum_a p(a, b|x, y) &= \sum_a p(a, b|x', y) \\ \sum_b p(a, b|x, y) &= \sum_b p(a, b|x, y'), \end{aligned} \quad (6.3)$$

for all a, b, x, x', y, y' . The probability distributions that satisfy these constraints are usually referred to as *non-signalling* distributions and the set of non-signalling distributions is indicated by \mathcal{NS} . We remark that quantum correlations are also non-signalling, as quantum theory does not violate relativity, and thus the non-signalling set strictly contains set of quantum correlations.

6.1.1 Bell inequalities

In this section we introduce the crucial tool used in DI scenarios to distinguish classical and quantum correlations: *Bell inequalities*. A Bell inequality is simply a linear constraint on the probability distribution $p(a, b|x, y)$ that is satisfied for all classical probability distributions, i.e., all distributions in the form of Eq. (6.1), and

violated by at least one quantum probability distribution. More specifically, a Bell inequality is an expression of the form

$$\sum_{a,b,x,y} G_{a,b,x,y} p(a,b|x,y) \leq \beta_L, \quad (6.4)$$

where $G_{a,b,x,y}$ are real coefficients and where the inequality is satisfied for all $p_L(a,b|x,y) \in \mathcal{L}$ and is violated by at least one $p_Q(a,b|x,y) \in \mathcal{Q}$. A Bell inequality can be seen as a hyperplane in the space of probability distributions that separates the classical set from the quantum set, similarly to what we showed for entanglement witnesses in sections 2.3.1 and 2.3.3. In Figure 6.2 we depict the structure of the set of correlations.

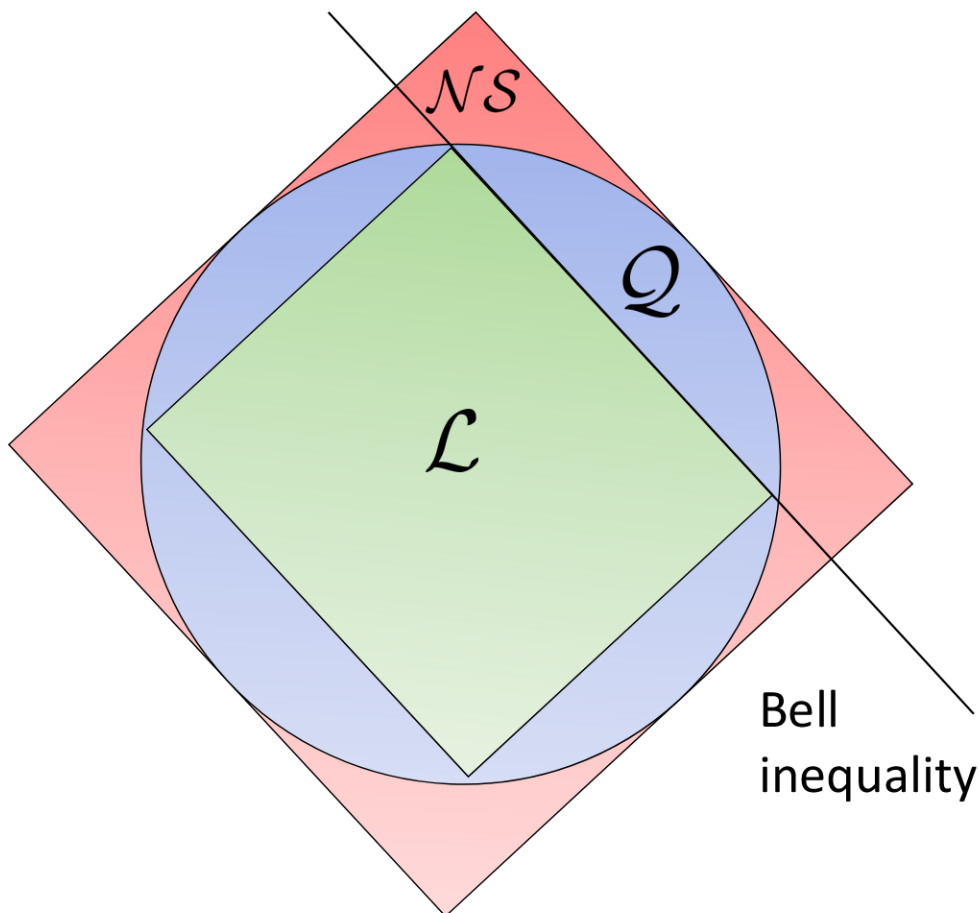


Fig. 6.2.: Depiction of the set of correlations. We indicate with \mathcal{L} , \mathcal{Q} and \mathcal{NS} the set of classical (or local), quantum and non-signalling correlations, respectively. A Bell inequality is a hyperplane that allows to separate classical correlations from at least one quantum probability distribution.

The most simple and famous Bell inequality is the *CHSH inequality* [Cla+69], named after the authors of the original work. We restrict to a scenario where the devices of Alice and Bob have two inputs, i.e., $x, y \in \{0, 1\}$ and two outputs, i.e., $a, b \in \{-1, +1\}$. In this scenario, we define the following *CHSH value*

$$S_{CHSH} := \langle a_0b_0 \rangle + \langle a_0b_1 \rangle + \langle a_1b_0 \rangle - \langle a_1b_1 \rangle, \quad (6.5)$$

where we define

$$\langle a_xb_y \rangle := \sum_{a,b=\pm 1} abp(a,b|x,y). \quad (6.6)$$

This Bell value defines a Bell inequality, as it is possible to show that for classical probability distributions $p_L(a,b|x,y) \in \mathcal{L}$ it holds

$$S_{CHSH} \leq 2, \quad (6.7)$$

whereas for quantum probability distributions it holds [Cir80]

$$S_{CHSH} \leq 2\sqrt{2}. \quad (6.8)$$

Therefore, if the parties observe a Bell value greater than 2, they can certify that their devices perform quantum measurements on a quantum system.

As already pointed out, if the devices contain quantum systems, the observed probability distribution takes the form of Eq. (6.2). Since we restrict to dichotomic measurements, i.e., since the parties have only two possible inputs and outputs, the quantum measurements are fully characterized by the *measurement observables* $\hat{A}_x := \hat{M}_{-1,x}^{(A)} - \hat{M}_{+1,x}^{(A)}$ and $\hat{B}_y := \hat{M}_{-1,y}^{(B)} - \hat{M}_{+1,y}^{(B)}$ for Alice and Bob, respectively. In this scenario, any Bell inequality can be recast, instead in terms of probabilities, in terms of the so-called *correlators*, defined as the expectation values of the measurement observables $\langle \hat{A}_x \rangle$, $\langle \hat{B}_y \rangle$ and $\langle \hat{A}_x \otimes \hat{B}_y \rangle$. In particular, we call $\langle \hat{A}_x \rangle$ and $\langle \hat{B}_y \rangle$ *1-body correlators* and $\langle \hat{A}_x \otimes \hat{B}_y \rangle$ *2-body correlators*. It is straightforward to write, from Eq. (6.2), the probabilities $p(a,b|x,y)$ (and thus any Bell inequality) as a function of the correlators. For example, the CHSH inequality, can be recast as

$$S_{CHSH} := \langle \hat{A}_0 \otimes \hat{B}_0 \rangle + \langle \hat{A}_0 \otimes \hat{B}_1 \rangle + \langle \hat{A}_1 \otimes \hat{B}_0 \rangle - \langle \hat{A}_1 \otimes \hat{B}_1 \rangle \leq 2. \quad (6.9)$$

One interesting property of the CHSH inequality is that the parties can obtain the maximal violation $S_{CHSH} = 2\sqrt{2}$ if and only if they share a maximally entangled Bell state $|\psi_+\rangle$ of Eq. (2.50), and their measurement observables are

$$\begin{aligned}\hat{A}_0 &= \hat{X}, \quad \hat{A}_1 = \hat{Z} \\ \hat{B}_0 &= \frac{\hat{X} + \hat{Z}}{2}, \quad \hat{B}_1 = \frac{\hat{X} - \hat{Z}}{2},\end{aligned}\tag{6.10}$$

where \hat{X} and \hat{Z} indicate the Pauli operators of Eq. (2.39). This result is particularly interesting as it allows the parties to completely characterize the devices if they observe a maximal violation.

6.1.2 Multipartite DI scenario

The DI scenario can be straightforwardly generalized for an arbitrary number of parties. Instead of Alice and Bob we consider N parties, labelled as A_1, \dots, A_N , holding black boxes with inputs x_1, \dots, x_N and outputs a_1, \dots, a_N . For our purposes we restrict to the two inputs/two outputs scenario, i.e., $x_i \in \{0, 1\} \forall i$ and $a_i \in \{-1, +1\} \forall i$. The devices are then characterized by the probability distribution $p(a_1, \dots, a_N | x_1, \dots, x_N)$. Once again, the classical (or local) probability distributions are the ones in the form

$$p(a_1, \dots, a_N | x_1, \dots, x_N) = \int d\lambda p(\lambda) p(a_1 | x_1, \lambda) \cdots p(a_N | x_N, \lambda),\tag{6.11}$$

whereas the quantum probability distributions are in the form

$$p(a_1, \dots, a_N | x_1, \dots, x_N) = \text{Tr} \left[\hat{M}_{x_1}^{a_1} \otimes \cdots \otimes \hat{M}_{x_N}^{a_N} \rho_{A_1, \dots, A_N} \right],\tag{6.12}$$

where $\hat{M}_{x_i}^{a_i}$ are the measurement operators of party A_i and ρ_{A_1, \dots, A_N} is a multipartite quantum state shared by all the parties. As shown for two parties, the measurements are uniquely characterized by the measurement observables $A_{x_i}^{(i)} = M_{x_i}^{-1} - M_{x_i}^{+1}$ for each party A_i .

In this scenario we can still define a Bell inequality as a linear combination

$$\sum_{a_1, \dots, a_N, x_1, \dots, x_N} G_{a_1, \dots, a_N, x_1, \dots, x_N} p(a_1 \dots a_N | x_1 \dots x_N) \leq \beta_L,\tag{6.13}$$

where, again, $G_{a_1, \dots, a_N, x_1, \dots, x_N}$ are real coefficients and where the inequality is satisfied for all classical probability distributions and violated by at least one quantum one. Once again, any Bell inequality can be also written in terms of the correlators, which in the multipartite case can be any k -body correlators for $k = 1, \dots, N$. Of par-

ticular interest for our work is the N -partite Bell inequality proposed in [Bac+20]. We start by defining the following Bell value

$$\begin{aligned}
S_\theta &= (N-1) \frac{\cos 2\theta}{\sqrt{1+\cos^2 2\theta}} \left(\langle A_0^{(1)} \rangle - \langle A_1^{(1)} \rangle \right) \\
&\quad + (N-1) \left(\langle A_0^{(1)} A_0^{(2)} \dots A_0^{(N)} \rangle + \langle A_1^{(1)} A_0^{(2)} \dots A_0^{(N)} \rangle \right) \\
&\quad + \frac{1}{\sqrt{1+\cos^2 2\theta}} \sum_{i=2}^N \left(\langle A_0^{(1)} A_1^{(i)} \rangle - \langle A_1^{(1)} A_1^{(i)} \rangle \right), \tag{6.14}
\end{aligned}$$

with $\theta \in [0, \frac{\pi}{4}]$. It is possible to show that this Bell value defines a Bell inequality, as we have

$$S_\theta \leq \beta_L(\theta), \tag{6.15}$$

where $\beta_L(\theta) := 2(N-1) \frac{1+\cos 2\theta}{\sqrt{1+\cos^2 2\theta}}$ for all classical probability distributions and

$$S_\theta \leq \beta_Q, \tag{6.16}$$

where $\beta_Q := 2\sqrt{2}(N-1)$ for quantum probability distributions. The most interesting property of this Bell inequality is that its maximal violation is attained when the parties share a *tilted GHZ-state* of the form

$$|\psi_\theta\rangle = \cos \theta |0\rangle^{\otimes N} + \sin \theta |1\rangle^{\otimes N}. \tag{6.17}$$

6.2 Device-Independent Randomness Expansion

As already anticipated, we focus now on *Device-Independent Randomness expansion (DIRE)* protocols, where some parties try to certify that the outcomes of their devices are uniformly random and unknown to possible eavsdroppers. In the most simple case one party, say Alice, uses her device n times and extracts a bit string K_A of length n using the outcomes of the device. The goal is to certify how many bits of the string K_A are uniformly random and unknown to a possible eavsdropper Eve that may have tampered with the device. At first sight the problem seems to be intractable, as we have to consider the whole bit string K_A . However, thanks to a powerful theoretical tool called *entropy accumulation theorem* [Arn+18b; DF19; DFR20], it is possible to reduce the problem to quantifying the randomness of the *single-round outcomes*. As already seen in section 3.1, to address this task we can use the conditional von Neumann entropy $H(A|E)$ where A indicates Alice's single-round outcome and E indicates Eve's quantum side-information. Here we also see how DIRE can be seen as a primitive for DIQKD: in the definition of the key rate of any QKD protocol, of

Eqs. (3.29) and (4.1), the same quantity appears to quantify the information leaked to Eve during the protocol. Therefore, in this scenario, we define the *DIRE rate* as

$$r^{(DIRE)} := H(A|E), \quad (6.18)$$

that is, the amount of random bits, unknown to Eve, that Alice is able to extract each round of the DIRE protocol.

The main idea behind any DI protocol, in particular DIRE, is the following: imagine Alice is able to certify, together with other parties, the violation of a given Bell inequality, by calculating a certain Bell value S . If we find a theoretical non-trivial lower bound on $H(A|E)$ as a function of the Bell value S , Alice is then able to certify $H(A|E)$ bits of randomness in the outcomes of her device each round of the protocol. For example, it is possible to show that the following lower bound holds

$$H(A|E) \geq 1 - h\left(\sqrt{\frac{S_{CHSH}^2}{4}} - 1\right), \quad (6.19)$$

where h is the binary entropy introduced in section 3.1 and S_{CHSH} is the CHSH value of Eq. (6.5). Using this bound, Alice is then able to successfully perform a DIRE protocol given the violation $S_{CHSH} \geq 2$ of the CHSH inequality.

This procedure can be straightforwardly generalized to the multipartite scenario. We consider N parties, labelled as A_1, \dots, A_N , k of which, labelled as A_1, \dots, A_k , want to extract random bits from their untrusted devices and make sure that the random bits are unknown to Eve. Similarly to the bipartite case, the amount of randomness that they can extract is given by the following DIRE rate

$$r_k^{(DIRE)} := H(A_1, \dots, A_k|E), \quad (6.20)$$

where $H(A_1, \dots, A_k|E)$ is the conditional von Neumann entropy of the joint outcomes of the k parties, conditioned on Eve's side information and where note that $r_k^{(DIRE)} \leq k$. Once again, the goal is, given that the parties are able to certify the violation of a certain multipartite Bell inequality by evaluating a Bell value S_N , to find a lower bound on $H(A_1, \dots, A_k|E)$ as a function of said Bell value S_N , thus lower bounding the DIRE rate. Examples of such entropic bounds can be found, e.g., in [Gra+21; Gra+23], where the authors find analytical lower bounds the von Neumann entropy of the outcomes of different combinations of parties as a function of the violation of some common multipartite Bell inequalities, such as the *Mermin-Ardehali-Belinskii-Klyshko (MABK)* inequality [Mer90; Ard92; BK93] or the *Holz* inequality [HKB20b].

However, finding such analytical bounds can be a challenging task. Therefore, to simplify the problem we can consider the conditional min-entropy, described in section 3.1.3. As already seen in Eq. (3.17), the conditional min-entropy lower bounds the conditional von Neumann entropy and therefore can be considered to lower bound the achievable DIRE rate. The main advantage of the conditional min-entropy is that, due to its operational interpretation related to the guessing probability, as in Eq. (3.20), it can be computed efficiently with Semidefinite Programming (SDP). On the other hand, the conditional min-entropy provides loose lower bounds, thus limiting the performances of the DIRE protocol. In the next section we will employ this method to evaluate a numerical lower bounds on the achievable DIRE rate as a function of the violation of the Bell inequality of Eq. (6.14).

6.2.1 DIRE with partially entangled states

As already anticipated, in this section we will introduce a DIRE protocol based on the certification of the violation of the Bell inequality of Eq. (6.14). The obtained results are interesting in the context of reducing the resource requirements in cryptographic protocols: the investigated Bell inequality, as already shown, is maximally violated by the state of Eq. (6.17), which is a partially entangled state. In a realistic implementation, such states could account for experimental imperfections when trying to generate a GHZ state or could even be easier to generate than a GHZ state. Let us then consider a two inputs/two outputs DI scenario with N parties, labelled as A_1, \dots, A_N , where the parties are able to certify the violation $S_\theta \geq \beta_L$ of the Bell inequality of Eq. (6.14). Our goal is, as shown, to find lower bounds on the conditional von Neumann entropy of the outcomes of subset of parties conditioned on Eve's side information.

We can numerically evaluate, using SDP relaxations of the problem [NPA08], the conditional min-entropy, which, as already discussed, lower bounds the conditional von Neumann entropy and thus the DIRE rate. We start with $N = 3$ and evaluate the conditional min-entropy of the joint outcomes of the second and third party $H_{min}(A_2, A_3|E)$. The results are shown in Figure 6.3. The numerical calculations show a very interesting behavior, which was already known for two parties: in the bipartite case, as seen in [12], for any value of $\theta \neq 0$ the parties are able to achieve a DIRE rate of 1 for the maximal violation of a similar (although not equivalent) Bell inequality. This implies that one party is able to extract 1 bit of uniform randomness

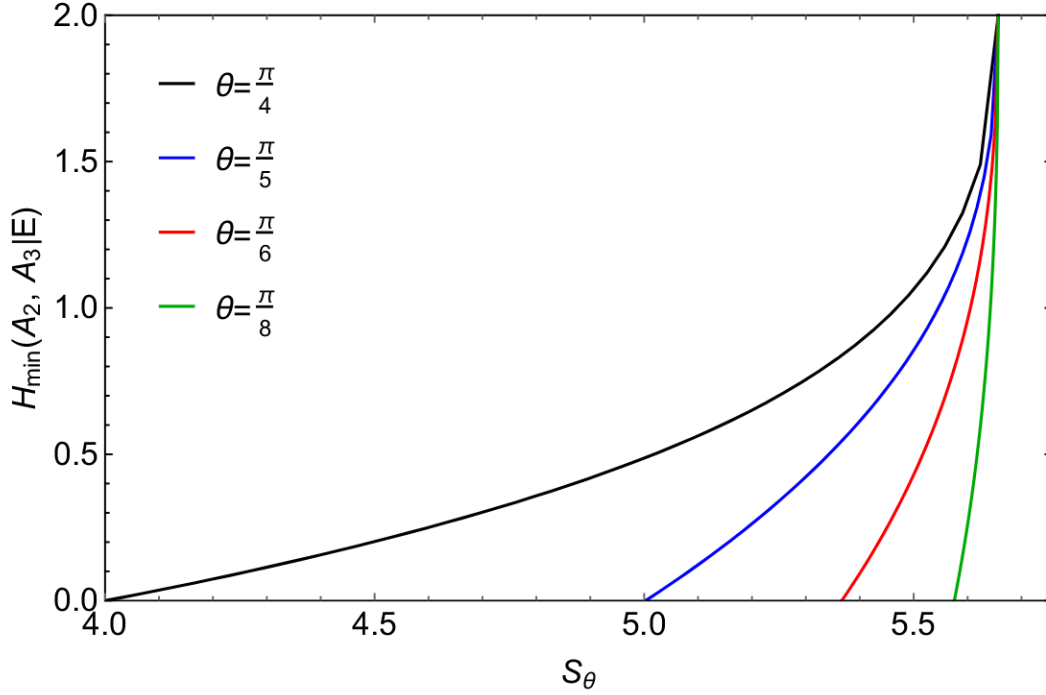


Fig. 6.3.: Plot of the conditional min-entropy of the joint outcomes of parties A_2 and A_3 as a function of the Bell violation S_θ , for $N = 3$ and different θ . The result shows that, for maximal violation of the Bell inequality, the parties are able to generate 2 bits of randomness in a DIRE protocol for any value of θ , even for θ close to 0 when the state certified in the devices, i.e., the state of Eq. (6.17), becomes almost separable.

each round of the protocol. This result is surprising, as for θ close to 0 the state maximally violating the Bell inequality, i.e., the *tilted Bell state*

$$|\psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \quad (6.21)$$

is almost separable, but the parties are still able to achieve a DIRE rate of 1. Our results show a similar behavior for $N = 3$, as the second and third party are able to achieve a DIRE rate of 2, thus certifying 2 bits of uniform randomness, when they certify the maximal violation of the Bell inequality of Eq. (6.14), for any value of $\theta \neq 0$. In other words the parties are able to achieve a DIRE rate of 2 when they certify that their devices contain partially entangled states of Eq. (6.17), even when these states are almost separable. We also numerically evaluated, for $N = 4$, the conditional min-entropy of the outcomes of parties A_2 , A_3 and A_4 , obtaining similar results. The results are shown in Figure 6.4. 6.3. The numerical evidence hints at the possibility that the N parties are able to obtain a DIRE rate of $N - 1$, thus certifying $N - 1$ bits of uniform randomness, for any value of $\theta \neq 0$, that is, even when the shared state is almost separable.

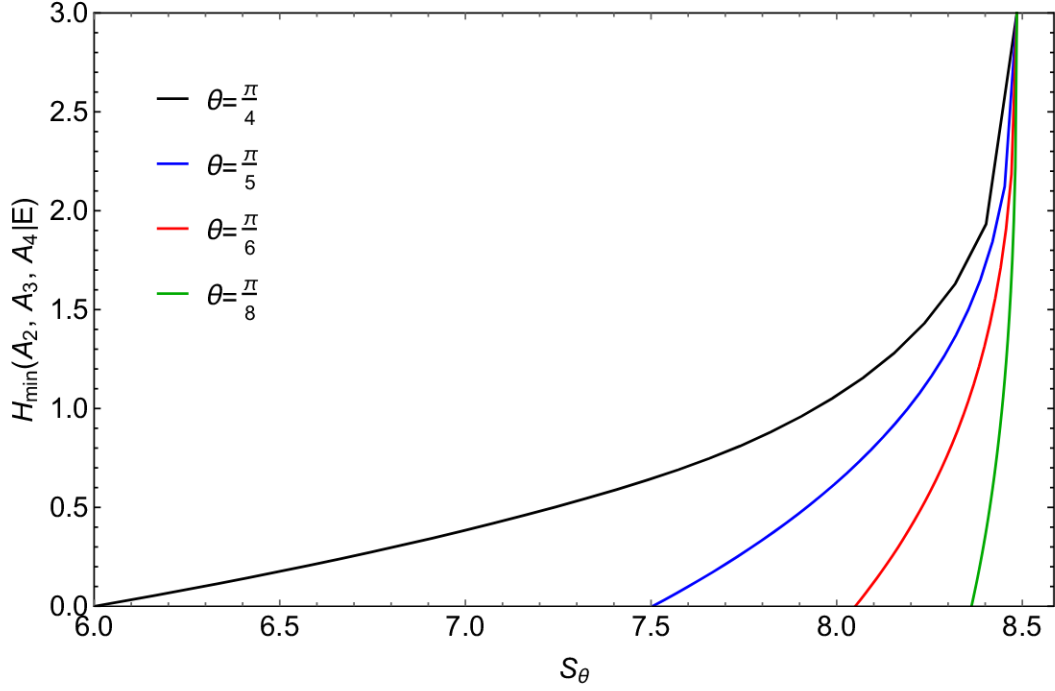


Fig. 6.4.: Plot of the conditional min-entropy of the joint outcomes of parties A_2 , A_3 and A_4 as a function of the Bell violation S_θ , for $N = 4$ and different θ . The result shows that, for maximal violation of the Bell inequality, the parties are able to generate 3 bits of randomness in a DIRE protocol for any value of θ , even for θ close to 0 when the state certified in the devices, i.e., the state of Eq. (6.17), becomes almost separable.

These numerical results open the way to investigate further DIRE, or even *DI Conference Key Agreement (DICKA)* protocols, using partially entangled states. Although the conditional min-entropy is a valid lower bound for the conditional von Neumann entropy, tighter bounds can be found by directly calculating analytically or numerically the conditional von Neumann entropy, as in [Gra+21; Gra+23], resulting in an improved DIRE rate of the protocol. Apart from the clear theoretical interest, such results could have an impact on practical implementations of said protocols, as partially entangled states, as the ones in Eq. (6.17), could naturally arise from imperfect state generation of GHZ states and could be used, as we have shown, for DI protocols.

Overview of the results

In this chapter we will give an overview of the results that led to the publications attached in appendices B and C.

Genuine multipartite entanglement is not a precondition for secure conference key agreement (Paper A)

In this first work [Car+21] we address one fundamental open question in the field of CKA protocols, that is, whether GME is necessary to successfully perform CKA. First, we utilize the properties of the von Neumann entropy to exclude some classes of states, which we prove are not usable for CKA. In particular, we show that all states that are separable with respect to a fixed partition will always lead to zero key rate in any CKA protocol, as, intuitively, all parties must share entanglement for the CKA protocol to succeed.

The obtained result allows us to restrict our analysis to the states that are not separable with respect to any partition but are still biseparable, as possible candidates for non-GME states that lead to a non-zero key rate in a CKA protocol. With this intuition, we define a class of N -partite mixed states, given in Eq. (4.12), where, in each term of the mixture, k parties share a GHZ state and the others a fully separable state. We show that by employing this states in the well-known N-BB84 protocol [GKB18], we can obtain a non-zero key rate for all values of N and k , thus answering the original question in the affirmative.

Furthermore, we analyze the performances of this class of states in the presence of local depolarizing noise and compare the results with another possible strategy to allow N parties to share a secret key, that is by performing a concatenation of bipartite BB84 protocols and classically post-process all the different keys into one shared key. The results show that the N-BB84 protocol with our class of states is able to outperform a concatenation of bipartite protocols for high k . Furthermore, we perform a detailed noise analysis and show that the advantage over concatenations of bipartite BB84 protocols is retained in the low noise regime.

As a final result, we explored a connection between key rate and entanglement witnesses, already outlined in [CLL04] for the bipartite scenario and here extended and improved for the multipartite one. The intuition is that a non-zero key rate can be seen as an entanglement witness, as entanglement across all partitions of the

parties is necessary for CKA, as shown in the beginning of our work. Moreover, since the set of states that can lead to a non-zero key rate is not convex, the key rate can be seen as a non-linear entanglement witness, surpassing the capabilities of usual, linear ones.

Overcoming Fundamental Bounds on Quantum Conference Key Agreement (Paper B)

Inspired by TF-QKD and by previous attempts of generalizing it to many parties [GKB19], in [CMG23] we design a simple and practical MDI-CKA protocol based on W state post-selection. First, we show the protocol, which consists in the following: N parties send weak coherent pulses for KG rounds and phase-randomized coherent states for PE rounds to a central relay, which is assumed to be controlled by Eve. In a honest implementation, the relay mixes all the modes with a network of BBS and measures the presence of a photon in each output of the network, publicly announcing the results. The parties are then able to post-select W state-like correlations by only keeping the rounds where one detector clicked.

We prove the security of the protocol by exploiting entropic uncertainty relations to bound the key rate as a function of two quantities: the QBER, estimated by the parties in KG rounds and the phase-error rate, which is the error in the conjugate basis of the KG rounds. Since the latter cannot be estimated by the parties in the protocol, we employ a novel multipartite decoy-state method to allow the parties to estimate the phase-error rate from the quantities they have available in the protocol in the PE rounds.

Furthermore, we perform extensive numerical simulations to assess the performances of the protocol in a realistic implementation. We choose a particular noise model where each party is connected to the relay with a lossy quantum channel with transmittance $\sqrt{\eta}$. We also consider other common sources of noise in the model, including polarization and phase misalignment and dark counts in the detectors. We are able to numerically evaluate the key rate and optimize it over the intensity α of the coherent pulses prepared by the parties, for $N = 3, 4, 5$.

Moreover, since one of the most striking features of bipartite TF-QKD is its high noise tolerance, represented by the possibility of beating the fundamental bound on the repeaterless transmission rate known as the PLOB bound [Pir+17], we compare the performances of the protocol with a similar bound for network scenarios, called the single-message multicast bound [Pir20]. We show that our protocol is also able to beat the single-message multicast bound in the high noise regime, at least for $N = 3$ and $N = 4$, showing its merits for practical, long-distance quantum communication.

Conclusions and Outlook

In conclusion we explored in detail one of the most promising application of quantum information processes, that is quantum cryptography. After introducing the basics of quantum mechanics and all the necessary tools to describe quantum systems, we presented the basic ideas behind bipartite QKD protocols and presented the first and most simple protocol, the BB84 protocol. We then moved from the bipartite scenario to the more complicated multipartite setting, describing the task of CKA, that is the generalization to many parties of the well-known and understood QKD.

In view of building a world-wide quantum network, the necessity of designing efficient and practical multipartite protocols is clear. Therefore, we analyzed our first original work, where we investigated the resources necessary to successfully perform CKA when using multipartite quantum resources. We investigated, in particular, the multipartite entanglement properties of the quantum state shared each round in a CKA protocol, showing that the strongest form of entanglement, namely GME, is not necessary to successfully perform common CKA protocols. We also drew an interesting connection between the conference key rate of a CKA protocol and the theory of entanglement witnesses and further introduced one particular network scenario, i.e., the triangle network scenario, where we laid the foundation to investigate further possible cryptographic applications in such network. As GME states can be in practice challenging to produce, our work paves the way to reduce the the practical requirements of realistic CKA protocols.

Afterwards we focused on a specific class of protocols, specifically MDI protocols. These protocols, designed to overcome the need for the parties to trust their measurement devices, are well suited for practical, near-term applications as they can be implemented with laser pulses and passive optical devices. In the bipartite scenario many such protocols have been designed, the most important being TF-QKD, and experimentally implemented. Therefore, we designed a similar protocol, scalable for an arbitrary number of users, which retains the same properties of the bipartite TF-QKD protocols, i.e., that is suitable for high-distance communication, being based on single-photon interference, and practically implementable with laser sources and passive optical devices.

Finally, we presented the most adversarial DI multipartite scenario, where the parties are not able to trust any of their devices. In this scenario we introduce a specific task, called DIRE, where the parties try to verify the violation of a Bell

inequality to certify uniform randomness in their outcomes. This task is particularly relevant as it can be considered a primitive task to DI quantum cryptography. We specifically looked at the case of a Bell inequality violated by partially entangled states and showed numerical evidence that the parties are able to extract many bits of uniform randomness by certifying almost separable multipartite states in their devices.

Whereas bipartite QKD protocols have been studied for almost five decades, multipartite protocols have attracted interest only recently, as the technological progress makes the vision of a world-wide quantum communication network possible. The field is thus open, with many lines of research that can be taken starting from our work. Firstly, different questions are still open on the side of the entanglement properties of the resource states used for CKA. For example, it would be desirable to obtain bounds on the achievable key rate for non-GME states based on the entanglement class they belong to. Moreover, it would be interesting to investigate real experimental scenarios where non-GME states could be less demanding to produce than GME states. On the side of MDI-CKA protocols, it would be interesting to extend the designed protocol to accommodate for real-life scenarios, where finite-key effects or asymmetries in the channels are considered. Finally, in the DI scenario, the goal of further work is to improve the performance of the DIRE protocol, by finding better lower bounds on the DIRE rate, using both numerical and analytical methods, and even designing DI cryptographic protocols that utilize partially entangled states. Nevertheless, all works presented in this thesis represent fundamental building blocks for future quantum cryptographic applications in network scenarios.

Bibliography

- [Ací+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, et al. “Device-Independent Security of Quantum Cryptography against Collective Attacks”. In: *Phys. Rev. Lett.* 98 (23 June 2007), p. 230501 (cit. on p. 75).
- [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 p. 82).
- [Arn+18a] 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 (Jan. 2018), p. 459 (cit. on p. 75).
- [Arn+18b] 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 (Jan. 2018), p. 459 (cit. on p. 81).
- [Bac+20] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín. “Scalable Bell Inequalities for Qubit Graph States and Robust Self-Testing”. In: *Phys. Rev. Lett.* 124 (2 Jan. 2020), p. 020402 (cit. on p. 81).
- [Bai+22] Jun-Lin Bai, Yuan-Mei Xie, Zhao Li, Hua-Lei Yin, and Zeng-Bing Chen. “Post-matching quantum conference key agreement”. In: *Opt. Express* 30.16 (Aug. 2022), pp. 28865–28881 (cit. on p. 63).
- [BR97] Stephen M. Barnett and Paul M. Radmore. *Methods in Theoretical Quantum Optics*. Oxford University Press, 1997 (cit. on p. 54).
- [Bea14] Normand J. Beaudry. *Assumptions in quantum cryptography*. PhD thesis, ETH Zurich, 2014 (cit. on p. 32).
- [BK93] A. V. Belinskii and D. N. Klyshko. “Interference of light and Bell’s theorem”. In: *Physics-Uspekhi* 36.8 (Aug. 1993), p. 653 (cit. on p. 82).
- [Bel64] J. S. Bell. “On the Einstein Podolsky Rosen paradox”. In: *Physics Physique Fizika* 1 (3 Nov. 1964), pp. 195–200 (cit. on p. 76).
- [Ben92] Charles H. Bennett. “Quantum cryptography using any two nonorthogonal states”. In: *Phys. Rev. Lett.* 68 (21 May 1992), pp. 3121–3124 (cit. on p. 21).
- [BB84] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 145–149 (cit. on pp. 2, 21, 34).

- [Ber+10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. “The uncertainty principle in the presence of quantum memory”. In: *Nature Physics* 6.9 (Sept. 2010), pp. 659–662 (cit. on p. 27).
- [Bih+06] Eli Biham, Michel Boyer, P. Oscar Boykin, Tali Mor, and Vwani Roychowdhury. “A Proof of the Security of Quantum Key Distribution”. In: *Journal of Cryptology* 19.4 (Oct. 2006), pp. 381–439 (cit. on pp. 21, 35).
- [Bru98] Dagmar Bruß. “Optimal Eavesdropping in Quantum Cryptography with Six States”. In: *Phys. Rev. Lett.* 81 (14 Oct. 1998), pp. 3018–3021 (cit. on p. 21).
- [Cao+21a] Xiao-Yu Cao, Jie Gu, Yu-Shuo Lu, Hua-Lei Yin, and Zeng-Bing Chen. “Coherent one-way quantum conference key agreement based on twin field”. In: *New Journal of Physics* 23.4 (Apr. 2021), p. 043002 (cit. on p. 63).
- [Cao+21b] Xiao-Yu Cao, Yu-Shuo Lu, Zhao Li, et al. “High Key Rate Quantum Conference Key Agreement With Unconditional Security”. In: *IEEE Access* 9 (2021), pp. 128870–128876 (cit. on p. 63).
- [Car+21] Giacomo Carrara, Hermann Kampermann, Dagmar Bruß, and Gláucia Murta. “Genuine multipartite entanglement is not a precondition for secure conference key agreement”. In: *Phys. Rev. Res.* 3 (1 Mar. 2021), p. 013264 (cit. on pp. 14, 39, 45–49, 87, 105).
- [CMG23] Giacomo Carrara, Gláucia Murta, and Federico Grasselli. “Overcoming Fundamental Bounds on Quantum Conference Key Agreement”. In: *Phys. Rev. Appl.* 19 (6 June 2023), p. 064017 (cit. on pp. 60, 63, 68, 70–72, 88, 115).
- [Che+22] Jiu-Peng Chen, Chi Zhang, Yang Liu, et al. “Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing”. In: *Phys. Rev. Lett.* 128 (18 May 2022), p. 180502 (cit. on p. 63).
- [Che+20] Jiu-Peng Chen, Chi Zhang, Yang Liu, et al. “Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km”. In: *Phys. Rev. Lett.* 124 (7 Feb. 2020), p. 070501 (cit. on p. 63).
- [Che+21] Jiu-Peng Chen, Chi Zhang, Yang Liu, et al. “Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas”. In: *Nature Photonics* 15.8 (Aug. 2021), pp. 570–575 (cit. on p. 63).
- [CL07] Kai Chen and Hoi-Kwong Lo. “Multi-partite quantum cryptographic protocols with noisy GHZ States”. In: *Quantum Inf. Comput.* 7.8 (2007), pp. 689–715 (cit. on p. 39).
- [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. 34).
- [Cir80] B. S. Cirel’son. “Quantum generalizations of Bell’s inequality”. In: *Letters in Mathematical Physics* 4.2 (Mar. 1980), pp. 93–100 (cit. on p. 79).
- [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 p. 79).

- [Cli+22] Cecilia Clivati, Alice Meda, Simone Donadello, et al. “Coherent phase transfer for real-world twin-field quantum key distribution”. In: *Nature Communications* 13.1 (Jan. 2022), p. 157 (cit. on p. 63).
- [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. 75).
- [CR12] Roger Colbeck and Renato Renner. “Free randomness can be amplified”. In: *Nature Physics* 8.6 (June 2012), pp. 450–453 (cit. on p. 75).
- [CT05] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, 2005 (cit. on p. 22).
- [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 p. 63).
- [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 (July 2019), p. 64 (cit. on pp. 56, 59, 63, 67, 68).
- [CLL04] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. “Entanglement as a Precondition for Secure Quantum Key Distribution”. In: *Phys. Rev. Lett.* 92 (21 May 2004), p. 217903 (cit. on pp. 45, 48, 87).
- [Das+21] Siddhartha Das, Stefan Bäuml, Marek Winczewski, and Karol Horodecki. “Universal Limitations on Quantum Key Distribution over a Network”. In: *Phys. Rev. X* 11 (4 Oct. 2021), p. 041016 (cit. on pp. 48, 51).
- [DW05] Igor Devetak and Andreas Winter. “Distillation of secret key and entanglement from quantum states”. In: *Proc. R. Soc. A.* 461 (2005) (cit. on pp. 31, 34).
- [DF19] Frédéric Dupuis and Omar Fawzi. “Entropy Accumulation With Improved Second-Order Term”. In: *IEEE Transactions on Information Theory* 65.11 (2019), pp. 7596–7612 (cit. on p. 81).
- [DFR20] Frédéric Dupuis, Omar Fawzi, and Renato Renner. “Entropy Accumulation”. In: *Communications in Mathematical Physics* 379.3 (Nov. 2020), pp. 867–913 (cit. on p. 81).
- [Eke91] Artur K. Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Phys. Rev. Lett.* 67 (6 Aug. 1991), pp. 661–663 (cit. on p. 21).
- [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. 39, 41).
- [Fan+20] Xiao-Tian Fang, Pei Zeng, Hui Liu, et al. “Implementation of quantum key distribution surpassing the linear rate-transmittance bound”. In: *Nature Photonics* 14.7 (July 2020), pp. 422–425 (cit. on p. 63).

- [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. 75).
- [Gal+13] Rodrigo Gallego, Lluís Masanes, Gonzalo De La Torre, et al. “Full randomness from arbitrarily deterministic events”. In: *Nature Communications* 4.1 (Oct. 2013), p. 2654 (cit. on p. 75).
- [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 (June 2011), p. 349 (cit. on p. 53).
- [Gra21] Federico Grasselli. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Springer International Publishing, 2021 (cit. on p. 21).
- [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 p. 67).
- [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. 39, 43, 60, 88, 115).
- [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. 39, 41, 87).
- [Gra+22] Federico Grasselli, Gláucia Murta, Jarn de Jong, et al. “Secure Anonymous Conferencing in Quantum Networks”. In: *PRX Quantum* 3 (4 Oct. 2022), p. 040306 (cit. on p. 39).
- [Gra+23] Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß. “Boosting device-independent cryptography with tripartite nonlocality”. In: *Quantum* 7 (Apr. 2023), p. 980 (cit. on pp. 75, 82, 85).
- [Gra+21] Federico Grasselli, Gláucia Murta, Hermann Kampermann, and Dagmar Bruß. “Entropy Bounds for Multiparty Device-Independent Cryptography”. In: *PRX Quantum* 2 (1 Jan. 2021), p. 010308 (cit. on pp. 75, 82, 85).
- [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 p. 67).
- [GHZ07] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. *Going Beyond Bell’s Theorem*. 2007. arXiv: 0712.0921 [quant-ph] (cit. on p. 14).
- [GT09] Otfried Gühne and Géza Tóth. “Entanglement detection”. In: *Physics Reports* 474.1 (2009), pp. 1–75 (cit. on pp. 10, 11).
- [HJP20] Frederik Hahn, Jarn de Jong, and Anna Pappa. “Anonymous Quantum Conference Key Agreement”. In: *PRX Quantum* 1 (2 Dec. 2020), p. 020325 (cit. on p. 39).

- [Han+22] Kiara Hansenne, Zhen-Peng Xu, Tristan Kraft, and Otfried Gühne. “Symmetries in quantum networks lead to no-go theorems for entanglement distribution and to verification techniques”. In: *Nature Communications* 13.1 (2022), p. 496 (cit. on pp. 49, 51).
- [HKB20a] Timo Holz, Hermann Kampermann, and Dagmar Bruß. “Genuine multipartite Bell inequality for device-independent conference key agreement”. In: *Phys. Rev. Res.* 2 (2 May 2020), p. 023251 (cit. on p. 75).
- [HKB20b] Timo Holz, Hermann Kampermann, and Dagmar Bruß. “Genuine multipartite Bell inequality for device-independent conference key agreement”. In: *Phys. Rev. Res.* 2 (2 May 2020), p. 023251 (cit. on p. 82).
- [Hor+09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. “Quantum entanglement”. In: *Rev. Mod. Phys.* 81 (2 2009), pp. 865–942 (cit. on p. 10).
- [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. 67).
- [KRS09] Robert König, Renato Renner, and Christian Schaffner. “The Operational Meaning of Min- and Max-Entropy”. In: *IEEE Transactions on Information Theory* 55.9 (2009), pp. 4337–4347 (cit. on p. 25).
- [Leo10] Ulf Leonhardt. *Essential Quantum Optics*. Cambridge, 2010 (cit. on p. 54).
- [Li+23] Chen-Long Li, Yao Fu, Wen-Bo Liu, et al. “Breaking universal limitations on quantum conference key agreement without quantum memory”. In: *Communications Physics* 6.1 (May 2023), p. 122 (cit. on p. 72).
- [Liu+21a] Hui Liu, Cong Jiang, Hao-Tao Zhu, et al. “Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km”. In: *Phys. Rev. Lett.* 126 (25 June 2021), p. 250502 (cit. on p. 63).
- [Liu+21b] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, et al. “Device-independent randomness expansion against quantum side information”. In: *Nature Physics* 17.4 (Apr. 2021), pp. 448–451 (cit. on p. 75).
- [Liu+22] Wen-Zhao Liu, Yu-Zhe Zhang, Yi-Zheng Zhen, et al. “Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution”. In: *Phys. Rev. Lett.* 129 (5 July 2022), p. 050502 (cit. on p. 75).
- [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 p. 63).
- [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 p. 67).
- [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 (May 2018), pp. 400–403 (cit. on pp. 63, 64).

- [Lyd+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, et al. “Hacking commercial quantum cryptography systems by tailored bright illumination”. In: *Nature Photonics* 4.10 (Oct. 2010), pp. 686–689 (cit. on p. 53).
- [MS83] Florence J. MacWilliams and Neil J. A. Sloane. *Theory of Error-Correcting Codes*. North-Holland publishing, 1983 (cit. on p. 29).
- [MPA11] Lluís Masanes, Stefano Pironio, and Antonio Acín. “Secure device-independent quantum key distribution with causally independent measurement devices”. In: *Nature Communications* 2.1 (Mar. 2011), p. 238 (cit. on p. 75).
- [May01] D. Mayers. “Unconditional security in quantum cryptography”. In: *J. ACM* 48.3 (2001) (cit. on pp. 21, 35).
- [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 p. 82).
- [MS16] Carl A. Miller and Yaoyun Shi. “Robust Protocols for Securely Expanding Randomness and Distributing Keys Using Untrusted Quantum Devices”. In: *J. ACM* 63.4 (Oct. 2016) (cit. on p. 75).
- [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 (May 2019), pp. 334–338 (cit. on p. 63).
- [Mur+20] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. “Quantum Conference Key Agreement: A Review”. In: *Advanced Quantum Technologies* 3.11 (2020), p. 2000025. eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202000025> (cit. on p. 45).
- [Nad+22] D. P. Nadlinger, P. Drmota, B. C. Nichol, et al. “Experimental quantum key distribution certified by Bell’s theorem”. In: *Nature* 607.7920 (July 2022), pp. 682–686 (cit. on p. 75).
- [Nav+20] Miguel Navascués, Elie Wolfe, Denis Rosset, and Alejandro Pozas-Kerstjens. “Genuine network multipartite entanglement”. In: *Physical Review Letters* 125.24 (2020), p. 240505 (cit. on pp. 49, 51).
- [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 p. 83).
- [NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000 (cit. on pp. 3, 17).
- [Ott+19] Carlo Ottaviani, Cosmo Lupo, Riccardo Laurenza, and Stefano Pirandola. “Modular network for high-rate quantum conferencing”. In: *Communications Physics* 2.1 (Sept. 2019), p. 118 (cit. on p. 39).
- [PV22] Carlos Palazuelos and Julio I. de Vicente. “Genuine multipartite entanglement of quantum states in the multiple-copy scenario”. In: *Quantum* 6 (June 2022), p. 735 (cit. on p. 48).

- [Pic+22] Alexander Pickston, Joseph Ho, Andrés Ulibarrena, et al. *Experimental network advantage for quantum conference key agreement*. 2022 (cit. on p. 39).
- [Pir+20] S. Pirandola, U. L. Andersen, L. Banchi, et al. “Advances in quantum cryptography”. In: *Adv. Opt. Photon.* 12.4 (Dec. 2020), pp. 1012–1236 (cit. on p. 21).
- [Pir20] Stefano Pirandola. “General upper bound for conferencing keys in arbitrary quantum networks”. In: *IET Quantum Communication* 1.1 (2020), pp. 22–25 (cit. on pp. 71, 88).
- [Pir+17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. “Fundamental limits of repeaterless quantum communications”. In: *Nature Communications* 8.1 (Apr. 2017), p. 15043 (cit. on pp. 59, 88).
- [Pir+10] S. Pironio, A. Acín, S. Massar, et al. “Random numbers certified by Bell’s theorem”. In: *Nature* 464.7291 (Apr. 2010), pp. 1021–1024 (cit. on p. 75).
- [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 p. 75).
- [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. 75).
- [Pit+21] Mirko Pittaluga, Mariella Minder, Marco Lucamarini, et al. “600-km repeater-like quantum communications with dual-band stabilization”. In: *Nature Photonics* 15.7 (July 2021), pp. 530–535 (cit. on p. 63).
- [PR22] Christopher Portmann and Renato Renner. “Security in quantum cryptography”. In: *Rev. Mod. Phys.* 94 (2 June 2022), p. 025008 (cit. on p. 31).
- [12] “Randomness versus Nonlocality and Entanglement”. In: *Phys. Rev. Lett.* 108 (10 Mar. 2012), p. 100402 (cit. on p. 83).
- [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 p. 75).
- [Rüc+22] Lukas Rüdckle, Jakob Budde, Jarn de Jong, et al. *Experimental anonymous conference key agreement using linear cluster states*. arXiv:quant-ph/2207.09487. 2022 (cit. on p. 39).
- [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 p. 31).
- [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. 75).
- [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. 75).

- [SK14] Valerio Scarani and Christian Kurtsiefer. “The black paper of quantum cryptography: Real implementation problems”. In: *Theoretical Computer Science* 560 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, pp. 27–32 (cit. on p. 32).
- [SR08] 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 pp. 31, 34).
- [Sha+21] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, et al. “Device-independent randomness expansion with entangled photons”. In: *Nature Physics* 17.4 (Apr. 2021), pp. 452–456 (cit. on p. 75).
- [Sha48] Claude E. Shannon. “A mathematical theory of communication”. In: *The Bell System Technical Journal* 27.3 (1948), pp. 379–423 (cit. on pp. 1, 22).
- [Sho94] Peter W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134 (cit. on p. 1).
- [SP00] Peter W. Shor and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. In: *Phys. Rev. Lett.* 85 (2 July 2000), pp. 441–444 (cit. on pp. 21, 35).
- [TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. “Fundamental rate-loss tradeoff for optical quantum key distribution”. In: *Nature Communications* 5.1 (Oct. 2014), p. 5235 (cit. on p. 59).
- [Tom16] Marco Tomamichel. *Quantum Information Processing with Finite Resources*. Springer, Cham, 2016 (cit. on pp. 21, 23, 36).
- [TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner. “A Fully Quantum Asymptotic Equipartition Property”. In: *IEEE Transactions on Information Theory* 55.12 (2009), pp. 5840–5847 (cit. on p. 26).
- [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 (Jan. 2012), p. 634 (cit. on p. 37).
- [VV12] Umesh Vazirani and Thomas Vidick. “Certifiable Quantum Dice: Or, True Random Number Generation Secure against Quantum Adversaries”. In: *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*. STOC ’12. New York, New York, USA: Association for Computing Machinery, 2012, pp. 61–76 (cit. on p. 75).
- [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. 75).
- [Ver26] Gilbert S. Vernam. “Cipher printing telegraph systems: For secret wire and radio telegraphic communications”. In: *Journal of the A.I.E.E.* 45.2 (1926), pp. 109–115 (cit. on p. 1).

- [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 p. 63).
- [Wan+22] Shuang Wang, Zhen-Qiang Yin, De-Yong He, et al. “Twin-field quantum key distribution over 830-km fibre”. In: *Nature Photonics* 16.2 (Feb. 2022), pp. 154–161 (cit. on p. 63).
- [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 p. 67).
- [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. 63).
- [WXG22] Yi-Xuan Wang, Zhen-Peng Xu, and Otfried Gühne. “Quantum networks cannot generate graph states with high fidelity”. In: *arXiv preprint arXiv:2208.12100* (2022) (cit. on pp. 49, 51).
- [Wil17] Mark M. Wilde. *Quantum Information Theory*. 2nd ed. Cambridge University Press, 2017 (cit. on p. 3).
- [Wol21] Ramona Wolf. *Quantum Key Distribution: an Introduction with Exercises*. Springer, 2021 (cit. on pp. 21, 29).
- [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 p. 75).
- [Yam+22] Hayata Yamasaki, Simon Morelli, Markus Miethlinger, et al. “Activation of genuine multipartite entanglement: Beyond the single-copy paradigm of entanglement characterisation”. In: *Quantum* 6 (Apr. 2022), p. 695 (cit. on p. 48).
- [Zha+22] Wei Zhang, Tim van Leent, Kai Redeker, et al. “A device-independent quantum key distribution system for distant users”. In: *Nature* 607.7920 (July 2022), pp. 687–691 (cit. on p. 75).
- [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. 39).
- [Zha+20] Shuai Zhao, Pei Zeng, Wen-Fei Cao, et al. “Phase-Matching Quantum Cryptographic Conferencing”. In: *Phys. Rev. Appl.* 14 (2 Aug. 2020), p. 024010 (cit. on p. 39).
- [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. 53).

Proofs

In this appendix we present some proofs that are too technical and articulated to be shown in the main text.

Proof of Theorem 5

In this section we show the proof of Theorem 5. The proof consist mainly in providing an explicit construction for ρ_{bs} . First, we define the following biseparable state

$$\rho_{bs} = \frac{1}{3}\tilde{\rho}_{AB} \otimes |00\rangle_{CC'}\langle 00| + \frac{1}{3}\tilde{\sigma}_{AC} \otimes |01\rangle_{BB'}\langle 01| + \frac{1}{3}\tilde{\tau}_{BC} \otimes |02\rangle_{AA'}\langle 02|, \quad (\text{A.1})$$

where $\tilde{\rho}_{AB} := \rho_{AB} \otimes |00\rangle_{A'B'}\langle 00|$, $\tilde{\sigma}_{AC} := \sigma_{AC} \otimes |11\rangle_{A'C'}\langle 11|$, $\tilde{\tau}_{BC} := \tau_{BC} \otimes |22\rangle_{B'C'}\langle 22|$ with the primed systems being classical flags and ρ_{AB} , σ_{AC} and τ_{BC} are the bipartite source states. Let us then consider n copies of ρ_{bs} , i.e.,

$$\rho_{bs}^{\otimes n} = \left(\frac{1}{3}\tilde{\rho}_{AB} \otimes |00\rangle_{CC'}\langle 00| + \frac{1}{3}\tilde{\sigma}_{AC} \otimes |01\rangle_{BB'}\langle 01| + \frac{1}{3}\tilde{\tau}_{BC} \otimes |02\rangle_{AA'}\langle 02| \right)^{\otimes n}. \quad (\text{A.2})$$

This state can be written, using a multinomial expansion, as

$$\rho_{bs}^{\otimes n} = \sum_{\substack{k_1, k_2, k_3 \geq 0 \\ k_1 + k_2 + k_3 = n}} \frac{1}{3^n} \mathcal{P} \left[(\tilde{\rho}_{AB} \otimes |00\rangle_{CC'}\langle 00|)^{\otimes k_1} \otimes (\tilde{\sigma}_{AC} \otimes |01\rangle_{BB'}\langle 01|)^{\otimes k_2} \otimes (\tilde{\tau}_{BC} \otimes |02\rangle_{AA'}\langle 02|)^{\otimes k_3} \right], \quad (\text{A.3})$$

where \mathcal{P} indicates a sum over all possible permutations of the tensor product terms, as the tensor product is not commutative. The parties now can perform the following local operations: they perform projective measurements on all their flags and obtain a string of outcomes that determines uniquely in which term of the mixture they are. Thus, they can trace out all flag systems and all copies of ρ_{AB} , σ_{AC} and τ_{BC} except one, obtaining the source state $\rho_{AB} \otimes \sigma_{A'C'} \otimes \tau_{B'C'}$. The described operations are local operations that do not involve any classical communication but only measurements and tracing out. We will indicate these local operations as $\mathcal{M}_{AA'} \otimes \mathcal{M}_{BB'} \otimes \mathcal{M}_{CC'}$. It is important to note that not all terms of the mixture are transformed in the source state by these local operations: in fact, if $k_1 = 0$, $k_2 = 0$ or $k_3 = 0$ the

resulting state will be different. For example, if $k_1 = 0$, the resulting state will be $|00\rangle_{AB}\langle 00| \otimes \sigma_{A'C} \otimes \tau_{B'C'}$. Overall, we can describe the state after the aforementioned local operation as

$$\begin{aligned}
\mathcal{M}_{AA'} \otimes \mathcal{M}_{BB'} \otimes \mathcal{M}_{CC'} \left[\rho_{bs}^{\otimes n} \right] &= \\
&= \frac{1}{3^n} \rho_{AB} \otimes |0000\rangle_{A'B'C_1C'} \langle 0000| + \frac{1}{3^n} \sigma_{A'C} \otimes |0000\rangle_{ABB'C'} \langle 0000| \\
&+ \frac{1}{3^n} \tau_{B'C'} \otimes |0000\rangle_{AA'BC} \langle 0000| + \frac{1}{3^n} \sum_{\substack{k_2, k_3 > 0 \\ k_2 + k_3 = n}} \binom{n}{k_2 \ k_3} \sigma_{A'C} \otimes \tau_{B'C'} \otimes |00\rangle_{AB} \langle 00| \\
&+ \frac{1}{3^n} \sum_{\substack{k_1, k_3 > 0 \\ k_1 + k_3 = n}} \binom{n}{k_1 \ k_3} \rho_{AB} \otimes \tau_{B'C'} \otimes |00\rangle_{A'C} \langle 00| \\
&+ \frac{1}{3^n} \sum_{\substack{k_1, k_2 > 0 \\ k_1 + k_2 = n}} \binom{n}{k_1 \ k_2} \rho_{AB} \otimes \sigma_{A'C} \otimes |00\rangle_{B'C'} \langle 00| \\
&+ \frac{1}{3^n} \sum_{\substack{k_1, k_2, k_3 > 0 \\ k_1 + k_2 + k_3 = n}} \binom{n}{k_1 \ k_2 \ k_3} \rho_{AB} \otimes \sigma_{A'C} \otimes \tau_{B'C'}, \tag{A.4}
\end{aligned}$$

where $\binom{n}{k_1 \dots k_m} = \frac{n!}{k_1! \dots k_m!}$ is the multinomial coefficient. We now use that $\sum_{k_1, \dots, k_m} \binom{n}{k_1 \dots k_m} = m^n$ to write the following

$$\sum_{\substack{k_1, k_2 > 0 \\ k_1 + k_2 = n}} \binom{n}{k_1 \ k_2} = \sum_{\substack{k_1, k_2 \geq 0 \\ k_1 + k_2 = n}} \binom{n}{k_1 \ k_2} - 2 = 2^n - 2. \tag{A.5}$$

Moreover, with similar calculations we have

$$\sum_{\substack{k_1, k_2, k_3 > 0 \\ k_1 + k_2 + k_3 = n}} \binom{n}{k_1 \ k_2 \ k_3} = \sum_{\substack{k_1, k_2, k_3 \geq 0 \\ k_1 + k_2 + k_3 = n}} \binom{n}{k_1 \ k_2 \ k_3} - 3 \sum_{\substack{k_1, k_2 > 0 \\ k_1 + k_2 = n}} \binom{n}{k_1 \ k_2} - 3 = 3^n - 3(2^n - 2) - 3 \tag{A.6}$$

We can therefore recast Eq. (A.4) as

$$\begin{aligned}
\mathcal{M}_{AA'} \otimes \mathcal{M}_{BB'} \otimes \mathcal{M}_{CC'} \left[\rho_{bs}^{\otimes n} \right] &= \\
&= \frac{1}{3^n} \rho_{AB} \otimes |0000\rangle_{A'B'C_1C'} \langle 0000| + \frac{1}{3^n} \sigma_{A'C} \otimes |0000\rangle_{ABB'C'} \langle 0000| \\
&+ \frac{1}{3^n} \tau_{B'C'} \otimes |0000\rangle_{AA'BC} \langle 0000| + \frac{1}{3^n} (2^n - 2) \sigma_{A'C} \otimes \tau_{B'C'} \otimes |00\rangle_{AB} \langle 00| \\
&+ \frac{1}{3^n} (2^n - 2) \rho_{AB} \otimes \tau_{B'C'} \otimes |00\rangle_{A'C} \langle 00| + \frac{1}{3^n} (2^n - 2) \rho_{AB} \otimes \sigma_{A'C} \otimes |00\rangle_{B'C'} \langle 00| \\
&+ \frac{1}{3^n} (3^n - 3(2^n - 2) - 3) \rho_{AB} \otimes \sigma_{A'C} \otimes \tau_{B'C'}, \tag{A.7}
\end{aligned}$$

which can be further simplified as

$$\mathcal{M}_{AA'} \otimes \mathcal{M}_{BB'} \otimes \mathcal{M}_{CC'} \left[\rho_{bs}^{\otimes n} \right] = \left(\frac{3 + 3(2^n - 2)}{3^n} \right) \rho_{trash} + \left(1 - \frac{3 + 3(2^n - 2)}{3^n} \right) \rho_{source}, \quad (\text{A.8})$$

where we defined

$$\begin{aligned} \rho_{trash} := & \frac{1}{3 + 3(2^n - 2)} \\ & (\rho_{AB} \otimes |0000\rangle_{A'B'CC'} \langle 0000| + \sigma_{A'C} \otimes |0000\rangle_{ABB'C'} \langle 0000| \\ & + \tau_{B'C'} \otimes |0000\rangle_{AA'BC} \langle 0000| + (2^n - 2)(\sigma_{A'C} \otimes \tau_{B'C'} \otimes |00\rangle_{AB} \langle 00| \\ & + \rho_{AB} \otimes \tau_{B'C'} \otimes |00\rangle_{A'C} \langle 00| + \rho_{AB} \otimes \sigma_{A'C} \otimes |00\rangle_{B'C'} \langle 00|) \end{aligned} \quad (\text{A.9})$$

and $\rho_{source} := \rho_{AB} \otimes \sigma_{A'C} \otimes \tau_{B'C'}$. We now remark that

$$\lim_{n \rightarrow \infty} \frac{3 + 3(2^n - 2)}{3^n} = 0, \quad (\text{A.10})$$

so that $\mathcal{M}_{AA'} \otimes \mathcal{M}_{BB'} \otimes \mathcal{M}_{CC'} \left[\rho_{bs}^{\otimes n} \right] \rightarrow \rho_{source}$ for $n \rightarrow \infty$, concluding the proof.

Genuine multipartite entanglement is not a precondition for secure conference key agreement

Title: Genuine multipartite entanglement is not a precondition for secure conference key agreement

Authors: Giacomo Carrara, Hermann Kampermann, Dagmar Bruß, Gláucia Murta

Journal: Physical Review Research

Publication status: Published

Date of publication: 19 March 2021

This publication corresponds to reference [Car+21]. A summary of its content can be found in chapter 7. The core idea behind the work, to show that non-GME states can be used for CKA, was given to me by GM. I developed the idea and expanded upon it under the guidance of GM, proving Theorem 1 and finding a suitable class of states for CKA with biseparable states. HK and DB participated in all the discussions and provided crucial insights, giving in particular the suggestion to further look into the entanglement witness theory, which led to the results contained in the last section of the paper. GM also pushed me to perform the noise analysis and the comparison with the concatenation of bipartite QKD protocols. I wrote the manuscript, which was proofread by all other co-authors who gave valuable feedback on how to improve it.

Genuine multipartite entanglement is not a precondition for secure conference key agreement

Giacomo Carrara^{*,*}, Hermann Kampermann, Dagmar Bruß, and Gláucia Murta[†]

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany



(Received 30 July 2020; accepted 16 February 2021; published 19 March 2021)

Entanglement plays a crucial role in the security of quantum key distribution. A secret key can only be obtained by two parties if there exists a corresponding entanglement-based description of the protocol in which entanglement is witnessed, as shown by Curty *et al.* [M. Curty, M. Lewenstein, and N. Lütkenhaus, *Phys. Rev. Lett.* **92**, 217903 (2004)]. Here we investigate the role of entanglement for the generalization of quantum key distribution to the multipartite scenario, namely, conference key agreement. In particular, we ask whether the strongest form of multipartite entanglement, namely, genuine multipartite entanglement, is necessary to establish a conference key. We show that, surprisingly, a nonzero conference key can be obtained even if the parties share biseparable states in each round of the protocol. Moreover, we relate conference key agreement with entanglement witnesses and show that a nonzero conference key can be interpreted as a nonlinear entanglement witness that detects a class of states which cannot be detected by usual linear entanglement witnesses.

DOI: [10.1103/PhysRevResearch.3.013264](https://doi.org/10.1103/PhysRevResearch.3.013264)

I. INTRODUCTION

Secure communication is a central demand for modern society. Security can be provided by quantum key distribution (QKD), which readily enters the industrial market. In QKD [1,2], entanglement plays a crucial role in the security proofs [3,4]. Indeed, even prepare-and-measure protocols [1,5], which do not require any entanglement for their implementation, have an entanglement-based counterpart [6] which can be used for the protocol's security analysis. In Ref. [7], the authors showed that entanglement is in fact a necessary condition to obtain a secure key in a QKD protocol and, moreover, the entanglement of the state shared by Alice and Bob can be witnessed using the measurements performed in the protocol.

We consider a generalization of QKD to the scenario where N parties wish to establish a common shared secret key. This task is called a conference key agreement (CKA) and allows for secure broadcast. CKA can be achieved using a concatenation of bipartite QKD [8–10], together with additional classical communication. However, the rich structure of multipartite correlations opens the possibility to design new protocols which can have clear advantages in certain network architectures [11]. Several protocols exploiting the correlations of multipartite entangled states have been proposed using qubit systems in the device-dependent [11–15] and device-independent scenario [16–18], as well as continuous-variable systems [19–21]. Even a proof of princi-

ple implementation of CKA with four nodes has been recently realized [22].

Here we ask the question of whether the strongest form of multipartite entanglement, namely, genuine multipartite entanglement, is a necessary ingredient for CKA based on multipartite quantum correlations. We will show that, counter-intuitively, this is not the case: N parties can establish a secret conference key even when the state distributed in each round of the protocol is biseparable. Moreover, we prove that, to obtain a no-zero conference key, the measurements used in the protocol need to be able to witness entanglement across any partition of the set of parties, extending the result of Ref. [7] to the multipartite scenario.

II. PRELIMINARIES

We focus on CKA protocols [23] consisting of several rounds where, in each round, a single copy of a multipartite state is distributed to the N parties, namely, Alice and Bob₁, ..., Bob _{$N-1$} . Upon receiving the systems, the parties perform local measurements and record the classical outcome. The scenario is sketched in Fig. 1.

In such protocols, an important figure of merit is the asymptotic secret key rate, i.e., the ratio between the number of extracted secret bits and the number of shared copies of the state, in the limit of an infinite number of rounds. Analogously to the bipartite case [24,25], the asymptotic secret key rate of the CKA protocols under consideration can be expressed, after the usual postprocessing (parameter estimation, one-way information reconciliation and privacy amplification) as [11]

$$r^\infty = \max [0, H(X|E) - \max_i H(X|Y_i)], \quad (1)$$

where X and Y_i denote the registers that store the outcomes of the measurements performed by Alice and Bob _{i} , respectively, in the key generation rounds. Here $H(X|E) = H(XE) - H(E)$ is the von Neumann entropy of Alice's outcome in the key generation rounds, conditioned on Eve's

*carrara@uni-duesseldorf.de

†glauca.murta@uni-duesseldorf.de

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International license](https://creativecommons.org/licenses/by/4.0/). Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

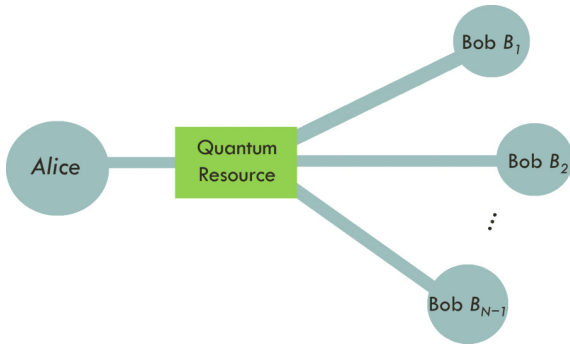


FIG. 1. Sketch of the considered CKA scenario: At each round of the protocol, a quantum resource is distributed to the parties (in our particular case, a multipartite quantum state). The parties perform local measurements and utilize the outcomes to extract a common secret key.

(possibly quantum) side information. $H(X|Y_i) = H(XY_i) - H(Y_i)$ represents the amount of information Alice needs to communicate to Bob_{*i*} so he can correct his raw key. The maximum over the Bobs in Eq. (1) illustrates the fact that Alice needs to communicate enough information to correct for the worst case of the Bobs. We recall that for a state ρ_X of a system X , the quantum von Neumann entropy is defined as $[H(X) = -\text{Tr}[\rho_X \log_2 \rho_X]]$.

The conditional von Neumann entropy satisfies the following properties [26]:

- (1) Additivity for product states [[26], Corollary 5.9]: If $\rho_{AB} = \rho_A \otimes \rho_B$, then $H(A|B) = H(A)$.
- (2) Data processing [[26], Corollary 5.5]: Considering ρ_{ABC} , then $H(A|BC) \leq H(A|B)$.
- (3) Conditioning on classical information [[26], Proposition 5.4]: If $\rho_{ABF} = \sum_j q_j \rho_{AB}^j \otimes |j\rangle\langle j|_F$ is a classical-quantum state where the system F is a classical register, then $H(A|BF) = \sum_j q_j H(A|BF = j)$ where $H(A|BF = j)$ is evaluated on the state ρ_{AB}^j .

Our goal is to investigate the role of multipartite entanglement in the single copy of the state shared by the N parties in each round of the protocol. In the bipartite case, either the state is separable and no key can be extracted or the state is entangled and can potentially be used for QKD [7]. In the multipartite scenario, however, different classes of entanglement can be defined, which have been extensively studied [27–31].

Let S_α be a proper subset of the parties and \bar{S}_α be the complement. Then a state $\rho_{AB_1 \dots B_{N-1}}$ is *separable with respect to the partition* $S_\alpha|\bar{S}_\alpha$ if it is of the form

$$\rho_{AB_1 \dots B_{N-1}} = \sum_j q_j \rho_{S_\alpha}^j \otimes \rho_{\bar{S}_\alpha}^j, \quad (2)$$

where $\rho_{S_\alpha}^j$ and $\rho_{\bar{S}_\alpha}^j$ are states shared by the parties in S_α and \bar{S}_α , respectively, and where $q_j \geq 0$ and $\sum_j q_j = 1$.

A state is called *biseparable* [27] if it is a convex combination of states that are separable with respect to different partitions, that is,

$$\rho_{bs} = \sum_{S_\alpha} \sum_j q_{S_\alpha}^j \rho_{S_\alpha}^j \otimes \rho_{\bar{S}_\alpha}^j, \quad (3)$$

where the first sum is performed over all proper subsets S_α of the parties. Again, the coefficients must satisfy $q_{S_\alpha}^j \geq 0 \forall j, S_\alpha$ and $\sum_\alpha \sum_j q_{S_\alpha}^j = 1$. It is worth noting that a state can be biseparable, yet not separable with respect to any partition.

Finally, if a state cannot be written in the form of Eq. (3) we call it *genuine multipartite entangled (GME)*. All CKA protocols based on multipartite entanglement proposed so far [11–17, 19–21] explore the correlations of GME states, such as the Greenberger-Horne-Zeilinger (GHZ) state [32] or the W state [33].

III. ENTANGLEMENT IS NECESSARY FOR CKA

In the following, we prove that entanglement across all partitions in the state shared by the parties is necessary to lead to a nonzero asymptotic conference key rate.

Theorem 1. Given a CKA protocol, if the state shared by the N parties is separable with respect to some partition $S_\alpha|\bar{S}_\alpha$, then $r^\infty = 0$.

Proof of Theorem 1 To prove the statement, since the asymptotic key rate in Eq. (1) includes an optimization over all the Bobs, it suffices to prove that $H(X|Y_i) \geq H(X|E)$ for a specific Bob_{*i*}. Let us consider a state separable with respect to a partition $S_\alpha|\bar{S}_\alpha$, in the form of Eq. (2), such that S_α contains Alice. We consider a Bob contained in \bar{S}_α , let us say Bob_{*l*}. Let Eve have a purification of the state of the form

$$|\psi_{AB_1, \dots, B_{N-1} E F F'}\rangle = \sum_j \sqrt{q_j} |\psi_{S_\alpha \bar{S}_\alpha E}^j\rangle |j\rangle_F |j\rangle_{F'}, \quad (4)$$

where $|\psi_{S_\alpha \bar{S}_\alpha E}^j\rangle$ is a purification of $\rho_{S_\alpha}^j \otimes \rho_{\bar{S}_\alpha}^j$ and the systems F and F' are classical registers held by Eve. The additional classical register F' is necessary to exploit the properties of the von Neumann entropy of classical-quantum states. In fact, tracing out the system F' , Eve’s system E and all the Bobs except Bob_{*l*} will result in a state of the form

$$\rho_{AB_l F} = \sum_j q_j \rho_A^j \otimes \rho_{B_l}^j \otimes |j\rangle\langle j|_F, \quad (5)$$

which is a classical-quantum state consisting of a separable state for Alice and Bob B_l , paired with the classical register F held by Eve. We remark that performing local measurements on a separable state will result in a separable state. Thus, after the measurements of the CKA protocol, the state will still be in the form of Eq. (5). Moreover, we can write the following chain of inequalities:

$$\begin{aligned} H(X|Y_l) &\geq H(X|Y_l F) \\ &= \sum_j q_j H(X|Y_l F = j) \\ &= \sum_j q_j H(X|F = j) \\ &= H(X|F) \geq H(X|E F F') = H(X|E_{\text{tot}}), \end{aligned} \quad (6)$$

where E_{tot} indicates the global subsystem of Eve, which includes the classical registers. In the first, second, and third line we used Property 2, Property 3, and Property 1 of the conditional Von Neumann entropy, respectively. Finally, in the

fourth line we used again Properties 2 and 3. This concludes the proof.

It follows that there must be some entanglement shared between Alice and all the Bobs to establish a secret common key. It is worth noting that for $N = 2$ this proof simplifies the argumentation given in Ref. [7].

IV. CKA WITHOUT GME

We will now focus on the main question, that is, whether a positive conference key can be established without GME. We answer this question in the affirmative by exhibiting a family of biseparable states that can lead to a nonzero conference key,

$$\rho_{AB_1, \dots, B_{N-1}}^{(N,k)} = \sum_{\alpha \in \mathcal{S}^{(k)}} \frac{1}{\mathcal{N}} \Phi_{S_\alpha}^{\text{GHZ},k} \bigotimes_{B_m \in S_\alpha} |+\rangle\langle +|_{B_m}, \quad (7)$$

where $\mathcal{S}^{(k)}$ is the set of subsets of k parties that contain Alice and $k - 1$ Bobs, $\Phi_{S_\alpha}^{\text{GHZ},k} = |\text{GHZ}\rangle\langle \text{GHZ}|_{S_\alpha}$ is the projector of the GHZ state shared by the k parties of the subset S_α , defined as $|\text{GHZ}\rangle_{S_\alpha} = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes k} + |1\rangle^{\otimes k})$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The normalization factor is equal to $\mathcal{N} = \binom{N-1}{k-1}$ since the number of terms in the convex combination is equal to the number of subsets of cardinality $k - 1$ within the $N - 1$ Bobs.

We show that this family of states can be used to generate a nonzero key in a simple CKA protocol, namely, the N-BB84 protocol [14]. The N-BB84 protocol consists of X -basis measurements for the parameter estimation rounds and Z -basis measurements for the key generation rounds.

The asymptotic conference key rate of the N-BB84 protocol for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, Eq. (7), as a function of the total number of parties N and the number of parties k that are entangled is given by

$$r_{N\text{-BB84}}^\infty(N, k) = \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \quad (8)$$

A strictly positive rate $r_{N\text{-BB84}}^\infty(N, k)$ is obtained for all possible values of N and k even though the family of states Eq. (7) is biseparable for $k < N$. Therefore, we have proven our main result:

Theorem 2. Genuine multipartite entanglement is not necessary for CKA, and a nonzero secret conference key rate r^∞ can be established in a CKA protocol that uses biseparable states at each round.

A detailed derivation of $r_{N\text{-BB84}}^\infty(N, k)$ is presented in Appendix A. Moreover, in Appendix B, we show that the key rate given in Eq. (8) is optimal for the family of states Eq. (7), when the key is generated with measurements in the Z basis.

In Fig. 2 we plot the secret key rate, $r_{N\text{-BB84}}^\infty(N, k)$, as a function of the number of parties N for different values of the number of entangled parties k . For comparison, we also plot the key rate of a CKA protocol based on the concatenation of multiple bipartite QKD protocols, in the noiseless scenario, for a network with bottleneck [11]. In this case, Alice runs $N - 1$ bipartite QKD protocols to establish a secret key with each of the Bobs.

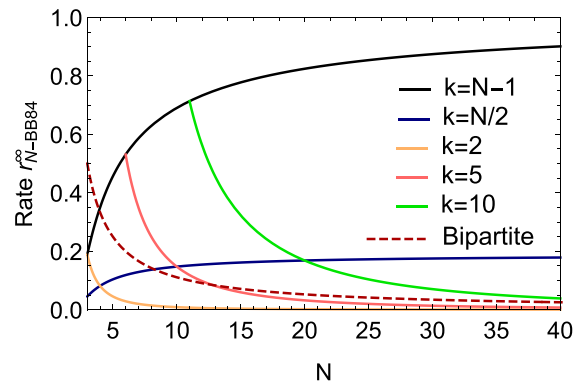


FIG. 2. Asymptotic secret key rate, $r_{N\text{-BB84}}^\infty(N, k)$, for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, Eq. (7), for the N -BB84 CKA protocol. The curves (straight lines) represent different values of k (light grey: from left to right, $k = 2, k = 5, k = 10$; dark grey: top, $k = N - 1$, bottom, $k = \frac{N}{2}$). We also plot the key rate of CKA based on multiple noiseless bipartite QKD protocols (dashed line), both as a function of N . We remark that since $k \leq N - 1$, the curves for fixed k start at different values of N .

Figure 2 shows that $r_{N\text{-BB84}}^\infty$ approaches 1 as N increases, if k equals $N - 1$. Moreover, even in the case when only two parties, Alice and one of the Bobs, are entangled in each term of the mixture, a nonzero secret key can be obtained. However, for a fixed value of k , $r_{N\text{-BB84}}^\infty \rightarrow 0$ as N increases. The comparison with the key rate of a concatenation of multiple bipartite QKD protocols yields interesting results: while, on one hand, no advantage can be obtained for $k = 2$, on the other hand an advantage can be obtained in the regime of a k close to N , with a marked advantage for high k .

To further analyze the advantage obtainable with the presented protocol compared to the concatenation of bipartite QKD protocols, we evaluate the performance of the family of states Eq. (7) in the presence of noise. We consider the case where the qubit of each Bob undergoes a *local depolarizing channel* \mathcal{D} , where $\mathcal{D}[\rho] = (1 - p)\rho + p\frac{1}{2}$. We compare this with a concatenation of bipartite QKD protocols that undergo the same type of noise. Details of this analysis can be found in Appendix C. Figure 3 illustrates the result for $N=6$. Even in the noisy scenario, an advantage can be obtained in the low noise regime and for k close to N .

Our results show that CKA without GME states is possible. We remark that in Ref. [34] the authors have established that GME is a necessary condition for a nonzero key in a one-shot CKA protocol. This result, at first, seems in contradiction to our findings, however, Ref. [34] refers to the *global* input state, that for the class of protocols we consider would be $\rho_{AB_1, \dots, B_{N-1}}^{\otimes n}$, where n is the number of rounds. Since the set of biseparable states is not closed under tensor product, the global input state can be GME even if the single copy of the state is biseparable. Here we focus on analyzing the entanglement properties of the single copy of the states. This is because we consider a class of protocols in which the states are distributed and measured at each round, therefore, no storage or quantum global operation on all the copies is required.

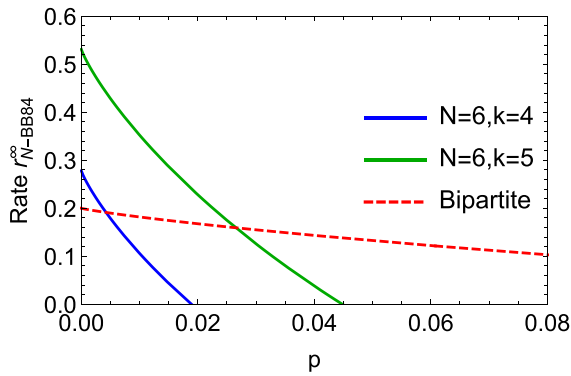


FIG. 3. Plot of the asymptotic key rate of the N-BB84 protocol for the state of Eq. (7) undergoing local depolarizing noise (solid lines), as a function of the depolarizing channel parameter p , for fixed $N = 6$ and different k : $k = 4$ (blue, left) and $k = 5$ (green, right). The results are compared with the key rate of a concatenation of noisy bipartite BB84 QKD protocols (red dashed line).

V. CKA AND ENTANGLEMENT WITNESSES

Theorem 1 provides us with a necessary condition to obtain a nonzero key rate in a CKA protocol. We now want to extend to the multipartite scenario the bipartite result presented in Ref. [7]: no secret key can be extracted in a QKD protocol unless Alice and Bob are able to witness entanglement in the shared state using the measurements performed in the protocol. An entanglement witness [31,35,36] is a Hermitian operator W such that $\text{Tr}(W\sigma) \geq 0$ for all separable states σ and $\text{Tr}(W\rho) < 0$ for at least one entangled state ρ . This definition of an entanglement witness is based on the fact that the set of separable states is closed and convex, and can thus be separated with a hyperplane from its complement [35,37]. In the multipartite scenario, given the more intricate structure of possible correlations, witnesses can be defined to distinguish different classes of states [31]. We thus consider the same approach of Ref. [[7], Theorem 1]: Starting from the measurements performed by the parties, we analyze the entanglement witnesses that can be constructed with them. We obtain the following theorem.

Theorem 3. Given a CKA protocol in which the parties use a set of local measurements, for the test and key generation rounds, which are represented by the Positive Operator-Valued Measures (POVMs) $\{G_x^a\}, \{G_{y_1}^{b_1}\}, \dots, \{G_{y_{N-1}}^{b_{N-1}}\}$, where a, b_1, \dots, b_{N-1} indicate the outputs of the measurements labeled by x, y_1, \dots, y_{N-1} , then one can obtain a nonzero asymptotic conference key rate $r^\infty > 0$ only if the presence of entanglement can be proved across any partition of the parties into two subsets.

Moreover, the presence of entanglement across each bipartition can be verified through a set of entanglement witnesses of the form

$$W_\alpha = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}, a, b_1, \dots, b_{N-1}}^{(\alpha)} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}}, \quad (9)$$

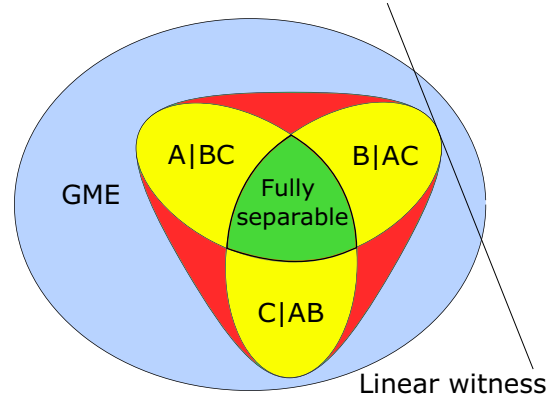


FIG. 4. Schematic representation of the set of tripartite states, adapted from Ref. [38]. In light blue (outer set) is represented the set of GME states. In red (dark grey area) is highlighted the set of biseparable states that are not separable with respect to any fixed partition, whereas in yellow (light grey) are represented the sets of states that are separable with respect to a fixed partition. In the middle, in green, is represented the set of fully separable states. A linear witness defines a hyperplane in the space of states. A nonzero conference key rate can be seen as a nonlinear entanglement witness, as it can detect states in the red area, i.e., outside a nonconvex set.

where α labels the partition $S_\alpha|\bar{S}_\alpha$ with S_α being a proper subset of the parties and \bar{S}_α is its complement, and where $c_{x, y_1, \dots, y_{N-1}, a, b_1, \dots, b_{N-1}}^{(\alpha)}$ are real coefficients.

The proof is given in Appendix D Theorem 3 implies that entanglement across any bipartition can be witnessed using the statistics of results of the measurements specified by the protocol, since the witness operators W_α are constructed from the POVM elements of these measurements. Theorem 3, combined with the results of the previous section, leads to the following Corollary.

Corollary 3.1. The figure of merit $r^\infty > 0$ is a nonlinear entanglement witness, detecting the presence of entanglement across any bipartition of the parties.

This corollary is due to the result of Theorem 3 in combination with the examples presented in the previous section: In fact, the union of all the sets of states that are separable with respect to a specific partition is not a convex set and thus cannot be separated by linear witnesses from its complement [35] (see Fig. 4). Moreover, if a CKA protocol is performed and a nonzero key rate is obtained, it is a necessary condition that the state shared by the parties is not separable across any partition of the parties. Therefore, a nonzero key rate reveals that the state utilized in the protocol is outside of the union of the sets of states that are separable with respect to a fixed partition. Finally, the results of the previous section tell us that non-GME states can also lead to a nonzero conference key, thus allowing us to conclude that the witness cannot be linear, hence the corollary.

VI. CONCLUSIONS

We addressed the question of whether GME is a necessary resource for a CKA protocol. We proved that, surprisingly, the parties can establish a conference key by sharing biseparable

states in each round of the protocol. To show this, we exhibited a family of suitable biseparable states, which lead to nonzero key rates in the simple N-BB84 CKA protocol. We showed that, in a network with bottleneck, the key rates achieved by our family of states outperform protocols based on a concatenation of bipartite QKD, especially for high numbers of entangled parties.

Furthermore, we related our results to the concept of entanglement witnesses, showing that a nonzero asymptotic conference key rate can only be obtained if one is able to detect entanglement, across any partition, in the state shared by the parties in each round of the CKA protocol. This extends the result of Ref. [7] for bipartite QKD to the multipartite scenario. As a consequence, we can infer that a nonzero asymptotic conference key rate represents a nonlinear entanglement witness, which can detect a type of entanglement that cannot be detected by the traditional linear entanglement witnesses.

Given our results, several lines of research can follow. For example, it is known that distillation of GHZ states starting from biseparable states is possible [31]. Moreover, the GHZ state can be used to generate a perfect conference key. It is an open question whether the considered class of CKA protocols is equivalent to the distillation of a GHZ state from biseparable states. Another open point is to establish converse bounds on the key rates achievable by different classes of multipartite entangled states for such simple CKA protocols. Finally, an interesting topic for further investigation is the consequence of our results for experimental implementations. An analysis tailored to particular setups and noise models could determine the payoff of using biseparable states to establish a conference key.

ACKNOWLEDGMENTS

We thank F. Grasselli for helpful discussions, and S. Das, S. Bäuml, M. Winczewski, and K. Horodecki for clarifying discussions about of the apparent contradiction of our results with Ref. [34]. We also thank an anonymous referee for valuable comments that inspired us to strengthen our results. This work was funded by the Deutsche Forschungsgemeinschaft (DFG) (the German Research Foundation) under Germany's Excellence Strategy–Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1–390534769.

APPENDIX A: CONFERENCE KEY RATE OF THE N-BB84 PROTOCOL WITH THE FAMILY OF STATES $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$

As a first step, we briefly sketch the N-BB84 protocol introduced in Ref. [14]. The protocol consists of the following steps:

- (1) A source distributes a state to the N parties.
- (2) The parties perform two type of measurements: For the parameter estimation rounds, they make measurements in the X basis. For the key generation rounds, they make measurements in the Z basis.
- (3) The parties compute the following parameters:

- (a) Using the outcomes of the parameter estimation rounds the parties compute

$$Q_X = \frac{1 - \langle X^{\otimes N} \rangle}{2}, \quad (\text{A1})$$

where $\langle X^{\otimes N} \rangle$ is the expectation value of the operator X for each party. Q_X represents the probability that the parties obtain an unexpected result from the parameter estimation rounds.

- (b) Using some of the outcomes of the key generation estimation rounds, the parties compute

$$Q_{AB_i} = \frac{1 - \langle Z_{AB_i} \rangle}{2}, \quad (\text{A2})$$

where $\langle Z_{AB_i} \rangle$ is the expectation value of the operator Z for Alice and Bob B_i . This parameter is computed for each Bob and represents the probability that Alice and Bob B_i get a discordant outcome in the key generation rounds.

- (4) The asymptotic key rate is given by

$$r_{N\text{-BB84}}^\infty = 1 - h(Q_X) - \max_i h(Q_{AB_i}), \quad (\text{A3})$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy.

To evaluate the performance of the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, Eq. (7), we need to evaluate the two parameters Q_X and Q_{AB_i} . It can be straightforwardly seen that $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, for all N and k is invariant under the application of the X operator on all parties. This implies $\langle X^{\otimes N} \rangle = 1$ and thus $Q_X = 0$ for any N and k .

To calculate $\langle Z_{AB_i} \rangle$, we remark that $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$ is a mixture of $\mathcal{N} = \binom{N-1}{k-1}$ terms, where each of these terms is a projector onto the GHZ state shared by Alice and $k-1$ Bobs, and a projector onto the $|+\rangle$ -state for the remaining Bobs. It is straightforward to see that $\langle Z_{AB_i} \rangle = 0$ for the terms in which Bob B_i is not entangled with Alice. On the other hand, the terms in which Bob B_i shares part of the GHZ state with Alice are invariant under the application of the Z operator on Alice and Bob B_i , so we obtain $\langle Z_{AB_i} \rangle = 1$ for these terms. Overall, the expectation value $\langle Z_{AB_i} \rangle$ reads

$$\langle Z_{AB_i} \rangle = \frac{f}{\mathcal{N}} = \frac{k-1}{N-1}, \quad (\text{A4})$$

where $f = \binom{N-2}{k-2}$ is the number of terms in which Bob B_i shares part of a GHZ state with Alice. We remark that, due to the symmetry of the state, this result holds for any Bob. Thus, dropping the index i we obtain

$$Q_{AB}(N, k) = \frac{N-k}{2(N-1)}. \quad (\text{A5})$$

With further, straightforward calculations, we obtain

$$\begin{aligned} r_{N\text{-BB84}}^\infty(N, k) &= 1 - h(Q_{AB}) = \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) \\ &\quad + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \end{aligned} \quad (\text{A6})$$

APPENDIX B: THE N-BB84 PROTOCOL IS OPTIMAL FOR Z MEASUREMENTS

In this Appendix, we prove that the N-BB84 protocol is the optimal protocol for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, when the parties use the Z basis for key generation. We prove this by analyzing the general class of protocol presented in the Introduction of the paper, thus assuming full state characterization. We show that the key rate of the N-BB84 protocol is identical to the one obtained assuming full tomography of the states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, thus proving that the N-BB84 protocol is optimal for this family of states.

1. Conditional entropy $H(X|E)$ for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$

Here we will calculate the conditional entropy $H(X|E)$ for a generalization of the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, as we consider states of the form

$$\rho_{AB_1, \dots, B_{N-1}} = \sum_{\alpha \in \mathcal{S}^{(k)}} q_\alpha \Phi_{S_\alpha}^{\text{GHZ},k} \bigotimes_{B_m \in S_\alpha} |+\rangle_{B_m} \langle +|_{B_m}, \quad (\text{B1})$$

$$\begin{aligned} \rho_{XB_1, \dots, B_{N-1}E} = & \sum_{\alpha, \beta \in \mathcal{S}^{(k)}} \frac{1}{2} \sqrt{q_\alpha q_\beta} \left(|0\rangle_X \langle 0| \bigotimes_{B_m \in I_{\alpha, \beta}} |0\rangle_{B_m} \langle 0| \bigotimes_{B_r \in \bar{U}_{\alpha, \beta}} |+\rangle_{B_r} \langle +| \bigotimes_{B_r \in S_\alpha \setminus I_{\alpha, \beta}} |0\rangle_{B_r} \langle +| \bigotimes_{B_r \in S_\beta \setminus I_{\alpha, \beta}} |+\rangle_{B_r} \langle 0| \otimes |e_\alpha\rangle \langle e_\beta| \right. \\ & \left. + |1\rangle_X \langle 1| \bigotimes_{B_m \in I_{\alpha, \beta}} |1\rangle_{B_m} \langle 1| \bigotimes_{B_r \in \bar{U}_{\alpha, \beta}} |+\rangle_{B_r} \langle +| \bigotimes_{B_r \in S_\alpha \setminus I_{\alpha, \beta}} |1\rangle_{B_r} \langle +| \bigotimes_{B_r \in S_\beta \setminus I_{\alpha, \beta}} |+\rangle_{B_r} \langle 1| \otimes |e_\alpha\rangle \langle e_\beta| \right), \quad (\text{B3}) \end{aligned}$$

where $I_{\alpha, \beta} = (S_\alpha \cap S_\beta)$ is the intersection and $U_{\alpha, \beta} = S_\alpha \cup S_\beta$ the union between the subsets of the Bobs in S_α and S_β , $\bar{U}_{\alpha, \beta}$ is the complement of $U_{\alpha, \beta}$, and $\rho_{XB_1, \dots, B_{N-1}E}$ indicates the state after Alice's measurement. We can then trace out all the Bobs, which leaves us with Alice and Eve's reduced state in the form

$$\begin{aligned} \rho_{XE} = & \sum_{\alpha, \beta} \frac{1}{2} \frac{\sqrt{q_\alpha q_\beta}}{2^{k-s_{\alpha, \beta}}} |0\rangle_X \langle 0| \otimes |e_\alpha\rangle \langle e_\beta| + \sum_{\alpha, \beta} \frac{1}{2} \frac{\sqrt{q_\alpha q_\beta}}{2^{k-s_{\alpha, \beta}}} |1\rangle_X \langle 1| \otimes |e_\alpha\rangle \langle e_\beta| \\ = & \sum_{\alpha, \beta} E_{\alpha, \beta} \frac{1}{2} (|0\rangle_X \langle 0| + |1\rangle_X \langle 1|) \otimes |e_\alpha\rangle \langle e_\beta| \\ = & \frac{\mathbb{1}_X}{2} \otimes \rho_E, \quad (\text{B4}) \end{aligned}$$

where $s_{\alpha, \beta}$ is the cardinality of $I_{\alpha, \beta}$, where we defined $E_{\alpha, \beta} = \frac{\sqrt{q_\alpha q_\beta}}{2^{k-s_{\alpha, \beta}}}$ in the second line of the equation and where $\rho_E = \sum_{\alpha, \beta} E_{\alpha, \beta} |e_\alpha\rangle \langle e_\beta|$ is Eve's reduced state. Finally, since ρ_{XE} is a product state, we can use Property 1 of the conditional entropy to write $H(X|E) = H(X) = 1$, thus concluding the proof.

2. Conference key rates for the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$

We now evaluate the analytical expression for the asymptotic key rate for the family of biseparable states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$, given by Eq. (7) in the main text. We recall that the number of terms in the convex combination is equal to the number of subsets of cardinality $k-1$ within the $N-1$ Bobs, which is equal to $\mathcal{N} = \binom{N-1}{k-1}$, and that we consider all the coefficients to be equal to $q_\alpha = \frac{1}{\mathcal{N}}$.

To calculate the asymptotic key rate, since $H(X|E) = 1$, as proven in Sec. B1, we need to evaluate the leakage $H(X|Y_i) \forall \text{ Bob}_i$ which, with our choice of coefficients, will be equal for all the Bobs. We thus calculate the reduced density matrix of Alice and Bob_{*i*} after they perform the key generation measurements, ρ_{XY_i} , to estimate the leakage term. Tracing out all the Bobs except one and performing the measurements both on Bob_{*i*} and Alice's side gives us the state

$$\rho_{XY_i} = \frac{1}{2} \frac{f}{\mathcal{N}} (|0\rangle_X \langle 0| \otimes |0\rangle_{Y_i} \langle 0| + |1\rangle_X \langle 1| \otimes |1\rangle_{Y_i} \langle 1|) + \left(1 - \frac{f}{\mathcal{N}}\right) \frac{\mathbb{1}_{XY_i}}{4}, \quad (\text{B5})$$

where $\Phi_{S_\alpha}^{\text{GHZ},k} = |\text{GHZ}\rangle \langle \text{GHZ}|_{S_\alpha}$ is the projector of the GHZ state shared by the parties of the subset S_α , defined as $|\text{GHZ}\rangle_{S_\alpha} = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes k} + |1\rangle^{\otimes k})$ and $|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$. We substituted $\frac{1}{\mathcal{N}}$ with some general real coefficients q_α such that $q_\alpha \geq 0 \forall \alpha$ and $\sum_\alpha q_\alpha = 1$.

We start the explicit calculation of the conditional entropy $H(X|E)$ by writing a purification of the state in Eq. (B1). An explicit valid purification of the state is given by

$$|\psi_{AB_1, \dots, B_{N-1}E}\rangle = \sum_{\alpha \in \mathcal{S}^{(k)}} \sqrt{q_\alpha} |\text{GHZ}\rangle_{S_\alpha} \bigotimes_{B_m \in S_\alpha} |+\rangle_{B_m} |e_\alpha\rangle, \quad (\text{B2})$$

where $\{|e_\alpha\rangle\}_\alpha$ is an orthonormal basis of Eve's subsystem of proper dimension. We thus look at the state after Alice performs her measurements on the Pauli Z basis. We obtain the following explicit expression of the state:

where f is the number of terms in which Bob $_i$ is entangled with Alice in the original state. The number f can be expressed in term of k and N as $f = \binom{N-2}{k-2}$. Thus the reduced density matrix in the computational basis has the form

$$\rho_{XY_i} = \begin{bmatrix} \frac{1}{4}(1 + C_{N,k}) & 0 & 0 & 0 \\ 0 & \frac{1}{4}(1 - C_{N,k}) & 0 & 0 \\ 0 & 0 & \frac{1}{4}(1 - C_{N,k}) & 0 \\ 0 & 0 & 0 & \frac{1}{4}(1 + C_{N,k}) \end{bmatrix}, \quad (\text{B6})$$

where $C_{N,k} = \frac{f}{N} = \frac{k-1}{N-1}$. Note that the reduced density matrix of Bob $_i$ after the measurement is $\rho_{Y_i} = \frac{\mathbb{1}_{Y_i}}{2}$. We therefore obtain

$$\begin{aligned} r^\infty(N, k) &= 1 - H(XY_i) + H(Y_i) \\ &= \frac{1}{2} \frac{N-k}{N-1} \log_2 \left(\frac{N-k}{N-1} \right) + \frac{1}{2} \frac{N+k-2}{N-1} \log_2 \left(\frac{N+k-2}{N-1} \right). \end{aligned} \quad (\text{B7})$$

The key rate obtained with this method is equivalent to Eq. (A6), thus proving that the N-BB84 protocol is optimal for Z -basis measurements for the key generation rounds.

APPENDIX C: NOISE ANALYSIS FOR THE N-BB84 PROTOCOL

In this Appendix, we consider a noise model for the N-BB84 protocol with the family of states $\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}$ and compare its performance with a concatenation of bipartite QKD protocols between Alice and $N-1$ Bobs, where all the channels between Alice and the Bobs are noisy. For a fair comparison, we thus consider local depolarizing noise. This corresponds to applying the map

$$\mathcal{D}[\rho] = (1-p)\rho + p\frac{\mathbb{1}}{2} \quad (\text{C1})$$

to each of the Bobs. The state we will consider will thus be

$$\rho_{AB_1, \dots, B_{N-1}}^{\text{noise}} = \mathcal{D}^{\otimes(N-1)}[\rho_{AB_1, \dots, B_{N-1}}^{(N,k)}]. \quad (\text{C2})$$

In this scenario, the parameters of the N-BB84 protocol can be analytically evaluated and read

$$Q_x = \frac{1 - (1-p)^{N-1}}{2}, \quad (\text{C3})$$

$$Q_{AB} = \frac{N-1 - (1-p)(k-1)}{2(N-1)}, \quad (\text{C4})$$

where, again, we dropped the index i since, due to the symmetry of the state, all Q_{AB_i} are equal. We thus can evaluate analytically the key rate for the N-BB84 protocol, which reads

$$\begin{aligned} r_{N\text{-BB84}}^\infty(N, k, p) &= \frac{1}{2}(1 - (1-p)^{N-1}) \log_2(1 - (1-p)^{N-1}) \\ &+ \frac{1}{2}(1 + (1-p)^{N-1}) \log_2(1 + (1-p)^{N-1}) \\ &+ \frac{N-1 - (1-p)(k-1)}{2(N-1)} \\ &\times \log_2 \left(\frac{N-1 - (1-p)(k-1)}{2(N-1)} \right) \\ &+ \frac{N-1 + (1-p)(k-1)}{2(N-1)} \log_2 \left(\frac{N-1 + (1-p)(k-1)}{2(N-1)} \right). \end{aligned} \quad (\text{C5})$$

We compare it with the scenario where Alice performs a bipartite BB84 protocol with each of the Bobs, sharing a maximally entangled state mixed with white noise, as in Eq. (C1). The resulting key rate of a concatenation of bipartite BB84 protocols reads [3,11]

$$r_{\text{QKD}}^\infty(N) = \frac{1 - 2h\left(\frac{p}{2}\right)}{N-1}, \quad (\text{C6})$$

where we divide the key rate of the bipartite BB84 protocol in the presence of white noise by the number of times Alice must perform the bipartite protocol to establish a secure key with each of the $N-1$ Bobs. The results are shown in Fig. 5. We can see that for some regimes, the N-BB84 protocol outperforms a concatenation of bipartite QKD protocols: For a low number of parties, we can obtain a marked advantage for k close to N in the low noise regime. Moreover, increasing the number of parties increases the advantage obtained and the range of k for which we can obtain it. However, we note that the N-BB84 protocol has a lower noise tolerance than the concatenation of bipartite QKD protocols, and thus for high noise regimes the latter is always preferred.

APPENDIX D: PROOF OF THEOREM 3

We give here the full proof of Theorem 3. For completeness, we repeat the statement of the theorem.

Theorem 3. Given a CKA protocol in which the parties use a set of local measurements, for the test and key generation rounds, which are represented by the POVMs $\{G_x^a\}, \{G_{y_1}^{b_1}\}, \dots, \{G_{y_{N-1}}^{b_{N-1}}\}$, where a, b_1, \dots, b_{N-1} indicate the outputs of the measurements labeled by x, y_1, \dots, y_{N-1} , then one can obtain a nonzero asymptotic conference key rate $r^\infty > 0$ only if the presence of entanglement can be proved across any partition of the parties.

Moreover, the presence of entanglement across each partition can be verified through a set of entanglement witnesses of the form

$$W_\alpha = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{(\alpha)} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}}, \quad (\text{D1})$$

where α labels the partition $S_\alpha | \bar{S}_\alpha$ with S_α being a proper subset of the parties and \bar{S}_α is its complement, and where $c_{x, y_1, \dots, y_{N-1}}^{(\alpha)}$ are real coefficients.

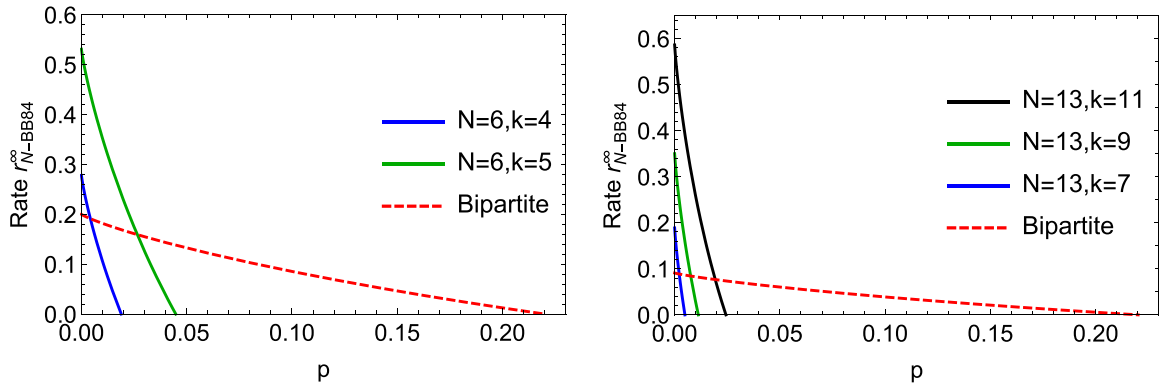


FIG. 5. Left panel: Plot of the asymptotic key rate of the N-BB84 protocol for the state of Eq. (C2) (solid lines) as a function of p , for fixed $N = 6$ and different k : $k = 4$ (blue, left) and $k = 5$ (green, right). The results are compared with the key rate of a concatenation of BB84 QKD protocols, given in Eq. (C6) (red dashed line), for $N = 6$, as a function of p . Right panel: Plot of the asymptotic key rate of the N-BB84 protocol for the state of Eq. (C2) (solid lines) as a function of p , for a fixed value of $N = 13$ and different values of k : $k = 7$ (blue, left), $k = 9$ (green, middle) and $k = 11$ (black, right). The results are compared with the key rate of a concatenation of BB84 QKD protocols, given in Eq. (C6) (red dashed line), for $N = 13$, as a function of p .

proof. We start by focusing on the probability distribution of the outcomes a, b_1, \dots, b_{N-1} given the inputs x, y_1, \dots, y_{N-1} of the measurements that can be performed in the test and key generation rounds of the CKA protocol, namely, $P(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1})$. The probability distributions are obtained as

$$P(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) = \text{Tr}(G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}} \rho_{AB_1 \dots B_{N-1}}), \quad (\text{D2})$$

where $G_x^a, G_{y_i}^{b_i}$ are the POVM elements of the measurements performed by Alice and Bob $_i$, respectively.

We analyze the map that maps each state into the corresponding probability distribution, given the measurements of the protocol, that is,

$$\Pi_{\text{CKA}} : \rho_{AB_1 \dots B_{N-1}} \mapsto \{P(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1})\}. \quad (\text{D3})$$

Considering a subset of the Hilbert space, namely, Σ , we call Σ^Π the projection of the subset Σ through the map Π_{CKA} , defined as in Eq. (D2). We now denote the set of states separable across the partition $S_\alpha|\bar{S}_\alpha$ as Σ_α . We note that Σ_α is a closed and convex set. Furthermore, the projection

of the set Σ_α through the linear map Π_{CKA} , namely, Σ_α^Π is still a closed and convex set. The elements of the projected set represent the probability distributions that come from states that are separable across the partition $S_\alpha|\bar{S}_\alpha$. Due to Theorem 1, a necessary condition to obtain a nonzero key rate is that the state is not separable with respect to any partition. This implies that, given a state $\rho_{A, B_1, \dots, B_{N-1}}^*$ that leads to a nonzero key rate in a specific protocol, the corresponding probability distribution $P^*(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1})$ is such that $P^*(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) \notin \Sigma_\alpha^\Pi \forall \alpha$. Moreover, since each Σ_α^Π is a convex and compact set, it is a well-known fact that each element of its complement $\bar{\Sigma}_\alpha^\Pi$ can be separated from Σ_α^Π with a proper hyperplane [35,37]. In the probability space, any hyperplane can be defined as

$$\sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}} P(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) = 0, \quad (\text{D4})$$

where $c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}}$ are real coefficients. Furthermore, for each probability distribution $P^*(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) \notin \Sigma_\alpha^\Pi \forall \alpha$, we can find, for each partition $S_\alpha|\bar{S}_\alpha$, coefficients $c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}(\alpha)}$, defining hyperplanes such that

$$\forall P_\alpha(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) \in \Sigma_\alpha^\Pi \quad \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}(\alpha)} P_\alpha(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) \geq 0 \quad \text{and}$$

$$\text{for } P^*(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) \notin \Sigma_\alpha^\Pi \forall \alpha, \quad \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}(\alpha)} P^*(a, b_1, \dots, b_{N-1}|x, y_1, \dots, y_{N-1}) < 0. \quad (\text{D5})$$

Finally, the coefficients define a set of entanglement witnesses in the form

$$W_\alpha = \sum_{\substack{x, y_1, \dots, y_{N-1} \\ a, b_1, \dots, b_{N-1}}} c_{x, y_1, \dots, y_{N-1}}^{a, b_1, \dots, b_{N-1}(\alpha)} G_x^a \otimes G_{y_1}^{b_1} \otimes \dots \otimes G_{y_{N-1}}^{b_{N-1}}, \quad (\text{D6})$$

such that, due to Eq. (D5), for each α :

$$\begin{aligned} \text{Tr}(W_\alpha \sigma_\alpha) &\geq 0, \quad \forall \sigma_\alpha \in \Sigma_\alpha \\ \text{Tr}(W_\alpha \rho_{A, B_1, \dots, B_{N-1}}^*) &< 0. \end{aligned} \quad (\text{D7})$$

As a matter of fact, Eq. (D7) tells us that the operator W_α is an entanglement witness [31,35] that detects entangle-

ment across partition $S_\alpha|\bar{S}_\alpha$. This concludes the proof of the theorem.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [4] H.-K. Lo, Proof of unconditional security of six-state quantum key distribution scheme, *Quantum Info. Comput.* **1**, 81 (2001).
- [5] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [6] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [7] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a Precondition for Secure Quantum Key Distribution, *Phys. Rev. Lett.* **92**, 217903 (2004).
- [8] C. Elliott, Building the quantum network, *New J. Phys.* **4**, 46 (2002).
- [9] M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, T. Walther, and J. Buchmann, The status of quantum-key-distribution-based long-term secure internet communication, *IEEE Trans. Sustain. Comput.*, 19 (2019).
- [10] 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, *et al.*, Satellite-Relayed Intercontinental Quantum Network, *Phys. Rev. Lett.* **120**, 030501 (2018).
- [11] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, *New J. Phys.* **19**, 093012 (2017).
- [12] A. Cabello, Multiparty key distribution and secret sharing based on entanglement swapping, [arXiv:quant-ph/0009025](https://arxiv.org/abs/quant-ph/0009025).
- [13] K. Chen and H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, *Quantum Info. Comput.* **7**, 689 (2007).
- [14] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, *New J. Phys.* **20**, 113014 (2018).
- [15] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, *New J. Phys.* **21**, 123002 (2019).
- [16] J. Ribeiro, G. Murta, and S. Wehner, Fully device-independent conference key agreement, *Phys. Rev. A* **97**, 022307 (2018).
- [17] J. Ribeiro, G. Murta, and S. Wehner, Reply to 'Comment on 'fully device-independent conference key agreement'', *Phys. Rev. A* **100**, 026302 (2019).
- [18] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Comment on 'Fully device-independent conference key agreement,' *Phys. Rev. A* **100**, 026301 (2019).
- [19] 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* **93**, 022325 (2016).
- [20] Z. Zhang, R. Shi, and Y. Guo, Multipartite continuous variable quantum conferencing network with entanglement in the middle, *Appl. Sci.* **8**, 1312 (2018).
- [21] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Modular network for high-rate quantum conferencing, *Commun. Phys.* **2** (2019).
- [22] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, [arXiv:2002.01491](https://arxiv.org/abs/2002.01491).
- [23] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, *Adv. Quantum Technol.* **3**, 2000025 (2020).
- [24] R. Renner, Security of quantum key distribution, [arXiv:quant-ph/0512258](https://arxiv.org/abs/quant-ph/0512258).
- [25] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A.* **461** (2005).
- [26] M. Tomamichel, *Quantum Information Processing with Finite Resources* (Springer, Cham, 2016).
- [27] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
- [28] M. Walter, D. Gross, and J. Eisert, Multi-partite entanglement [arXiv:1612.02437](https://arxiv.org/abs/1612.02437).
- [29] F. Clivaz, M. Huber, L. Lami, and G. Murta, Genuine-multipartite entanglement criteria based on positive maps, *J. Math. Phys.* **58**, 082201 (2017).
- [30] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, *Nat. Rev. Phys.* **1**, 72 (2019).
- [31] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep.* **474**, 1 (2009).
- [32] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond Bell's theorem [arXiv:0712.0921](https://arxiv.org/abs/0712.0921).
- [33] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, *Phys. Rev. A* **62**, 062314 (2000).
- [34] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, Universal limitations on quantum key distribution over a network [arXiv:1912.03646](https://arxiv.org/abs/1912.03646).
- [35] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, *Phys. Lett. A* **223**, 1 (1996).
- [36] B. M. Terhal, Detecting quantum entanglement, *Theor. Comput. Sci.* **287**, 313 (2002), natural Computing.
- [37] R. E. Edwards, *Functional Analysis, Theory and Application* (Holt, Rinehart and Winston, New York, 1965).
- [38] A. Acín, D. Bruß, M. Lewenstein, and A. Sanpera, Classification of Mixed Three-Qubit States, *Phys. Rev. Lett.* **87**, 040401 (2001).

Overcoming Fundamental Bounds on Quantum Conference Key Agreement

Title: Overcoming Fundamental Bounds on Quantum Conference
Key Agreement

Authors: Giacomo Carrara, Gláucia Murta, Federico Grasselli

Journal: Physical Review Applied

Publication status: Published


Date of publication: 6 June 2023

This publication corresponds to reference [CMG23]. A summary of its content can be found in chapter 7. The research project started as a continuation of FG's previous work [GKB19] on the generalization of TF-QKD to the multipartite scenario. FG proposed the basic idea of the idealized, PM protocol for 4 parties. I generalized the idea and managed to generalize the protocol for N users. Furthermore, under FG's guidance, I designed the practical protocol and developed the multipartite decoy-state analysis. I also proposed the security proof, which was further improved and refined by FG. GM participated in all the discussions and provided valuable ideas and feedback. I performed all the numerical simulations and produced all plots. All the results were carefully checked by GM and FG, who corrected minor mistakes. I wrote the first draft of the manuscript, which was then improved by FG, in particular regarding Section III, and GM.

Overcoming Fundamental Bounds on Quantum Conference Key Agreement

Giacomo Carrara¹, Gláucia Murta¹, and Federico Grasselli^{1*}

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, Düsseldorf D-40225, Germany

 (Received 20 January 2023; revised 25 January 2023; accepted 2 May 2023; published 6 June 2023)

Twin-field quantum key distribution (TFQKD) enables two distant parties to establish a shared secret key, by interfering weak coherent pulses (WCPs) in an intermediate measuring station. This allows TFQKD to reach greater distances than traditional QKD schemes and makes it the only scheme capable of beating the repeaterless bound on the bipartite private capacity. Here, we generalize TFQKD to the multipartite scenario. Specifically, we propose a practical conference key agreement protocol that only uses WCPs and linear optics and prove its security with a multiparty decoy-state method. Our protocol allows an arbitrary number of parties to establish a secret conference key by single-photon interference, enabling it to overcome recent bounds on the rate at which conference keys can be established in quantum networks without a repeater.

DOI: [10.1103/PhysRevApplied.19.064017](https://doi.org/10.1103/PhysRevApplied.19.064017)

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties to take advantage of quantum mechanical properties to share a common secret key with information-theoretic security. In the past decades, QKD developed at an increasingly high pace and today represents one of the most mature applications of quantum information science, both in terms of theoretical development and experimental implementation [1,2]. More recently, in view of building quantum communication networks, a lot of effort has been put into generalizing QKD to the multipartite scenario with conference key agreement (CKA) [3–9], which has already seen the first experimental implementations [10,11]. CKA exploits the correlations offered by multipartite entanglement to deliver the same conference key to a set of parties and it has recently been extended to guarantee anonymity of the communicating parties in a larger network [12–14].

However, CKA protocols are faced with the difficulty of establishing multipartite entanglement over large distances, limiting their applicability in real-world scenarios. In particular, most of the protocols proposed so far exploit Greenberger-Horne-Zeilinger (GHZ) correlations, which are known to be difficult to distribute at large distances [3–8].

In the bipartite case, a variant of QKD, named twin-field QKD (TFQKD) [15–19], enables two parties to share keys at much longer distances than most other QKD protocols. The founding idea of TFQKD [17–19] consists in a measurement-device independent (MDI) scheme where

a single photon sent by either of the parties interferes in an intermediate untrusted relay, thus halving the communication distance. This enables TFQKD to beat the well-known repeaterless Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound on the secret key capacity [20] (see also Refs. [21,22] for other preliminary bounds), as demonstrated by several experiments [23–33].

In an effort to extend the range of CKA, Ref. [34] introduces a CKA protocol based on single-photon interference that is inspired by the TFQKD setup. This protocol, however, is highly unpractical as it requires each party to entangle solid-state qubits with the optical signals sent to the relay. Moreover, each party must store their qubit until the relay announces the interference outcome and then measure the qubit accordingly.

Alternatively, more practical generalizations of TFQKD were devised in Refs. [8,35–37], where the parties are only required to send weak coherent pulses or interfere the pulses with linear optics. However, the protocols in Refs. [35–37] are not MDI and, what is more, are limited to tripartite configurations and cannot be scaled to an arbitrary number of parties.

In this work, we introduce an MDI CKA protocol that does not present such drawbacks. Our protocol can be realized using only weak coherent pulses interfered with linear optics at an untrusted relay and allows an arbitrary number of parties to establish a conference key. In particular, our protocol postselects correlations belonging to W -class states [38] through single-photon interference, independently of the number of parties. This enables our CKA protocol to operate at much higher losses than previous CKA schemes, which require either the simultaneous

*federico.grasselli@hhu.de

distribution of photonic multipartite entangled states [3–5,10,11] or the postselection of GHZ-type correlations [6–8].

We prove the security of our protocol against collective attacks in the asymptotic regime by developing a multiparty decoy-state analysis [39–41], through which we derive analytical upper bounds on multipartite yields. We simulate the performance of our protocol with a realistic channel model that accounts for photon loss, dark counts in the detectors as well as phase and polarization misalignment.

Furthermore, we benchmark the protocol's conference key rate with recent upper bounds that apply to arbitrary quantum networks, namely the single-message multicast bound derived in Ref. [42], adopting a similar approach used to benchmark bipartite TFQKD setups. In particular, we consider network architectures where the relay is removed and compute their single-message multicast bounds. Our simulations show that our CKA protocol can overcome such bounds for certain noise regimes and number of parties, thus paving the way for long-distance CKA in quantum networks.

The paper is structured as follows. In Sec. II we describe our CKA protocol and in Sec. III we prove its security. In Sec. IV we detail our multipartite decoy-state method. We simulate the protocol's performance in Sec. V and conclude in Sec. VI. Appendix A describes the optical setup in the untrusted relay. In Appendix B we draw the connection between our protocol and the correlations of W states. The analytical upper bounds on multipartite yields are derived in Appendix C. Appendix D contains details on the channel model and related calculations, while Appendix E provides details on the numerical simulations.

II. PROTOCOL

In this section we present our CKA protocol based on single-photon interference, which is schematically represented in Fig. 1. We limit the description to the asymptotic regime, where the effects due to finite detection statistics are negligible.

In the following, the symbol \vec{v} stands for the binary representation of the integer v , with components $v_i \in \{0, 1\}$, and $|\vec{v}|$ is the Hamming weight of the vector \vec{v} .

The CKA protocol is run by N parties, which we denote A_0, A_1, \dots, A_{N-1} .

Protocol 1 (CKA protocol)

1. Quantum state distribution and measurement: repeat the following steps a sufficiently large number of times.

1.1. Each party A_i prepares an optical mode a_i in a state that depends on whether the round is labeled as a PE round or KG round (the type of round could be predetermined, e.g., by a short preshared key held by every party [4,5]). In a PE round, they prepare a phase-randomized coherent

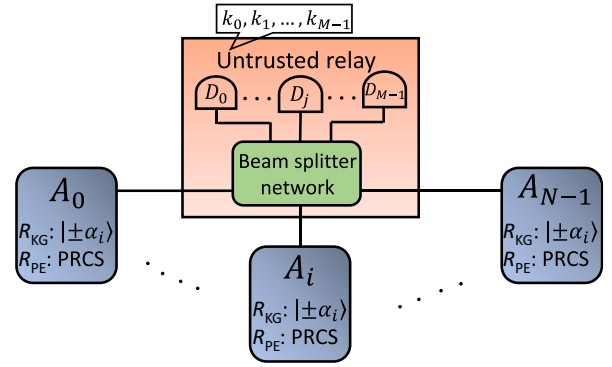


FIG. 1. Schematic representation of our CKA protocol. In a key generation (KG) round, each party sends one of two coherent states $|\pm\alpha_i\rangle$ at random. In a parameter estimation round (PE), they send a phase-randomized coherent state (PRCS). In an honest implementation of the protocol, the relay combines the signals from each party with a beam-splitter network with M inputs and a threshold detector at each of the M outputs (see Fig. 2 for the case $M = 4$ and Appendix A for general M). The relay announces the detection pattern $\vec{k} = (k_0, k_1, \dots, k_{M-1})$.

state (PRCS):

$$\rho_{a_i}(\beta_i) = e^{-\beta_i} \sum_{n=0}^{\infty} \frac{\beta_i^n}{n!} |n\rangle\langle n|, \quad (1)$$

where the intensity β_i of the coherent state is chosen at random from a finite set \mathcal{S}_i and where $|n\rangle$ is a Fock state. They record the intensity β_i . In a KG round, each party A_i prepares the coherent state $|x_i\alpha_i\rangle_{a_i}$ for a fixed $\alpha_i \in \mathbb{R}$, where $x_i = \pm 1$ is randomly chosen. They record the outcome x_i .

1.2. Every party sends their optical pulse to an untrusted relay through an insecure channel.

1.3. The untrusted relay performs an arbitrary operation on the N optical signals and announces the pattern $\vec{k} \in \{0, 1\}^M$, with $M \geq N$. [In an honest implementation of the protocol, $k_j = 1$ ($k_j = 0$) corresponds to a click (no click) in threshold detector D_j .] The round gets discarded if $|\vec{k}| \neq 1$ and we label Ω_j the event where $k_j = 1$ and $k_{\neq j} = 0$.

2. Parameter estimation: the parties partition their outcomes and intensities in M sets, where each set corresponds to the event Ω_j (for $j = 0, \dots, M-1$). For each partition, the parties reveal a fraction of their outcomes in order to estimate the probabilities $\Pr(\Omega_j | x_0, x_i, R_{KG})$ that event Ω_j occurs in a KG round, given that parties A_0 and A_i prepared coherent states $|x_0\alpha_0\rangle$ and $|x_i\alpha_i\rangle$, respectively. With the estimated probabilities, the parties calculate the quantum bit error rate (QBER) with respect to reference party A_0 , for every party pair and every partition (Q_{x_0, x_i}^j). Similarly, for each partition the parties reveal the intensities β_i used in the PE rounds and estimate the so-called *gains*, $G_{\beta_0, \dots, \beta_{N-1}}^j := \Pr(\Omega_j | \beta_0, \dots, \beta_{N-1})$, i.e.,

the probability of the event Ω_j in a PE round, given that the parties prepared PRCSSs in Eq. (1) with intensities $\beta_0, \dots, \beta_{N-1}$, respectively. Using the gains, the parties compute an upper bound (\overline{Q}_Z^j) on the phase error rate (Q_Z^j) of the protocol.

3. Classical postprocessing: the parties extract a secret conference key from the remaining (undisclosed) KG outcomes. To do so, for each partition labeled by Ω_j , party A_i flips their outcomes x_i when $(-1)^{\tilde{j}-i} = -1$. The parties then perform error correction and privacy amplification. The asymptotic conference key rate of the protocol is

$$r = \sum_{j=0}^{M-1} \Pr(\Omega_j | R_{\text{KG}}) \left[1 - h(\overline{Q}_Z^j) - \max_{i \geq 1} h(Q_{X_0 X_i}^j) \right], \quad (2)$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy and where $\Pr(\Omega_j | R_{\text{KG}}) = (1/4) \sum_{x_0, x_i = \pm 1} \Pr(\Omega_j | x_0, x_i, R_{\text{KG}})$ is the probability of event Ω_j in a KG round.

We prove the security of the CKA protocol in Sec. III. We remark that the security holds for any implementation of the quantum channels and of the relay, as far as the relay announces a pattern in every round.

In an honest implementation of the protocol, the optical signals are sent through potentially noisy and lossy channels to the relay, where they interfere in a balanced beam-splitter (BBS) network of M inputs and M outputs, with $M \geq N$ and M being a power of 2. The BBS network for $M = 4$ is depicted in Fig. 2, while the structure for generic M is reported in Appendix A. We note that the total number of beam splitters required by the BBS network scales favourably with the number N of parties, as $\mathcal{O}(N \log_2 N)$. The network transforms the input modes (\hat{a}_i^\dagger) in a balanced combination of the output modes (\hat{d}_j^\dagger), i.e.,

$$\hat{a}_i^\dagger \rightarrow \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (-1)^{\tilde{j}-i} \hat{d}_j^\dagger. \quad (3)$$

We point out that a setup designed with M inputs can be used by any number of parties $N \leq M$, by simply pairing the modes of the N parties with $M - N$ additional modes in the vacuum state. However, it is worth noting that adding unused ports in the BBS network introduces unwanted noise and may reduce the performance of the protocol. Then, the relay measures each output mode d_j with a threshold detector D_j , for $j = 0, \dots, M-1$, and announces the detection pattern $\vec{k} \in \{0, 1\}^M$, where $k_j = 1$ if detector D_j clicked and $k_j = 0$ otherwise. The round is retained only when exactly one detector clicks (event Ω_j for some j).

In the following, we provide the formulas to compute the QBER ($Q_{X_0 X_i}^j$) and the upper bound on the phase error

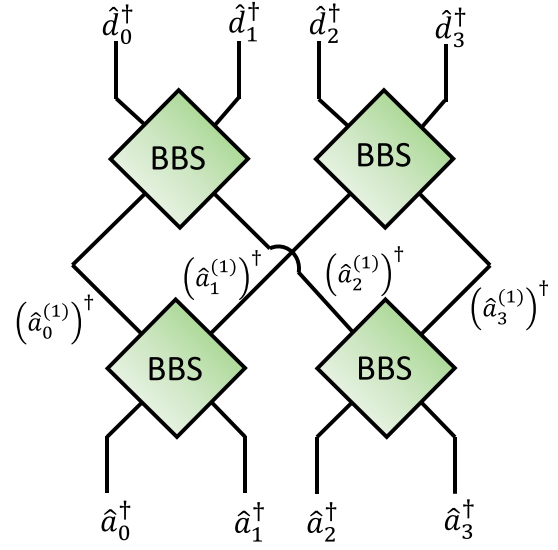


FIG. 2. BBS network for $M = 4$ inputs, which can be used by $N = 2$, $N = 3$, and $N = 4$ parties. We indicate the input modes with \hat{a}_i^\dagger and the output modes with \hat{d}_i^\dagger , for $i = 0, 1, 2, 3$. The network for a general number of inputs ($M = 2^s$) is described in Appendix A.

rate (\overline{Q}_Z^j). The QBER is defined for every pair of parties (A_0, A_i) and for every partition labeled by Ω_j , as follows:

$$Q_{X_0 X_i}^j = \Pr(X_0 \neq (-1)^{\tilde{j}-i} X_i | \Omega_j, R_{\text{KG}}), \quad (4)$$

where X_i is the binary random variable with outcomes $x_i = \pm 1$. The QBER is computed through Bayes' theorem:

$$Q_{X_0 X_i}^j = \sum_{x_0 \neq (-1)^{\tilde{j}-i} x_i} \frac{\Pr(\Omega_j | x_0, x_i, R_{\text{KG}})}{4 \Pr(\Omega_j | R_{\text{KG}})}. \quad (5)$$

The computation of the upper bound on the phase error rate is more involved. Indeed, it requires the derivation of upper bounds on quantities called *yields* and defined as

$$Y_{n_0, \dots, n_{N-1}}^j := \Pr(\Omega_j | n_0, \dots, n_{N-1}), \quad (6)$$

i.e., the probability of the event Ω_j given the hypothetical scenario where the parties send Fock states with photon numbers n_0, \dots, n_{N-1} . In Eq. (34), we provide analytical upper bounds ($\overline{Y}_{n_0, \dots, n_{N-1}}^j$) on the yields as a function of the estimated gains $G_{\beta_0, \dots, \beta_{N-1}}^j$. Then, one can compute the

upper bound on the phase error rate as follows:

$$\bar{Q}_Z^j = \frac{1}{\Pr(\Omega_j | R_{\text{KG}})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0 + \dots + n_{N-1} \leq \bar{n}} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \sqrt{\bar{Y}_{n_0, \dots, n_{N-1}}} + \Delta_{v, \bar{n}} \right)^2, \quad (7)$$

where \bar{n} is a positive even number, while the set \mathcal{V} , the coefficients $c_{i,n_i}^{(v_i)}$ and the quantity $\Delta_{v, \bar{n}}$ are defined as follows:

$$\mathcal{V} = \{v \in \{0, 2^N - 1\} : |\bar{v}| \bmod 2 = 0\}, \quad (8)$$

$$c_{i,n}^{(l)} = \begin{cases} e^{-\alpha_i^2/2} \frac{\alpha_i^n}{\sqrt{n!}} & \text{if } n+l \text{ is even} \\ 0 & \text{if } n+l \text{ is odd} \end{cases} \quad (9)$$

$$\Delta_{v, \bar{n}} = \sum_{n_0 + \dots + n_{N-1} \geq \bar{n} + 2} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)}. \quad (10)$$

The full derivation of the upper bound (7) on the phase error rate is provided Sec. III.

We remark that the protocol presented here uses the correlations of postselected W -like states to obtain a secret conference key. In Appendix B we clarify the connection between the correlations generated in the CKA protocol and the W state. Moreover, we note that, for two parties ($N = 2$), our protocol reduces to the TFQKD protocol introduced in Ref. [17] (see Appendix A).

III. SECURITY PROOF

Here we prove the security of the CKA protocol presented in Sec. II under the assumption of collective attacks.

Theorem 1.—The CKA protocol (Protocol II), under collective attacks by the eavesdropper and in the asymptotic limit, generates a conference key with rate r , given by Eq. (2).

Proof.—In the asymptotic limit and under collective attacks, the achievable conference key rate r of a CKA protocol with one-way reconciliation is lower bounded by the following [9]:

$$r \geq H(X_0|E) - \max_{i \geq 1} H(X_0|X_i), \quad (11)$$

where $H(X_0|E)$ ($H(X_0|X_i)$) is the von Neumann (Shannon) entropy of the KG outcome of reference party A_0 , conditioned on the eavesdropper's total side information (party A_i 's KG outcome), and it is evaluated on the state shared by the parties in a KG round. Note that the probability of a KG round is set to one in Eq. (11), since, asymptotically, the fraction of PE rounds becomes negligible.

In the case of our protocol, we postselect the KG rounds where event Ω_j occurred and discard all the other rounds. And for each event Ω_j , we independently extract a conference key. Hence, the asymptotic conference key rate of the whole protocol is bounded by

$$r \geq \sum_{j=0}^{M-1} \Pr(\Omega_j | R_{\text{KG}}) \left[H(X_0|E)_{\Omega_j} - \max_{i \geq 1} H(X_0|X_i)_{\Omega_j} \right], \quad (12)$$

where the entropies are computed on the state shared by the parties in a KG round, conditioned on event Ω_j .

Recall that, in an honest implementation, Ω_j corresponds to the event where only detector D_j clicks. Although our proof holds regardless of the physical details associated to the event Ω_j , in the following we often refer to Ω_j in terms of detector clicks for concreteness.

The second term in Eq. (12) is the conditional Shannon entropy between the KG outcomes of parties A_0 and A_i , when only detector D_j clicked. Thus, it can be readily bounded through Fano's inequality with the corresponding QBER in Eq. (4) as follows:

$$H(X_0|X_i)_{\Omega_j} \leq h(Q_{X_0, X_i}^j). \quad (13)$$

In order to lower bound the first conditional entropy in Eq. (12), we employ the entropic uncertainty relation [43]. To apply the uncertainty relation, we need to view the outcome X_0 corresponding to the coherent state prepared by party A_0 as the result of a fictitious measurement. To this aim, we consider an equivalent formulation of the protocol where each party, in a KG round, first prepares the following entangled state between their optical mode a_i and a virtual qubit Q_i :

$$|\psi_i\rangle_{Q_i a_i} = \frac{1}{\sqrt{2}} (|+\rangle_{Q_i} |\alpha_i\rangle_{a_i} + |-\rangle_{Q_i} |-\alpha_i\rangle_{a_i}), \quad (14)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and then measures their qubit in the X basis. Note that, from the eavesdropper's point of view, the fictitious protocol is completely equivalent to the actual protocol, even in the case that the parties delay their X -basis measurement until after the relay's announcement. This allows us to consider the state of the N qubits and optical modes, conditioned on detector D_j clicking in a KG round, prior to the X -basis measurements. The state reads

$$|X_j\rangle_{Q_0 Q_1 \dots Q_{N-1} E} := \frac{\hat{K}_j \left(\bigotimes_{i=0}^{N-1} |\psi_i\rangle_{Q_i a_i} \right)}{\sqrt{\Pr(\Omega_j | R_{\text{KG}})}}, \quad (15)$$

where \hat{K}_j is the Kraus operator [44] that models the action of the untrusted relay, i.e., the eavesdropper, when

it announces the event Ω_j . The operator \hat{K}_j acts between the Fock space of optical modes $a_0 \dots a_{N-1}$ and a generic Hilbert space \mathcal{H}_E , i.e., $\hat{K}_j : \mathcal{H}_{a_0} \otimes \dots \otimes \mathcal{H}_{a_{N-1}} \rightarrow \mathcal{H}_E$.

We remark that, due to the assumption of collective attacks, the operator \hat{K}_j remains the same in every KG and PE round. Nevertheless, due to the partial distinguishability of the states prepared in KG and PE rounds, \hat{K}_j could model the attempt to guess the type of round followed by an operation, which is specific to KG and PE rounds. This implies that, in general, $\Pr(\Omega_j | R_{\text{KG}}) \neq \Pr(\Omega_j | R_{\text{PE}})$.

With the pure state in Eq. (15), we can apply the entropic uncertainty relation by considering the hypothetical scenario where party A_0 performs either an X -basis or a Z -basis measurement on their qubit. We thus obtain the following lower bound on the first entropy in Eq. (12):

$$H(X_0|E)_{\Omega_j} \geq 1 - H(Z_0|Q_1 \dots Q_{N-1})_{\Omega_j}, \quad (16)$$

where both conditional entropies are computed on the state (15). We then derive an upper bound on the entropy on the right-hand side of Eq. (16) by using the fact that quantum maps on the conditioning systems can only increase the entropy [45]:

$$\begin{aligned} H(Z_0|Q_1 \dots Q_{N-1})_{\Omega_j} &\leq H(Z_0|\prod_{i=1}^{N-1} Z_i)_{\Omega_j} \\ &\leq h(Q_Z^j). \end{aligned} \quad (17)$$

In the second line, we use Fano's inequality and the definition of phase error rate:

$$Q_Z^j = \Pr(\prod_{i=0}^{N-1} Z_i = 1 | \Omega_j, R_{\text{KG}}), \quad (18)$$

which expresses the probability that, in the hypothetical scenario where each party measures in the Z basis their virtual qubit, the product of the outcomes is one. By employing Eqs. (13) and (17) in Eq. (12), we obtain the following expression for the asymptotic conference key rate of our CKA protocol:

$$r \geq \sum_{j=0}^{M-1} \Pr(\Omega_j | R_{\text{KG}}) \left[1 - h(Q_Z^j) - \max_{i \geq 1} h(Q_{X_0 X_i}^j) \right]. \quad (19)$$

To complete the security proof, we still need to bound the phase error rate (Q_Z^j) with the statistics collected by the parties in the PE rounds. The derivation of the bound is inspired by the security proof in Ref. [17] for a bipartite TFQKD protocol.

By definition (18), the phase error rate is the probability that an even number of parties obtains -1 as the outcome of their Z -basis measurement, in the hypothetical scenario in which all parties measured their virtual qubit in the Z

basis in a KG round and detector D_j clicks. Through the N -qubit state (15), which describes the state of the virtual qubits in a KG round conditioned on the click of detector D_j , we are able to express the phase error rate as follows:

$$Q_Z^j = \sum_{v \in \mathcal{V}} \left\| \langle \vec{v} |_{Q_0 \dots Q_{N-1}} | \chi_j \rangle \right\|^2, \quad (20)$$

where the set \mathcal{V} is defined in Eq. (8), i.e., the set of binary strings with parity zero. In order to bound the expression in Eq. (20), we observe that, for $l = 0, 1$, we have $Q_i \langle l | \psi_i \rangle_{Q_i a_i} = |C_i^{(l)}\rangle_{a_i}$, where $|C_i^{(l)}\rangle_{a_i}$ are unnormalized ‘‘cat states’’:

$$|C_i^{(l)}\rangle_{a_i} = \frac{|\alpha_i\rangle + (-1)^l |-\alpha_i\rangle}{2} = \sum_{n=0}^{\infty} c_{i,n}^{(l)} |n\rangle_{a_i}, \quad (21)$$

with $c_{i,n}^{(l)}$ defined in Eq. (9). By employing the states in Eq. (21), we can derive an upper bound on each term in the sum of Eq. (20) as follows:

$$\begin{aligned} \Pr(\Omega_j | R_{\text{KG}}) \left\| \langle \vec{v} |_{Q_0 \dots Q_{N-1}} | \chi_j \rangle \right\|^2 &= \left\| \hat{K}_j \bigotimes_{i=0}^{N-1} |C_i^{(v_i)}\rangle_{a_i} \right\|^2 \\ &= \left\| \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \hat{K}_j \bigotimes_{i=0}^{N-1} c_{i,n_i}^{(v_i)} |n_i\rangle \right\|^2 \\ &\leq \left(\sum_{n_0, \dots, n_{N-1}=0}^{\infty} \left\| \hat{K}_j \bigotimes_{i=0}^{N-1} c_{i,n_i}^{(v_i)} |n_i\rangle \right\| \right)^2 \\ &= \left(\sum_{n_0, \dots, n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \sqrt{Y_{n_0, \dots, n_{N-1}}^j} \right)^2, \end{aligned} \quad (22)$$

where we use the fact that \hat{K}_j acts only on the optical systems in the first equality and the triangle inequality in the third line. Moreover, we identified

$$\begin{aligned} \left\| \hat{K}_j |n_0\rangle_{a_0} \dots |n_{N-1}\rangle_{a_{N-1}} \right\|^2 &= \Pr(\Omega_j | n_0, \dots, n_{N-1}) \\ &=: Y_{n_0, \dots, n_{N-1}}^j, \end{aligned} \quad (23)$$

as the yields. We derive an upper bound on the phase error rate by employing the inequality (22) in Eq. (20). We

obtain

$$\mathcal{Q}_Z^j \leq \bar{\mathcal{Q}}_Z^j = \frac{1}{\Pr(\Omega_j | R_{\text{KG}})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0, \dots, n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} c_{i, n_i}^{(v_i)} \sqrt{Y_{n_0, \dots, n_{N-1}}^j} \right)^2, \quad (24)$$

where the set \mathcal{V} is given in Eq. (8) and the coefficients $c_{i, n_i}^{(v_i)}$ are given in Eq. (9).

The bound in Eq. (24) is not yet sufficient to obtain a computable lower bound on the key rate (19) of our CKA protocol, i.e., an expression that can be evaluated from the observed statistics. Indeed, the yields in Eq. (24) are not directly observed and must be estimated through a multipartite decoy-state method.

From the detection statistics of PE rounds, the parties can estimate the gains. By recalling that, under the assumption of collective attacks, the Kraus operator \hat{K}_j corresponding to the event Ω_j is the same in every round, we can express the gains as follows:

$$\begin{aligned} G_{\beta_0, \dots, \beta_{N-1}}^j &= \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \text{Tr} \left[\hat{K}_j \bigotimes_{i=0}^{N-1} e^{-\beta_i} \frac{\beta_i^{n_i}}{n_i!} |n_i\rangle \langle n_i| \hat{K}_j^\dagger \right] \\ &= \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} P_{\beta_i}(n_i) \text{Tr} \left[\hat{K}_j \bigotimes_{i=0}^{N-1} |n_i\rangle \langle n_i| \hat{K}_j^\dagger \right] \\ &= \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} P_{\beta_i}(n_i) Y_{n_0, \dots, n_{N-1}}^j, \end{aligned} \quad (25)$$

where we use Eq. (23) in the last equality and defined the Poisson distribution $P_\lambda(n) = e^{-\lambda} \lambda^n / n!$. The last expression links the observed gains to the yields and forms the basis of our multipartite decoy-state method, which we detail in Sec. IV. Our method allows us to obtain analytical upper bounds $\bar{Y}_{n_0, \dots, n_{N-1}}^j$ on any yield.

Although our method is general and works for any choice of photon numbers n_0, \dots, n_{N-1} , in practice it is not necessary to bound every yield appearing in Eq. (24) with a nontrivial upper bound. This is because the product of the coefficients defined in Eq. (9) satisfies

$$\prod_{i=0}^{N-1} c_{i, n_i}^{(v_i)} \neq 0 \iff n_{\text{tot}} := \sum_{i=0}^{N-1} n_i \text{ is even.} \quad (26)$$

Therefore, the only yields contributing to the phase error rate upper bound in Eq. (24) are those with $n_{\text{tot}} = 0, 2, 4, \dots$ and so on. Moreover, the product of the coefficients rapidly decreases with n_{tot} , implying that it is

sufficient to nontrivially bound only the yields corresponding to the first few values of n_{tot} , while the rest of the yields can be bounded by one.

With the yields' bounds, we can further bound the quantity in Eq. (24) and obtain the following upper bound on the phase error rate:

$$\mathcal{Q}_Z^j \leq \bar{\mathcal{Q}}_Z^j = \frac{1}{\Pr(\Omega_j | R_{\text{KG}})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0 + \dots + n_{N-1} \leq \bar{n}} \prod_{i=0}^{N-1} c_{i, n_i}^{(v_i)} \sqrt{Y_{n_0, \dots, n_{N-1}}^j + \Delta_{v, \bar{n}}} \right)^2, \quad (27)$$

where $\bar{Y}_{n_0, \dots, n_{N-1}}^j$ are the nontrivial bounds derived in Sec. IV and $\Delta_{v, \bar{n}}$ is the residual term obtained by bounding by one all the remaining yields. We have

$$\Delta_{v, \bar{n}} = \sum_{n_0 + \dots + n_{N-1} \geq \bar{n} + 2} \prod_{i=0}^{N-1} c_{i, n_i}^{(v_i)}, \quad (28)$$

where \bar{n} is an even number.

By employing Eq. (27) in Eq. (19), we recover the computable lower bound on the conference key rate in Eq. (2). This concludes the security proof. \blacksquare

As a final remark, we stress that the assumption on collective attacks, i.e., the operator \hat{K}_j being constant in every round, is instrumental in our proof. Extending the security proof to coherent attacks would mean that \hat{K}_j could not only guess the type of the current round, but also depend on the sequence of previous guesses, thus not remaining constant throughout the protocol run. The security of our protocol under coherent attacks could be proved by adapting the technique in Ref. [46]. Indeed, in Ref. [46] the authors perform a full finite-key analysis against coherent attacks for the TFQKD protocol in Ref. [17], which is recovered by our protocol when $N = 2$. We conjecture that the asymptotic key rate of our protocol would not be affected by coherent attacks, as suggested by taking the asymptotic limit of the finite key rate in Ref. [46] and realizing that it coincides with our asymptotic key rate, Eq. (2), when $N = 2$.

IV. MULTIPARTITE DECOY-STATE METHOD

In this section we present a technique that generalizes the decoy-state method to the multipartite scenario and provides an analytical upper bound on any yield $Y_{n_0, \dots, n_{N-1}}^j$, when an arbitrary number of parties N use the same set of two decoy intensities: $\mathcal{S} = \{\beta_0, \beta_1\}$.

The starting point of the multipartite decoy-state method is the equation that relates the observed gains with the

yields, Eq. (25), which we report here for clarity:

$$G_{\vec{f}}^j = \sum_{n_0, \dots, n_{N-1}=0}^{\infty} Y_{n_0, \dots, n_{N-1}}^j \prod_{i=0}^{N-1} \frac{e^{-\beta_{f_i}} \beta_{f_i}^{n_i}}{n_i!}, \quad (29)$$

where we introduce the binary vector \vec{f} that fixes the choice of intensity to β_{f_i} for party A_i .

Of note, the yields are independent of \vec{f} , i.e., of the selected intensities. Thus, Eq. (29) can be interpreted as a system of 2^N linear equations, each one labeled by \vec{f} , where the yields are the unknowns. By performing appropriate linear combinations of the system of equations, one can derive equalities where only a subset of yields survive, thus reducing the number of unknowns. However, the number of unknowns is infinite, implying that such a technique cannot generate the exact solution for each yield. Nevertheless, from the linear combinations presenting a reduced number of yields, one can still obtain nontrivial upper bounds.

For concreteness, consider the following toy example of an equality linking a function B of the observed statistics to a (possibly infinite) subset of yields, Y and Y_i ,

$$B = cY + \sum_i c_i Y_i, \quad (30)$$

where c and c_i are real coefficients. Suppose that our goal is to derive an upper bound on the yield Y . To do so, we first split the sum of the other yields in two sums, one in which the coefficients c_i have the same sign as c and another where they have opposite sign. By labeling $s_i := \text{sign}(c_i)$ (s) the sign of coefficient c_i (c), we have

$$B = cY + \sum_{i:s_i=s} c_i Y_i + \sum_{i:s_i \neq s} c_i Y_i. \quad (31)$$

Now, by multiplying both sides by s and isolating Y , we get

$$Y|c| = sB - \sum_{i:s_i=s} |c_i| Y_i + \sum_{i:s_i \neq s} |c_i| Y_i. \quad (32)$$

Then, it is straightforward to obtain an upper bound on Y by minimizing the yields Y_i whose coefficients have the same sign as the coefficient of Y ($s_i = s$) and by maximizing the other yields ($s_i \neq s$). In the case we do not have nontrivial bounds on the yields Y_i , we simply set the former to zero and the latter to one. In many cases, the described procedure can lead to a nontrivial bound on Y :

$$Y \leq \min \left\{ B/c + \sum_{i:s_i \neq s} |c_i/c|, 1 \right\}, \quad (33)$$

where the minimum is taken to ensure that the bound is never greater than 1.

In Appendix C, we apply this method on the system in Eq. (29) and obtain a nontrivial upper bound on the generic yield $Y_{n_0, \dots, n_{N-1}}^j$, given by

$$\begin{aligned} \bar{Y}_{n_0, \dots, n_{N-1}}^j &= \min\{U_{n_0, \dots, n_{N-1}}^j, 1\}, \\ U_{n_0, \dots, n_{N-1}}^j &= \prod_{\substack{i \text{ s.t.} \\ n_i \neq 0}} \frac{n_i!}{\beta_0^{n_i} - \beta_1^{n_i}} \left[\frac{B_{\vec{h}}^j (-1)^{N-m}}{(\beta_0 - \beta_1)^{N-m}} \right. \\ &\quad \left. + (e^{\beta_0} - e^{\beta_1})^m \sum_{k=0}^{\lfloor (N-m-1)/2 \rfloor} \binom{N-m}{2k+1} \right. \\ &\quad \left. \times \left(\frac{\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1}{\beta_0 - \beta_1} \right)^{2k+1} \right], \quad (34) \end{aligned}$$

where \vec{h} is the binary vector with components:

$$h_i = \begin{cases} 1 & \text{if } n_i \geq 1 \\ 0 & \text{if } n_i = 0, \end{cases} \quad (35)$$

while $m = |\vec{h}|$, $\lfloor x \rfloor$ is the floor function, and $B_{\vec{h}}^j$ is given by

$$B_{\vec{h}}^j = \sum_{\vec{f}=0}^{2^N-1} (-1)^{|\vec{f}|} \beta_0^{(\vec{1}-\vec{h}) \cdot \vec{f}} \beta_1^{(\vec{1}-\vec{h}) \cdot (\vec{1}-\vec{f})} \frac{G_{\vec{f}}^j}{\prod_{i=0}^{N-1} e^{-\beta_{f_i}}}. \quad (36)$$

As a final remark, our analytical technique can be generalized to scenarios with different and more intensities for each party. Besides, we point out that the calculation of the yields' bounds required by the phase error rate bound in Eq. (7) can also be done numerically by using linear programming techniques [16].

V. SIMULATIONS

In order to assess the performance of our protocol, we simulate its key rate (2) under a channel model that includes different sources of noise. First, we model the losses between each party and the detectors at the relay with the same pure-loss channel with transmittance η . We also account for a polarization and phase misalignment of 2% between the reference party A_0 and each other party. Moreover, we account for dark counts in the detectors by computing the key rates considering different dark-count probabilities, namely, 10^{-8} , 10^{-9} , and 10^{-10} . In Appendix D we describe the channel model in detail and provide the calculations of the protocol's statistics under such model.

In our symmetric channel model each party experiences the same loss. Thus, the optimal signal intensities are independent of the party, implying that we can set $\alpha_i = \alpha$ and $\mathcal{S}_i = \mathcal{S}$ for every i , without losing in performance. Under these conditions, we analytically verify (see Appendix D)

that the detection statistics, i.e., $\Pr(\Omega_j|x_0, x_i, R_{\text{KG}})$ and $\Pr(\Omega_j|\beta_0, \dots, \beta_{N-1})$, are independent of which detector clicks (j) and of the party (i).

This readily implies that the QBER in Eq. (5) is independent of the party and of the detector and we can indicate it as $Q'_{x_0, x_i} = Q_X$. Similarly, the analytical upper bounds on the yields presented in Sec. IV are independent of j since the gains are independent of j . We employ our yields bounds, Eq. (34), in the calculation of the bound \bar{Q}_Z on the phase error rate (7), where we choose $\bar{n} = 4$ as the cutoff number above which every yield is trivially bounded by one. The choice is motivated by the fact that, for $\bar{n} = 4$, the residual term $\Delta_{v, \bar{n}}$ in Eq. (10) becomes negligible.

By considering the discussed symmetries, the asymptotic conference key rate of our simulations simplifies to

$$r \geq M \Pr(\Omega|R_{\text{KG}}) [1 - h(\bar{Q}_Z) - h(Q_X)], \quad (37)$$

where $\Pr(\Omega|R_{\text{KG}})$ is the probability that a fixed detector clicks in a KG round and $M \geq N$ is the number of detectors in the relay.

In order to benchmark the performance of our protocol, we follow the approach used for TFQKD schemes. Typically, the key rate of a TFQKD protocol is benchmarked against the repeaterless bound [20], i.e., the bound on the private capacity between Alice and Bob when the relay between the two parties is removed. If the TFQKD rate surpasses the repeaterless bound, this indicates that adding an untrusted relay enables higher secret key rates and proves the usefulness of the TFQKD protocol. Similarly, in our multipartite setting we compare the conference key rate of our protocol with the ultimate conference key rate that could be achieved in the quantum network without the relay. This is the single-message multicast bound of the quantum network [42] and it depends on the network architecture. In our scenario, there are at least two network configurations (star network and fully connected network) that can arise when removing the relay, which we depict in Fig. 3.

In the star network (left configuration in Fig. 3), there is a pure-loss bosonic channel with transmittance η^2 between

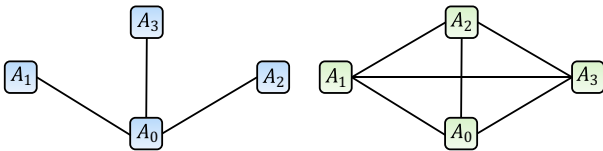


FIG. 3. Two possible network configurations that arise when the relay is removed, for $N = 4$ parties. In the left configuration, there is a bipartite link between A_0 and each other party (star network). In the right configuration, each party is connected with each other (fully connected network). The transmittance of the channel connecting any two parties is η^2 .

party A_0 and each other party A_i (for $i = 1, \dots, N - 1$). In this case, the single-message multicast bound is independent of the number of parties N and coincides with the bipartite repeaterless bound [20] used to benchmark TFQKD protocols:

$$r \leq -\log_2(1 - \eta^2) =: R_1. \quad (38)$$

In the right configuration of Fig. 3, the resulting network is fully connected, such that each party is linked to each other with the same pure-loss bosonic channel with transmittance η^2 . In this case, the single-message multicast bound reads [42]

$$r \leq -(N - 1) \log_2(1 - \eta^2) =: R_2(N). \quad (39)$$

In this network configuration the single-message multicast bound increases with the number of parties, N . This could be explained by the quadratic scaling of the number of bipartite links with N , compared to the linear scaling of the star network. It is worthwhile to emphasize that, in order to obtain the network configurations of Fig. 3 when removing the relay, additional pure-loss channels need to be added on top of the existing channels used by our protocol. For instance, the star network can be seen as the result of a combination of six channels with transmittance η : three channels connect A_0 to the point where the relay was located and are subsequently linked to the three channels connecting to parties A_1 , A_2 , and A_3 . While our CKA protocol requires only four such channels (from the relay to each of the parties) when $N = 4$. This contrasts with the benchmarking of bipartite TFQKD against the repeaterless bound, where the relay is removed and the two original channels are linked together without the need to add further channels. Therefore, when comparing the multicast bounds (38) and (39) with the CKA rate of our protocol, one should consider that the multicast bounds can only be attained if additional channels are used.

In Fig. 4, we plot the key rate (37) of our protocol for $N = 3$, $N = 4$, and $N = 5$ parties (for every N , we fix the number of inputs M in the BBS network to the smallest power of two such that $M \geq N$), together with the multicast bounds, Eqs. (38) and (39). In Fig. 4(a), we compute the phase error rate bound in Eq. (7) with our analytical upper bounds on the yields (34) obtained with two decoy intensities fixed to $\beta_0 = 0.5$ and $\beta_1 = 0$, respectively. In Fig. 4(b), instead, we assume that the relevant yields in the phase error rate bound (7) are known and use their exact analytical expression (D74) (see Appendix D for the calculation). This corresponds to the limit where the parties have an infinite number of decoy intensities and can estimate the yields exactly. In both plots, we optimize the key rate at each level of loss over the signal amplitude α . Further details on the numerical simulations and on the optimal values for α are reported in Appendix E.

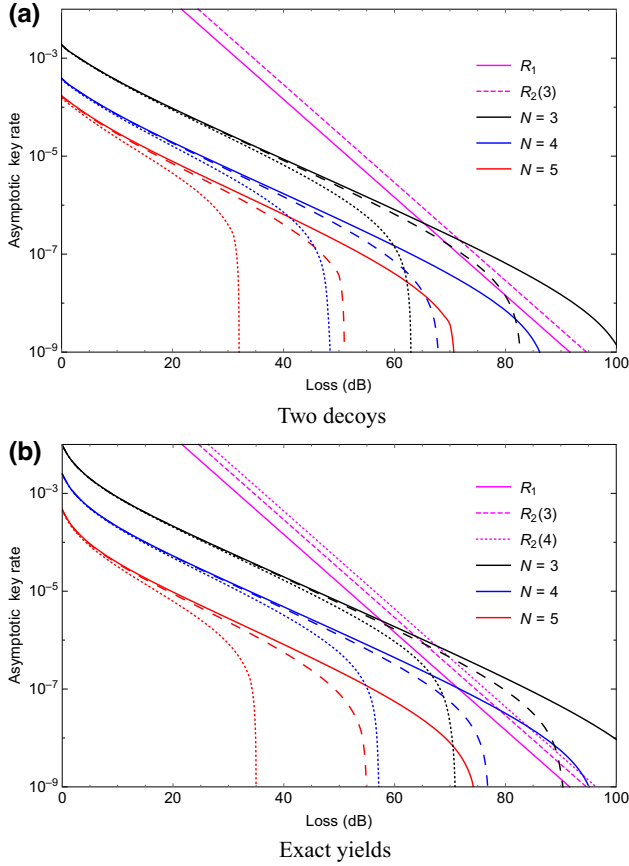


FIG. 4. Asymptotic conference key rate of our protocol [Eq. (37)] as a function of the loss (in dB) between any two parties, when (a) each party uses two decoy intensities; (b) the parties can perfectly estimate the yields. We plot the key rate for different dark-count probabilities: $p_d = 10^{-10}$ (solid lines), $p_d = 10^{-9}$ (dashed lines), and $p_d = 10^{-8}$ (dotted lines) and a different number of parties N , while we fix the polarization and phase misalignment to 2%. We report the single-message multicast bound R_1 [Eq. (38), solid magenta line] for the star network and the bounds $R_2(3)$ and $R_2(4)$ [Eq. (39), dashed and dotted magenta line] for the fully connected network. (a) For sufficiently high loss, our protocol with two decoys can overcome the multicast bounds for both configurations when $N = 3$. (b) A tighter estimation of the yields (e.g., by adding decoy intensities) would allow our protocol to overcome both multicast bounds for $N = 3$ and $N = 4$.

From Fig. 4(a) we observe that our protocol, already with two decoy intensities per party, is capable of overcoming both the single-message multicast bounds R_1 and R_2 , for three parties and in the high-loss regime. This is explained by the fact that our protocol relies on single-photon interference events, regardless of the number of parties, hence its key rate scales with the transmittance between one party and the relay: $r \sim \eta$. Conversely, the multicast bounds in Eqs. (38) and (39) for a quantum network without a relay cannot scale better than $r \sim \eta^2$.

However, as the number of parties increases, the key rate of our protocol drops due to the unavoidable QBER inherited from W -state correlations and cannot beat the multicast bounds. This can be mitigated by increasing the number of decoy intensities per party, as suggested by Fig. 4(b) that represents the best-case scenario of infinite decoys. Indeed, we observe a significant improvement of the key rate, especially in the high-loss regime, allowing it to overcome the multicast bounds R_1 and R_2 for three and four parties. The advantage provided by our protocol could extend beyond four parties when compared to more realistic multicast bounds that account for additional noise on top of pure loss (for example, the noise model used in the simulations), as well as tighter multicast bounds (the multicast bounds used in our comparison are not proven to be tight and might be quite loose [42]).

The improvement of the key rate in the high-loss regime occurs because adding decoy intensities to the multipartite decoy-state method allows for tighter yields' bounds when evaluating the phase error rate through (7). As a consequence, the optimal value of the signal intensity (α^2) can increase without severely affecting the phase error rate bound, as shown in Appendix E. In turn, higher signal intensities increase the probability that exactly one detector clicks (up to the limit where multiple-photon contributions become dominant), thus increasing the key rate. The gain in the key rate is particularly visible in the high-loss regime, where the effect of dark counts on the detector clicks is comparable to the arrival of a signal.

In parallel, the key rate computed with the exact yields [Fig. 4(b)] is higher than the one computed with two decoys [Fig. 4(a)] even in the low-loss regime. This is due to the fact that the latter is not optimized over the decoy intensities. In particular, the value of $\beta_0 = 0.5$ is chosen such that it is close-to-optimal only for high losses, thus explaining the suboptimal behavior of the key rate with two decoys at low losses.

VI. CONCLUSION

We design a practical, measurement-device-independent, conference key agreement protocol that delivers a shared conference key to an arbitrary number of parties. In the protocol, each party only has to transmit coherent pulses to an untrusted relay, which interferes the pulses in a network of balanced beam splitters and performs threshold measurements. Our protocol harnesses single-photon interference at the relay in order to establish a common key. This can be understood by realizing that the correlations postselected by our protocol correspond to the correlations of a W state, which can indeed generate conference keys [9].

We prove the security of our protocol against collective attacks and derive an analytical expression for the asymptotic key rate, by combining the entropic uncertainty

relation [43] with an developed multipartite decoy-state analysis. We emphasize that our protocol and its security proof are general and can account for scenarios with arbitrary asymmetric losses. Moreover, we provide extended numerical simulations with a realistic channel model that accounts for phase and polarization misalignment, photon loss, and dark counts in the detectors. We show that our protocol is capable, in certain regimes, of overcoming the ultimate conference key rates achievable in a quantum network without a relay, by comparing it to single-message multicast bounds [42].

A notable byproduct of our work is the derivation of analytical upper bounds on the yields of any combination of Fock states sent by the parties, which may find application in other multipartite protocols where yields need to be estimated. Our analytical bounds on the yields are the first bounds derived for an arbitrary number of parties.

At the same time, our protocol represents the first example of a CKA protocol that can beat single-message multicast bounds in quantum networks [42]. This heralds a key step for long-distance CKA, similarly to how the introduction of TFQKD [15] allowed QKD to reach much longer distances by beating the repeaterless bound [20]. Indeed, our results show that adding an untrusted relay, with a relatively simple optical setup, in a quantum network, can increase the rate at which the network users establish conference keys over long distances. In particular, the scaling improvement in the key rate (the key rate scales with η instead of η^2) matches the one that could be achieved by future quantum repeaters.

In addition, our protocol is readily implementable with current technology as it does not add further experimental requirements compared to state-of-the-art experiments on TFQKD protocols [23–33]. As a matter of fact, for two parties our CKA scheme reduces to the bipartite TFQKD protocol in Ref. [17], which has already been implemented in several experiments [23,25,28,31]. In such experiments, phase-tracking and phase-locking techniques are required in order to ensure that the parties' signals remain in phase. This, however, might become more challenging when more parties are involved. A solution could be found by multiplexing in time and/or frequency as shown in Refs. [47,48]. We remark that the implementation of our CKA protocol would represent the first instance of a multipartite conference key agreement, which does not rely on GHZ-type states.

The work presented in this paper can be further developed along different lines of research. From a security perspective, a complete finite-key analysis along the lines of the proof given in Ref. [46] for bipartite TFQKD is required, in order to prove the protocol secure in the presence of statistical fluctuations and coherent attacks.

Moreover, our decoy-state analysis assumes a highly symmetrical configuration where every party uses the same set of decoy intensities, which is optimal in the scenario

of symmetric channel losses analyzed in this work. However, real-life scenarios would likely display asymmetric channel losses, which require a more general decoy analysis with independent decoy intensities for each party, as shown for the bipartite case in Ref. [49]. On a similar note, our decoy analysis employs only two decoy settings per party, which is not sufficient to achieve close-to-optimal key rates (i.e., key rates obtained with infinite decoy settings), as shown by Fig. 4. Hence, it is likely that using more than two decoy settings to derive numerical or analytical bounds on the yields appearing in the phase error rate could improve the resulting key rate.

Finally, the efficiency of the protocol at lower losses could be improved by retaining those rounds where more than one detector clicks and using them to extract extra conference key bits. The security proof presented in this work could be naturally extended to make use of such rounds.

To conclude, we believe that our work constitutes a significant step towards increasing the practicality of multipartite cryptographic protocols and their applicability in high-loss regimes.

ACKNOWLEDGMENTS

We thank Álvaro Navarrete for insightful discussions and Hermann Kampermann and Dagmar Bruß for their useful comments. 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. F.G. acknowledges support by the DFG Individual Research Grant BR2159/6-1.

Note added.—Recently, another CKA scheme has been posted on preprint servers [50], with our same goal of extending the communication distance of CKA. However, we believe that the protocol in Ref. [50] is much more technologically demanding than ours. For the legitimate users, the protocol in Ref. [50] requires the parallel generation of multiple one-photon pulses from each party, compared to only a phase randomized weak coherent pulse in our protocol. For the measuring station, the protocol in Ref. [50] requires a quantum nondemolition measurement that heralds the arrival of a photon, followed by a GHZ-state analyzer acting on the heralded signals, while in our protocol we require only an interferometric measurement as depicted in Fig. 2.

CODE AVAILABILITY

The code used to run the simulations can be made available upon request to the authors.

APPENDIX A: THE BALANCED BEAM-SPLITTER NETWORK

In this Appendix, we provide a complete description of the BBS network that describes the honest implementation of the untrusted relay. The network is composed of s layers, labeled by $r = 0, \dots, s-1$, and each layer receives as input $M = 2^s$ optical modes $\hat{a}_i^{(r)}$, for $0 \leq i \leq M-1$. Note that for $r = 0$ the modes correspond to the modes arriving at the relay from the parties.

In a generic layer r , the optical mode $\hat{a}_i^{(r)}$ is mixed with the mode $\hat{a}_{i+2^r}^{(r)}$ in a BBS, for all modes $\hat{a}_i \in F_r$. The set F_r for layer r contains the modes:

$$F_r := \bigcup_{k=0}^{2^{s-r-1}-1} \{\hat{a}_{k2^{r+1}}, \hat{a}_{k2^{r+1}+1}, \dots, \hat{a}_{k2^{r+1}+2^r-1}\}. \quad (\text{A1})$$

For example, F_0 contains the even modes and F_1 contains modes 0, 1, 3, 4, and so on. This pattern repeats until the last layer, that contains the first half of the modes. Each layer contains $M/2$ beam splitters. Hence, the total number of beam splitters in the BBS network, in terms of the number of inputs M , is

$$n_{\text{BS}} = \frac{M}{2} \log_2 M. \quad (\text{A2})$$

We note that the BBS network, due to its structure, must be prepared for a number of inputs M equal to a power of 2 but can be used by any number of parties $N \leq M$. We also remark that, for $s = 1$, the BBS network reduces to a single beam splitter and coincides with the setup used in the TFQKD protocol of Ref. [17].

We are interested in the evolution of the creation operators in layer r through a BBS, which is given by

$$\begin{aligned} (\hat{a}_i^{(r)})^\dagger &\rightarrow \frac{1}{\sqrt{2}} [(\hat{a}_i^{(r+1)})^\dagger + (\hat{a}_{i+2^r}^{(r+1)})^\dagger] \quad \forall i \in F_r \\ (\hat{a}_j^{(r)})^\dagger &\rightarrow \frac{1}{\sqrt{2}} [(\hat{a}_{j-2^r}^{(r+1)})^\dagger - (\hat{a}_j^{(r+1)})^\dagger] \quad \forall j \in \bar{F}_r, \end{aligned} \quad (\text{A3})$$

where \bar{F}_r indicates the complement of F_r .

By going through all layers until $r = s-1$, we are able to transform each input mode in a balanced combination of all the output modes, whose coefficients are at most a minus sign. The global mode transformation, which includes the transformation of each layer, is given in the following theorem.

Theorem 2.—Given $M = 2^s$ input modes in the BBS network described above where, in each layer r , the modes

transform according to Eq. (A3). Then, the global evolution of the modes over all the s layers is given by

$$\hat{a}_i^\dagger \rightarrow \frac{1}{(\sqrt{2})^s} \sum_{k=0}^{2^s-1} f_{k,i}^{(s)} (\hat{a}_k^{(s)})^\dagger \quad \forall i = 0, \dots, 2^s - 1, \quad (\text{A4})$$

where the function $f_{k,i}^{(s)}$ is given by

$$f_{k,i}^{(s)} = \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor}, \quad (\text{A5})$$

and $\lfloor \cdot \rfloor$ is the floor function. Moreover, $f_{k,i}^{(s)}$ can be recast as follows:

$$f_{k,i}^{(s)} = (-1)^{\vec{k} \cdot \vec{i}}, \quad (\text{A6})$$

where \vec{k} and \vec{i} are the binary vectors of length s representing the integers k and i in binary representation.

Proof.—The theorem is proved by induction on s . Hence, the first step of the proof is to prove the result for $s = 1$, i.e., just two inputs. We thus have two optical modes \hat{a}_0^\dagger and \hat{a}_1^\dagger mixed in a BBS. The transformation of the modes is given in Eq. (A3), for $r = 0$, i.e.,

$$\begin{aligned} \hat{a}_0^\dagger &\rightarrow \frac{1}{\sqrt{2}} [(\hat{a}_0^{(1)})^\dagger + (\hat{a}_1^{(1)})^\dagger] \\ \hat{a}_1^\dagger &\rightarrow \frac{1}{\sqrt{2}} [(\hat{a}_0^{(1)})^\dagger - (\hat{a}_1^{(1)})^\dagger]. \end{aligned} \quad (\text{A7})$$

The formula provided in the theorem's statement, Eq. (A4), for $s = 1$ reads

$$\hat{a}_i \rightarrow \frac{1}{\sqrt{2}} \sum_{k=0}^1 (-1)^{ki} (\hat{a}_k^{(1)})^\dagger, \quad (\text{A8})$$

which is equivalent to the transformation of the modes of Eq. (A7). The theorem is thus proved for $s = 1$.

Now, in the inductive step we assume that the theorem's statement in Eq. (A4) is correct for generic s and show that it induces the same transformation for $s+1$, i.e., that the theorem holds for $s+1$.

We start by adding to the modes labeled by i another set of 2^s modes, labeled by $j = 2^s, \dots, 2^{s+1} - 1$, that undergoes the same kind of transformations, i.e.,

$$\hat{a}_j^\dagger \rightarrow \frac{1}{(\sqrt{2})^s} \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_k^{(s)})^\dagger \quad \forall j = 2^s, \dots, 2^{s+1} - 1. \quad (\text{A9})$$

We now follow the prescription in Eq. (A3) and combine the modes in the $s+1$ layer of the BBS network. This means that we combine the mode $(\hat{a}_i^{(s)})^\dagger$ with the corresponding mode $(\hat{a}_{i+2^s}^{(s)})^\dagger$, and obtain

$$\begin{aligned}
(\hat{a}_i^{(s)})^\dagger &\rightarrow \frac{1}{\sqrt{2}}[(\hat{a}_i^{(s+1)})^\dagger + (\hat{a}_{i+2^s}^{(s+1)})^\dagger] \quad \forall i = 0, \dots, 2^s - 1 \\
(\hat{a}_j^{(s)})^\dagger &\rightarrow \frac{1}{\sqrt{2}}[(\hat{a}_{j-2^s}^{(s+1)})^\dagger - (\hat{a}_j^{(s+1)})^\dagger] \quad \forall j = 2^s, \dots, 2^{s+1} - 1.
\end{aligned} \tag{A10}$$

We use the assumption in the inductive step. That is, we use Eqs. (A4) and (A9) to describe the transformations of the modes in the first s layers. We separately address the transformations on the first 2^s modes \hat{a}_i^\dagger , described by Eq. (A4), and the transformations on the other 2^s modes \hat{a}_j^\dagger , described by Eq. (A9).

1. For the modes \hat{a}_i^\dagger with $i = 0, \dots, 2^s - 1$, we employ the first equation in Eq. (A10) together with Eq. (A4). We obtain the following transformation of the modes after $s + 1$ layers:

$$\begin{aligned}
\hat{a}_i^\dagger &\rightarrow \frac{1}{(\sqrt{2})^s} \sum_{k=0}^{2^s-1} f_{k,i}^{(s)} \frac{1}{\sqrt{2}} [(\hat{a}_k^{(s+1)})^\dagger + (\hat{a}_{k+2^s}^{(s+1)})^\dagger] \\
&= \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,i}^{(s)} (\hat{a}_k^{(s+1)})^\dagger + \sum_{k=0}^{2^s-1} f_{k,i}^{(s)} (\hat{a}_{k+2^s}^{(s+1)})^\dagger \right)
\end{aligned} \tag{A11}$$

Now let us consider the coefficient $f_{k,i}^{(s+1)}$. By definition (A5), we have

$$\begin{aligned}
f_{k,i}^{(s+1)} &= \prod_{l=0}^s (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor} \\
&= (-1)^{\lfloor k/2^s \rfloor \lfloor i/2^s \rfloor} \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor} \\
&= (-1)^{\lfloor k/2^s \rfloor \lfloor i/2^s \rfloor} f_{k,i}^{(s)}.
\end{aligned} \tag{A12}$$

However, since $i = 0, \dots, 2^s - 1$ we have that $\lfloor i/2^s \rfloor = 0 \forall i$, which in turn implies

$$f_{k,i}^{(s+1)} = f_{k,i}^{(s)} \quad \forall i = 0, \dots, 2^s - 1, \forall k. \tag{A13}$$

We use this result in Eq. (A11) combined with a rescaling of the second sum with $k \rightarrow k - 2^s$ to write

$$\begin{aligned}
\hat{a}_i^\dagger &\rightarrow \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right. \\
&\quad \left. + \sum_{k=2^s}^{2^{s+1}-1} f_{k-2^s,i}^{(s)} (\hat{a}_k^{(s+1)})^\dagger \right),
\end{aligned} \tag{A14}$$

where

$$f_{k-2^s,i}^{(s)} = \prod_{l=0}^{s-1} (-1)^{\lfloor (k-2^s)/2^l \rfloor \lfloor i/2^l \rfloor} = \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l - 2^{s-l} \rfloor \lfloor i/2^l \rfloor}. \tag{A15}$$

Since $k \geq 2^s$ we have that $k/2^l \geq 2^{s-l}$. Moreover, $s > l$ for every l , which means that 2^{s-l} is a positive, even integer. We thus can write

$$\begin{aligned}
f_{k-2^s,i}^{(s)} &= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor - 2^{s-l} \lfloor i/2^l \rfloor} \\
&= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor} (-1)^{-2^{s-l} \lfloor i/2^l \rfloor} \\
&= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor} = f_{k,i}^{(s)} = f_{k,i}^{(s+1)},
\end{aligned} \tag{A16}$$

where $(-1)^{-2^{s-l} \lfloor i/2^l \rfloor} = 1 \forall i$ because 2^{s-l} is even for all l and where we use Eq. (A13) in the last equality. With the last expression, we can simplify (A14) as follows:

$$\begin{aligned}
\hat{a}_i^\dagger &\rightarrow \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right. \\
&\quad \left. + \sum_{k=2^s}^{2^{s+1}-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right) \\
&= \frac{1}{(\sqrt{2})^{s+1}} \sum_{k=0}^{2^{s+1}-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger,
\end{aligned} \tag{A17}$$

which concludes the proof for $i = 0, \dots, 2^s - 1$.

2. For the modes \hat{a}_j^\dagger , with $j = 2^s, \dots, 2^{s+1} - 1$, we combine the second equation in Eq. (A10) with the assumption (A9) and obtain

$$\hat{a}_j^\dagger \rightarrow \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_{k-2^s}^{(s+1)})^\dagger - \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_k^{(s+1)})^\dagger \right). \tag{A18}$$

Once again, we can rescale the first sum with $k \rightarrow k + 2^s$ in the last expression and obtain

$$\hat{a}_j^\dagger \rightarrow \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k+2^s,j}^{(s)} (\hat{a}_k^{(s+1)})^\dagger - \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_k^{(s+1)})^\dagger \right). \quad (\text{A19})$$

Since 2^{s-l} is a positive, even integer, we can simplify the coefficient in the first sum as follows:

$$\begin{aligned} f_{k+2^s,j}^{(s)} &= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor + 2^{s-l} \lfloor j/2^l \rfloor} \\ &= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor} (-1)^{2^{s-l} \lfloor j/2^l \rfloor} \\ &= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor} = f_{k,j}^{(s)}. \end{aligned} \quad (\text{A20})$$

Moreover, since $k = 0, \dots, 2^s - 1$, one has that $\lfloor k/2^s \rfloor = 0$ and hence that

$$\begin{aligned} f_{k,j}^{(s+1)} &= \prod_{l=0}^s (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor} \\ &= (-1)^{\lfloor k/2^s \rfloor \lfloor j/2^s \rfloor} \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor} \\ &= (-1)^{\lfloor k/2^s \rfloor \lfloor j/2^s \rfloor} f_{k,i}^{(s)} = f_{k,i}^{(s)}, \end{aligned} \quad (\text{A21})$$

which means that we can replace the coefficient $f_{k+2^s,j}^{(s)}$ in the first sum of Eq. (A19) with $f_{k,j}^{(s+1)}$. Regarding the second sum in Eq. (A19), we can write the coefficient as

$$(-1) f_{k,j}^{(s)} = (-1)^{g(k,j)} f_{k,j}^{(s)}, \quad (\text{A22})$$

where $g(k,j)$ is a function that is odd for $j, k = 2^s, \dots, 2^{s+1} - 1$. For instance, we can choose the function to be the following:

$$g(k,j) = \lfloor k/2^s \rfloor \lfloor j/2^s \rfloor. \quad (\text{A23})$$

Then, the coefficient of the second sum in Eq. (A19) becomes

$$(-1) f_{k,j}^{(s)} = (-1)^{\lfloor k/2^s \rfloor \lfloor j/2^s \rfloor} f_{k,j}^{(s)} \equiv f_{k,j}^{(s+1)}. \quad (\text{A24})$$

With the above expressions, we can recast Eq. (A19) as follows and conclude the proof for $j = 2^s, \dots, 2^{s+1} - 1$:

$$\begin{aligned} \hat{a}_j^\dagger &\rightarrow \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,j}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right. \\ &\quad \left. + \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right) \\ &= \frac{1}{(\sqrt{2})^{s+1}} \sum_{k=0}^{2^{s+1}-1} f_{k,j}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger. \end{aligned} \quad (\text{A25})$$

The combination of the two results in Eqs. (A17) and (A25) imply that the global transformation of the modes, for $M = 2^{s+1}$ inputs, is given by Eq. (A4) where s is replaced by $s + 1$. This proves the theorem for $s + 1$ and concludes the proof. \blacksquare

APPENDIX B: W -STATE CORRELATIONS

In this Appendix we present the logical steps that brought us to design the protocol presented in Sec. II and show the connection between the correlations generated by our protocol and the correlations of the W state [38].

We start by describing an Ideal protocol, i.e., a protocol that is less practical than the one presented in the main text but has the merit of elucidating the core ideas that lead to the CKA protocol of Sec. II. The protocol is run by N parties, which we call A_0, \dots, A_{N-1} , and consists of the following steps.

Protocol 2 (Ideal protocol)

1. Quantum part: repeat what follows for a sufficient amount of iterations.
 - 1.1. Every party holds an optical mode a_i and a qubit Q_i and prepares the following entangled state:

$$|\phi_i\rangle = \sqrt{q_i}|0\rangle_{Q_i}|0\rangle_{a_i} + \sqrt{1-q_i}|1\rangle_{Q_i}|1\rangle_{a_i}, \quad (\text{B1})$$

where $|0\rangle_{Q_i}$ and $|1\rangle_{Q_i}$ are two orthogonal states of the qubit, $|0\rangle_{a_i}$ and $|1\rangle_{a_i}$ are the vacuum and one-photon state of the optical mode, respectively, and $0 < q_i < 1$.

- 1.2. Every party sends their optical pulse through a noisy and lossy channel to an untrusted relay.
- 1.3. In the untrusted relay, the optical signals interfere in a BBS network of $M = 2^s$ inputs and M outputs, for some natural number s with $M \geq N$. The BBS network is described in Appendix A. The network transforms the input modes in a balanced combination of the output modes, i.e.,

$$\hat{a}_i^\dagger \rightarrow \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (-1)^{j \cdot i} \hat{a}_j^\dagger, \quad (\text{B2})$$

where \hat{a}_i^\dagger and \hat{d}_j^\dagger are the creation operators of the input and output modes, respectively, and \vec{j} and \vec{i} the binary representations of the integers j and i and $\vec{j} \cdot \vec{i}$ is their scalar product.

- 1.4. The untrusted relay measures each output mode d_j with a threshold detector D_j , for $j = 0, \dots, M-1$. The relay announces the detection pattern $\vec{k} \in \{0, 1\}^M$ for each detector, where $k_j = 1$ if detector D_j clicked and $k_j = 0$ otherwise. The round gets discarded unless only one detector clicked, i.e., if $|\vec{k}| = 1$, where $|\vec{x}|$ is the Hamming weight of vector \vec{x} .
- 1.5. Each party A_i measures their qubit Q_i . If the round is labeled as a PE round, each party measures in the Z basis and obtains an outcome $Z_i = \pm 1$. If the round is a KG round, each party measures in the X basis and obtains outcome $X_i = \pm 1$.

2. Parameter estimation: the parties partition their outcomes in M sets, where each set corresponds to the event Ω_j where only detector D_j clicks. For each partition, the parties reveal a fraction of their X -basis outcomes in order to compute the QBER, with respect to reference party A_0 . The QBER is defined as

$$Q_{X_0, X_i}^j = \Pr(X_0 \neq (-1)^{\vec{j} \cdot \vec{i}} X_i | \Omega_j, R_{KG}). \quad (\text{B3})$$

Similarly, for each partition of outcomes the parties reveal their Z -basis outcomes and evaluate the phase error rate, defined as follows:

$$Q_Z^j = \Pr\left(\prod_{i=0}^{N-1} Z_i = 1 | \Omega_j, R_{KG}\right). \quad (\text{B4})$$

3. Classical postprocessing: the parties extract a secret conference key from the remaining undisclosed X -basis outcomes. To do so, for each partition labeled by Ω_j , party A_i flips their X -basis outcomes when $(-1)^{\vec{j} \cdot \vec{i}} = -1$. The parties then perform error correction and privacy amplification.

We remark that the probabilities defining the QBER (B3) and the phase error rate (B4) are conditioned on the event that only detector D_j clicked and the round was chosen to be a KG round. While the QBER can be directly computed from the outcomes collected in KG rounds, the phase error rate refers to the hypothetical scenario where the parties measured in the Z basis in a KG round. However, since the only difference between KG and PE rounds is the local qubit measurement, the choice of the type of round can be delayed until the qubit measurement is performed. Hence, the phase error rate, as defined in Eq. (B4), effectively coincides with the analogous quantity observed from the PE data: $Q_Z^j \equiv \Pr\left(\prod_{i=0}^{N-1} Z_i = 1 | \Omega_j, R_{PE}\right)$. As we discuss below, this fact does not hold in our CKA protocol (Sec. II), where the

phase error rate (18) is indirectly bounded with the PE statistics thanks to a multipartite decoy-state method.

The Ideal protocol is designed to exploit the correlations of a particular class of multipartite, W -type states, which are postselected due to single-photon interference. As a matter of fact, a noisy version of such states is recovered as the conditional state of the qubit systems postselected on the event that only detector D_j clicks. In order to see this more clearly, one can derive such a state under the Ideal conditions of no losses in the channels and $q_i = q \rightarrow 1$ for every i —indeed, the optimal values of q are close to one [34], hence we approximate the state to first order in $(1 - q)$. Under these simplifications, the state of the qubits $Q_0 \dots Q_{N-1}$ shared by the N parties, once postselected on the click of detector D_j , reads

$$|W_j\rangle_{Q_0, \dots, Q_{N-1}} := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{j} \cdot \vec{i}} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}}, \quad (\text{B5})$$

where the vector \vec{b}_i is defined as the N -bit vector of all zeroes except for the i th element that is one.

The state in Eq. (B5) is a W -type state, where each term in the sum presents a real phase determined by the detector that clicked. The state is postselected from the events where only one photon is effectively sent by any of the parties with equal probability. Indeed, under the above approximations, the probability that the W -type state in Eq. (B5) is postselected is $q^{N-1}(1 - q)N/M$.

In this regard, the Ideal protocol resembles the CKA protocol of Ref. [34] as it exploits the multipartite correlations of a W state to establish a shared conference key. As a matter of fact, we note that in the classical postprocessing the parties flip their X -basis outcomes according to $(-1)^{\vec{j} \cdot \vec{i}}$, where \vec{i} depends on the party and \vec{j} on the detector that clicked. This can be equivalently seen as party A_i applying a Z gate on their qubit before the X -basis measurement, if $\vec{j} \cdot \vec{i}$ is odd. In other words, party A_i applies the gate $Z^{\vec{j} \cdot \vec{i}}$ (note that $Z^2 = \mathbb{1}$). Since such a gate does not change the Z -basis outcomes in the PE rounds, we can assume, without loss of generality, that party A_i applies the gate $Z^{\vec{j} \cdot \vec{i}}$ before measuring their qubit in any basis. If we now apply the gates in the postselected state of the qubits (B5), we obtain

$$\begin{aligned} |W_j\rangle_{Q_0, \dots, Q_{N-1}} &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{j} \cdot \vec{i}} \bigotimes_{k=0}^{N-1} Z^{\vec{j} \cdot \vec{k}} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}} \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{j} \cdot \vec{i}} (-1)^{\vec{j} \cdot \vec{i}} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}} \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |\vec{b}_i\rangle_{Q_0, \dots, Q_{N-1}}, \end{aligned} \quad (\text{B6})$$

where we use the fact that the operator $Z_i^{\vec{k}}$ has no effect on the ket $|\vec{b}_i\rangle$ except for $k = i$, i.e., when it acts on the i th qubit that is in state $|1\rangle$. From Eq. (B6) we see that the postselected state, after the local operations that simulate the classical postprocessing of the outcomes, coincides with the W state, as claimed. The Ideal protocol presents a crucial difference from the protocol in Ref. [34], which is made explicit in the following remark:

Remark.—In Ref. [34] the parties needed to tailor their KG measurements depending on which detector clicks, in order to neutralize the effects of complex phases in their postselected W -type state. In the Ideal protocol, thanks to the bespoke BBS network, the postselected state (B5) only presents real phases, which are corrected as discussed above by simply flipping the KG outcomes and without changing the measurement basis.

This implies that, in the Ideal protocol, the parties' measurements are independent of the relay's announcements, hence they commute with the action of the relay. This enables us to reformulate the Ideal protocol in prepare-and-measure (PM) form. In the resulting PM protocol, the parties first measure their qubits and record the outcome. Then they send the optical mode, whose state is conditioned on the outcome, to the relay. Hence, the PM protocol coincides with the Ideal protocol except for Step 1.1.

Protocol 3 (Prepare-and-measure protocol)

1. Quantum part: repeat what follows for a sufficient amount of iterations.

1.1. Each party A_i prepares an optical mode a_i in a state that depends on whether the round is labeled as a PE or KG round.

(a) In a PE round, they prepare the vacuum state $|0\rangle_{a_i}$ with probability q_i , corresponding to the outcome $Z_i = +1$, and the one-photon state $|1\rangle_{a_i}$ with probability $1 - q_i$, corresponding to the outcome $Z_i = -1$.

(b) In a KG round, they prepare with equal probability either the state $|+\rangle_{a_i} = \sqrt{q_i}|0\rangle_{a_i} + \sqrt{1 - q_i}|1\rangle_{a_i}$, corresponding to the outcome $X_i = +1$, or the state $|-\rangle_{a_i} = \sqrt{q_i}|0\rangle_{a_i} - \sqrt{1 - q_i}|1\rangle_{a_i}$, corresponding to the outcome $X_i = -1$.

- 1.2. same as in Ideal prot.
 - 1.3. same as in Ideal prot.
 - 1.4. same as in Ideal prot.
 - 2. same as in Ideal prot.
 - 3. same as in Ideal prot.
-

Note that, while the PM protocol is more practical than the Ideal protocol (e.g., it does not require qubit-photon entanglement), it is equivalent to the latter from the point of view of security, since an adversary could not distinguish which of the two protocols is run. Despite the increased practicality, the PM protocol still requires

the preparation of single-photon states and their superposition with the vacuum. This prompts us to reduce even further the complexity of the protocol's implementation and obtain a practical, prepare-and-measure, CKA protocol.

In order to derive a practical CKA protocol, we observe that the states prepared in the KG rounds of the PM protocol $(|\pm\rangle_{a_i})$ can be approximated by coherent states of suitable amplitude $(|\pm\alpha_i\rangle)$, for $\alpha_i \in \mathbb{R}$, where the information about the X -basis outcome is encoded in the amplitude's sign. At the same time, the statistics collected in PE rounds and used to compute the phase error rate (B4) are linked to the so-called yields, i.e., the probability that a detector clicks given that each party sent a fixed number of photons. This suggests us to prepare phase-randomized coherent states in PE rounds and use their detection statistics to apply the decoy-state method and compute the yields, with which we bound the phase error rate. This heuristic reasoning leads us to the practical CKA protocol presented in Sec. II, where, we recall, each party A_i prepares a coherent state $|x_i\alpha_i\rangle_{a_i}$ with $x_i = \pm 1$ in KG rounds and phase-randomized coherent states in PE rounds.

We emphasize that, in the protocol of Sec. II, the choice of the type of round (KG or PE) cannot be delayed until after the action of the untrusted relay, contrary to the Ideal protocol. Indeed, the average state prepared by A_i in KG rounds, $(1/2)(|\alpha_i\rangle\langle\alpha_i| + |-\alpha_i\rangle\langle-\alpha_i|)$, differs from the average state prepared in PE rounds, $(1/|\mathcal{S}_i|) \sum_k \rho_{a_i}(\beta_k)$, due to the coherences of the former in the Fock basis. This means that an adversary controlling the relay could partially distinguish the type of round being executed and act accordingly. Another way to see this is that there is no equivalent entanglement-based version of the CKA protocol. That is, party A_i cannot find two suitable POVMs (one for KG rounds and one for PE rounds) such that the state of their optical mode, conditioned on measuring with one of the two POVMs a fictitious system entangled with the optical mode, corresponds to the state that A_i should prepare in that round [51].

One of the implications of the above fact is that the phase error rate (B4) affecting the KG rounds cannot be directly observed from the statistics of the PE rounds, as instead happens in the Ideal protocol. Nevertheless, in the security proof provided in Sec. III, we show how to use the PE statistics to derive an upper bound on the phase error rate (B4). Specifically, we develop a multipartite decoy-state method that allows us to bound certain yields through the PE statistics. The yields, in turn, are needed to analytically upper bound the phase error rate with Eq. (7).

This concludes our connection between the Ideal protocol, which manifestly makes use of W -state correlations and whose phase error rate can be directly observed in PE rounds, and the CKA protocol discussed in the main text, whose phase error rate is bounded by PE statistics combined with the decoy-state method.

APPENDIX C: ANALYTICAL UPPER BOUND ON THE YIELDS

In this Appendix, we report the full derivation of the analytical bounds on the yields as a function of the observed gains, Eq. (34). The bounds are derived with a multipartite decoy-state method in which each party is provided with the same set of two decoy intensities: $\mathcal{S} = \{\beta_0, \beta_1\}$.

We recall that the gains are probabilities that can be directly estimated from the observed data and are defined as $G_{\vec{f}}^j := \Pr(\Omega_j | \beta_{f_0}, \dots, \beta_{f_{N-1}})$, where \vec{f} is an N -dimensional binary vector that covers all the possible choices of intensities by the parties. From Eq. (25) in Sec. III, we show that the gains are related to the yields by the following equality:

$$\begin{aligned} G_{\vec{f}}^j &= \sum_{n_0, \dots, n_{N-1}=0}^{\infty} Y_{n_0, \dots, n_{N-1}}^j \prod_{i=0}^{N-1} P_{\beta_{f_i}}(n_i) \\ &= \sum_{n_0, \dots, n_{N-1}=0}^{\infty} Y_{n_0, \dots, n_{N-1}}^j \prod_{i=0}^{N-1} \frac{e^{-\beta_{f_i}} \beta_{f_i}^{n_i}}{n_i!} \\ &= \prod_{i=0}^{N-1} e^{-\beta_{f_i}} \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \frac{Y_{n_0, \dots, n_{N-1}}^j}{n_0! \cdots n_{N-1}!} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i}. \quad (C1) \end{aligned}$$

We remark that, in principle, the gains can depend on the detector D_j that clicks and so can the yields. However, for simplicity of notation, in this section we drop the superscript j from the gains and yields. Moreover, in our simulations, due to the symmetric losses affecting each party, the gains and hence the yields are independent of which detector clicks (see Appendix D). Hence their dependency on j vanishes.

The last equality in Eq. (C1) brings us to define a rescaled gain, $\tilde{G}_{\vec{f}}$, as follows:

$$\tilde{G}_{\vec{f}} := \frac{G_{\vec{f}}}{\prod_{i=0}^{N-1} e^{-\beta_{f_i}}} = \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i}. \quad (C2)$$

We now define, from a fixed binary vector \vec{h} of dimension N and Hamming weight $|\vec{h}| = m$, the following quantity:

$$B_{\vec{h}} := \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{i=0}^{N-1} \left(\beta_1^{1-h_i} \beta_0^{n_i} - \beta_0^{1-h_i} \beta_1^{n_i} \right), \quad (C3)$$

which can be recast as a combination of rescaled gains $\tilde{G}_{\vec{f}}$. To see this, we expand the product over i in the last expression as a sum of 2^N products, each labeled by a binary

vector \vec{f} , where each term in the sum is the product of either $\beta_1^{1-h_i} \beta_0^{n_i}$ or $-\beta_0^{1-h_i} \beta_1^{n_i}$ for every $i = 0, \dots, N-1$. In particular, $f_i = 0$ ($f_i = 1$) indicates that the former (latter) quantity is picked. With this in mind, we can write

$$\begin{aligned} &\prod_{i=0}^{N-1} \left(\beta_1^{1-h_i} \beta_0^{n_i} - \beta_0^{1-h_i} \beta_1^{n_i} \right) \\ &= \sum_{f=0}^{2^N-1} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i} (-1)^{f_i} \beta_0^{(1-h_i)f_i} \beta_1^{(1-h_i)(1-f_i)} \\ &= \sum_{f=0}^{2^N-1} (-1)^{|\vec{f}|} \beta_0^{(\vec{1}-\vec{h}) \cdot \vec{f}} \beta_1^{(\vec{1}-\vec{h}) \cdot (\vec{1}-\vec{f})} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i}. \quad (C4) \end{aligned}$$

By replacing the last expression in Eq. (C3), we can employ Eq. (C2) to directly relate $B_{\vec{h}}$ and $\tilde{G}_{\vec{f}}$. We obtain

$$B_{\vec{h}} = \sum_{f=0}^{2^N-1} (-1)^{|\vec{f}|} \beta_0^{(\vec{1}-\vec{h}) \cdot \vec{f}} \beta_1^{(\vec{1}-\vec{h}) \cdot (\vec{1}-\vec{f})} \tilde{G}_{\vec{f}}. \quad (C5)$$

This expression is fundamental as it constitutes the link between the quantity $B_{\vec{h}}$, which in the following is used to bound the yields, and the observed gains.

By recasting Eq. (C3) as follows:

$$\begin{aligned} B_{\vec{h}} &= \sum_{n_0, \dots, n_{N-1}=0}^{\infty} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \left(\beta_0^{n_i} - \beta_1^{n_i} \right) \\ &\quad \times \prod_{\substack{i \text{ s.t.} \\ h_i=0}} \left(\beta_1 \beta_0^{n_i} - \beta_0 \beta_1^{n_i} \right), \quad (C6) \end{aligned}$$

we notice that, whenever $h_i = 1$, the coefficient of the yields $Y_{n_0, \dots, 0, \dots, n_{N-1}}$ (i.e., with $n_i = 0$) is null, implying that they do not contribute to the value of $B_{\vec{h}}$. Similarly, when $h_i = 0$, all yields of the form $Y_{n_0, \dots, 1, \dots, n_{N-1}}$ are removed. With this observation, we can now obtain a non-trivial upper bound on any yield $Y_{n_0, \dots, n_{N-1}}$ in terms of a certain combination of $B_{\vec{h}}$.

To do so, we recast Eq. (C6) as follows, where in the first term we sum only over the indexes n_i that correspond to $h_i = 1$ and set all the other photon indexes to zero, while in the second term we account for all the other possibilities:

$$\begin{aligned}
 B_{\vec{h}} = & (-1)^{N-m} (\beta_0 - \beta_1)^{N-m} \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}(\vec{h})} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \\
 & + \sum_{(n_0, \dots, n_{N-1}) \in \tilde{\mathcal{N}}(\vec{h})} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.} \\ h_i=0}} (\beta_1 \beta_0^{n_i} - \beta_0 \beta_1^{n_i}), \tag{C7}
 \end{aligned}$$

where the sets of indexes $\mathcal{N}(\vec{h})$ and $\tilde{\mathcal{N}}(\vec{h})$ are defined as

$$\mathcal{N}(\vec{h}) := \{(n_0, \dots, n_{N-1}) : n_i = h_i r_i, r_i \geq 1\}, \tag{C8}$$

$$\tilde{\mathcal{N}}(\vec{h}) := \{(n_0, \dots, n_{N-1}) : n_i \geq 1 \text{ (if } h_i = 1\text{); } n_i \geq 2 \text{ or } n_i = 0 \text{ (if } h_i = 0\text{)}\} \setminus \mathcal{N}(\vec{h}), \tag{C9}$$

where k_i are integers. Note that the sum over n_i in the second term skips the case $n_i = 1$ for $h_i = 0$ since this contribution is null in Eq. (C6) (see observation above).

We observe that the yields in the first sum in Eq. (C7) contain exactly m nonzero photon numbers, which allowed us to factor out the quantities $(\beta_1 \beta_0^{n_i} - \beta_0 \beta_1^{n_i})$. Now, we split the second sum in Eq. (C7) in a sum of $N - m$ terms, where each term contains only yields with $m + k$ nonzero photon numbers, for $k = 1, \dots, N - m$. In this way, we can factor out the quantities $(\beta_1 \beta_0^{n_i} - \beta_0 \beta_1^{n_i})$ even in the second sum. This becomes relevant later, when we want to evaluate the sign in front of each yield. In order to sum over the various combinations of yields with $m + k$ photon numbers, we introduce the binary vectors $\vec{h}^{(k)}$, which can be seen as “expansions” of the vector \vec{h} obtained by flipping k of its zeros to ones. Thus, we have that $|\vec{h}^{(k)}| = m + k$ and that $h_i^{(k)} = 1$ whenever $h_i = 1$, which can be formally stated as the condition: $\vec{h}^{(k)} \wedge \vec{h} = \vec{h}$, where \wedge is the bitwise AND operation. Analogously to \vec{h} , when $h_i^{(k)} = 0$ we fix the corresponding photon number n_i to zero. Then, in analogy with $\mathcal{N}(\vec{h})$, we define a set of indexes $\mathcal{N}(\vec{h}, \vec{h}^{(k)})$ for each expansion $\vec{h}^{(k)}$ that represents the combinations of photon numbers that are allowed by the chosen vector $\vec{h}^{(k)}$:

$$\mathcal{N}(\vec{h}, \vec{h}^{(k)}) := \{(n_0, \dots, n_{N-1}) : n_i = h_i^{(k)} r_i, r_i \geq 1 + h_i^{(k)} - h_i\}, \tag{C10}$$

where we account for the fact that each additional bit equal to one in $\vec{h}^{(k)}$, which is a zero in \vec{h} , corresponds to an index n_i that starts from two instead of one. According to this, we obtain

$$\begin{aligned}
 B_{\vec{h}} = & (-1)^{N-m} (\beta_0 - \beta_1)^{N-m} \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}(\vec{h})} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \\
 & + \sum_{k=1}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} (\beta_0 \beta_1)^k \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}_k(\vec{h})} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)}-h_i=1}} (\beta_0^{n_i-1} - \beta_1^{n_i-1}), \tag{C11}
 \end{aligned}$$

where we define the following set that accounts for all possible choices of $\vec{h}^{(k)}$, for a given k :

$$\mathcal{N}_k(\vec{h}) := \bigcup_{\substack{\vec{h}^{(k)} \in \{0,1\}^N: \\ |\vec{h}^{(k)}| = m+k \\ \vec{h}^{(k)} \wedge \vec{h} = \vec{h}}} \mathcal{N}(\vec{h}, \vec{h}^{(k)}), \tag{C12}$$

where the operation \wedge represents the entry-wise product. Now, we wish to isolate a specific yield $Y_{u_0, \dots, u_{N-1}}$ from the first sum in Eq. (C11) in order to derive an upper bound on it. Note that we can choose any combination of photon numbers

(u_0, \dots, u_{N-1}) such that $u_i = h_i k_i$, for $k_i \geq 1$. Since the choice of the vector \vec{h} is arbitrary, the photon numbers are also arbitrary. By isolating the yield $Y_{u_0, \dots, u_{N-1}}$ in Eq. (C11), we obtain

$$\begin{aligned}
B_{\vec{h}} &= (-1)^{N-m} (\beta_0 - \beta_1)^{N-m} Y_{u_0, \dots, u_{N-1}} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{(\beta_0^{u_i} - \beta_1^{u_i})}{u_i!} \\
&+ (-1)^{N-m} (\beta_0 - \beta_1)^{N-m} \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}(\vec{h}) \setminus \{(u_0, \dots, u_{N-1})\}} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \\
&+ \sum_{k=1}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} (\beta_0 \beta_1)^k \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}_k(\vec{h})} \frac{Y_{n_0, \dots, n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)} - h_i=1}} (\beta_0^{n_i-1} - \beta_1^{n_i-1}).
\end{aligned} \tag{C13}$$

We now derive an upper bound on $Y_{u_0, \dots, u_{N-1}}$. To this aim, we observe that the yield $Y_{u_0, \dots, u_{N-1}}$ and each of the yields in the second term in Eq. (C13) are multiplied by coefficients of the same sign. Indeed, they are multiplied by the same number of terms of the form $(\beta_0^s - \beta_1^s)$. More quantitatively, the sign of the coefficient $C_{u_0, \dots, u_{N-1}}$ of $Y_{u_0, \dots, u_{N-1}}$ and of the coefficients of the yields in the second term is

$$\text{sign}(C_{u_0, \dots, u_{N-1}}) = (-1)^{N-m} [\text{sign}(\beta_0 - \beta_1)]^N. \tag{C14}$$

By similar arguments, the yields in the third term in Eq. (C13) are multiplied by coefficients $C_{n_0, \dots, n_{N-1}}$ with the following sign:

$$\text{sign}(C_{n_0, \dots, n_{N-1}}) = (-1)^{N-m-k} [\text{sign}(\beta_0 - \beta_1)]^N. \tag{C15}$$

In order to extract an upper bound on $Y_{u_0, \dots, u_{N-1}}$, we need to minimize all the yields carrying the same sign as $Y_{u_0, \dots, u_{N-1}}$ and maximize all the yields with opposite sign in Eq. (C13). In our case, this means setting to zero all the yields in the first sum and all the yields in the second sum that correspond to even values of k . The other yields are set to one. By applying this reasoning to Eq. (C13), we obtain the following expression satisfied by an upper bound $U_{u_0, \dots, u_{N-1}}$ on $Y_{u_0, \dots, u_{N-1}}$:

$$\begin{aligned}
B_{\vec{h}} &= (-1)^{N-m} (\beta_0 - \beta_1)^{N-m} U_{u_0, \dots, u_{N-1}} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{(\beta_0^{u_i} - \beta_1^{u_i})}{u_i!} + \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} (\beta_0 \beta_1)^k \\
&\times \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}_k(\vec{h})} \frac{1}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)} - h_i=1}} (\beta_0^{n_i-1} - \beta_1^{n_i-1}).
\end{aligned} \tag{C16}$$

In order to simplify the above expression, we first focus on the term with the sum over k , which we denote $B_{\vec{h}}^{(2)}$ and recast as follows:

$$\begin{aligned}
B_{\vec{h}}^{(2)} &= \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} (\beta_0 \beta_1)^k \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}_k(\vec{h})} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{\beta_0^{n_i} - \beta_1^{n_i}}{n_i!} \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)} - h_i=1}} \frac{\beta_0^{n_i-1} - \beta_1^{n_i-1}}{n_i!} \\
&= \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} (\beta_0 \beta_1)^k \\
&\times \sum_{\substack{\vec{h}^{(k)} \in \{0,1\}^N \\ |\vec{h}^{(k)}| = m+k \\ \vec{h}^{(k)} \wedge \vec{h} = \vec{h}}} \sum_{(n_0, \dots, n_{N-1}) \in \mathcal{N}(\vec{h}, \vec{h}^{(k)})} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{\beta_0^{n_i} - \beta_1^{n_i}}{n_i!} \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)} - h_i=1}} \frac{\beta_0^{n_i-1} - \beta_1^{n_i-1}}{n_i!},
\end{aligned} \tag{C17}$$

where in the second equality we split the second sum over all the different subsets $\mathcal{N}(\vec{h}, \vec{h}^{(k)})$ in $\mathcal{N}_k(\vec{h})$ using Eq. (C12). We can now swap the innermost sum in the last expression with the products and obtain

$$B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} (\beta_0 \beta_1)^k \sum_{\substack{\vec{h}^{(k)} \in \{0,1\}^N: \\ |\vec{h}^{(k)}|=m+k \\ \vec{h}^{(k)} \wedge \vec{h} = \vec{h}}} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \left(\sum_{n_i=1}^{\infty} \frac{\beta_0^{n_i} - \beta_1^{n_i}}{n_i!} \right) \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)} - h_i = 1}} \left(\sum_{n_i=2}^{\infty} \frac{\beta_0^{n_i-1} - \beta_1^{n_i-1}}{n_i!} \right). \quad (C18)$$

It can now be easily seen, using the Taylor series of the exponential function, that the following identities hold:

$$\sum_{n=1}^{\infty} \frac{\beta_0^n - \beta_1^n}{n!} = e^{\beta_0} - e^{\beta_1}, \quad (C19)$$

$$\sum_{n=2}^{\infty} \frac{\beta_0^{n-1} - \beta_1^{n-1}}{n!} = \frac{1}{\beta_0 \beta_1} (\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1). \quad (C20)$$

By using the above identities in Eq. (C18), we obtain

$$B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} \sum_{\substack{\vec{h}^{(k)} \in \{0,1\}^N: \\ |\vec{h}^{(k)}|=m+k \\ \vec{h}^{(k)} \wedge \vec{h} = \vec{h}}} (e^{\beta_0} - e^{\beta_1})^m (\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1)^k, \quad (C21)$$

where we observe that the argument of the sum over $\vec{h}^{(k)}$ is independent of $\vec{h}^{(k)}$. Therefore, the sum reduces to counting all the possible choices of $\vec{h}^{(k)}$ for a given k . This number is given by the possible combinations of k bits in $\vec{h}^{(k)}$ that are set to one, chosen among the $N - m$ elements that correspond to zeroes in \vec{h} . Hence, we have $\binom{N-m}{k}$ choices and we obtain

$$B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k} (\beta_0 - \beta_1)^{N-m-k} \binom{N-m}{k} (e^{\beta_0} - e^{\beta_1})^m (\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1)^k \\ = \sum_{k=0}^{\lfloor (N-m-1)/2 \rfloor} (-1)^{N-m-2k-1} (\beta_0 - \beta_1)^{N-m-2k-1} \binom{N-m}{2k+1} (e^{\beta_0} - e^{\beta_1})^m (\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1)^{2k+1}, \quad (C22)$$

where $\lfloor x \rfloor$ is the floor function. Finally, by employing (C22) in Eq. (C16), we obtain the following equality satisfied by the upper bound on the selected yield

$$B_{\vec{h}} = (-1)^{N-m} (\beta_0 - \beta_1)^{N-m} U_{u_0, \dots, u_{N-1}} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{(\beta_0^{u_i} - \beta_1^{u_i})}{u_i!} + \sum_{k=0}^{\lfloor (N-m-1)/2 \rfloor} (-1)^{N-m-2k-1} (\beta_0 - \beta_1)^{N-m-2k-1} \\ \times \binom{N-m}{2k+1} (e^{\beta_0} - e^{\beta_1})^m (\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1)^{2k+1}. \quad (C23)$$

By isolating the yield's upper bound and relabeling $u_i \rightarrow n_i$, we obtain the final expression of the yield bound: $\bar{Y}_{n_0, \dots, n_{N-1}} = \min\{U_{n_0, \dots, n_{N-1}}, 1\}$, where

$$U_{n_0, \dots, n_{N-1}} = \prod_{\substack{i \text{ s.t.} \\ n_i \neq 0}} \frac{n_i!}{\beta_0^{n_i} - \beta_1^{n_i}} \left[\frac{B_{\vec{h}} (-1)^{N-m}}{(\beta_0 - \beta_1)^{N-m}} + (e^{\beta_0} - e^{\beta_1})^m \sum_{k=0}^{\lfloor (N-m-1)/2 \rfloor} \binom{N-m}{2k+1} \left(\frac{\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1}{\beta_0 - \beta_1} \right)^{2k+1} \right], \quad (C24)$$

where $B_{\vec{h}}$ is given in Eq. (C5) (and in principle can depend on the detector D_j through the gains) and $m = |\vec{h}|$, while \vec{h} is the binary vector with components h_i defined by

$$h_i = \begin{cases} 1 & \text{if } n_i \geq 1 \\ 0 & \text{if } n_i = 0. \end{cases} \quad (\text{C25})$$

APPENDIX D: CHANNEL MODEL

In this Appendix we describe our channel model and compute the detection statistics of the protocol. The channel model includes the following sources of noise.

1. Pure-photon loss: the optical mode of party goes through the same lossy channel. The lossy channel is modeled with a beam splitter with transmittance η , where the additional input port of the beam splitter is fed with the vacuum.

2. Polarization misalignment: the optical mode of each party undergoes a polarization misalignment modeled by a unitary operation that maps the creation operator of each mode according to

$$\hat{a}_i^\dagger \rightarrow \cos \theta_i \hat{a}_{i,P}^\dagger - \sin \theta_i \hat{a}_{i,P_\perp}^\dagger, \quad (\text{D1})$$

where $\hat{a}_{i,P}^\dagger$ is the creation operator on the original polarization and $\hat{a}_{i,P_\perp}^\dagger$ is the creation operator on the orthogonal polarization.

3. Phase shift: the optical mode of each party undergoes a phase shift ϕ_i , modelled by multiplying the mode operator \hat{a}_i^\dagger by a phase ϕ_i .

4. Dark counts in the detectors: each detector is affected by dark counts, with a probability p_d that is equal for all detectors and independent on the state sent.

In Sec. V we argue that since the channel of each party is equally lossy, the optimal choice for the signal intensities is the same for each party. Hence, here we assume that the amplitudes of each party in KG and PE rounds coincide: $\alpha_i = \alpha$ and $\mathcal{S}_i = \mathcal{S}$, for every i . Moreover, we choose the same polarization misalignment between the reference party A_0 and each other party. This means that we choose a misalignment of θ_0 for A_0 and θ_1 for the other parties. Similarly for the phase shift, we set $\phi_0 = 0$ and $\phi_i = \phi$ for $i \neq 0$.

1. Computation of $\Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{\text{KG}})$

We start by computing the detection probability $\Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{\text{KG}})$, which is the probability that only detector D_j clicks, given that party A_i prepared, in a KG round, the coherent state $|x_i \alpha\rangle$, with $x_i = \pm 1$. This detection probability is needed to compute the QBER, Eq. (4), through Eq. (5).

The state prepared by the N parties in a KG round, before any noise or loss is applied, reads

$$|\psi_{\text{in}}\rangle = \bigotimes_{i=0}^{N-1} |x_i \alpha\rangle. \quad (\text{D2})$$

We now apply the sources of noise discussed above.

1. The resulting state after the lossy channel is the following:

$$|\psi'_{\text{in}}\rangle = \bigotimes_{i=0}^{N-1} |x_i \sqrt{\eta} \alpha\rangle. \quad (\text{D3})$$

2. After applying the polarization misalignment, we obtain

$$|\psi''_{\text{in}}\rangle = \bigotimes_{i=0}^{N-1} |x_i \cos \theta_i \sqrt{\eta} \alpha\rangle_P | -x_i \sin \theta_i \sqrt{\eta} \alpha\rangle_{P_\perp}. \quad (\text{D4})$$

3. After the phase shift ϕ_i is applied on each mode, we get

$$|\psi_{\text{in}}'''\rangle = \bigotimes_{i=0}^{N-1} |x_i \cos \theta_i e^{i\phi_i} \sqrt{\eta} \alpha\rangle_P | -x_i \sin \theta_i e^{i\phi_i} \sqrt{\eta} \alpha\rangle_{P_\perp}. \quad (\text{D5})$$

The state in Eq. (D5) is the global state of the N parties' modes, after the noisy and lossy channel and before entering the BBS network. We now evolve the modes through the M -input and M -output BBS network, according to the transformation in Eq. (3). We define the coefficients of the inverse transformation of the modes as $f_{i,j} := (-1)^{-i,j}$. Here, we make the nonrestrictive assumption that the N modes sent by the parties correspond to the first N inputs of the BBS network. A different choice would not alter the protocol's performance. The output state after the BBS network reads

$$|\psi_{\text{out}}\rangle = \bigotimes_{j=0}^{M-1} \left| \sqrt{\frac{\eta}{M}} \alpha \sum_{i=0}^{N-1} x_i f_{i,j} \cos \theta_i e^{i\phi_i} \right\rangle_P \left| -\sqrt{\frac{\eta}{M}} \alpha \sum_{i=0}^{N-1} x_i f_{i,j} \sin \theta_i e^{i\phi_i} \right\rangle_{P_\perp}. \quad (\text{D6})$$

At this point, the relay performs a threshold measurement on each mode that returns a click in the corresponding detector if one or more photons are detected. We are interested in the probability that only detector D_j clicks, i.e., $\Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{\text{KG}})$. By including the effect of dark counts, we can express such probability as follows:

$$\begin{aligned} \Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{\text{KG}}) &= p_d (1 - p_d)^{M-1} \text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] + (1 - p_d)^{M-1} \text{Tr} \left[\rho_{\text{out}} (\mathbb{1}_j - |0\rangle\langle 0|_j) \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] \\ &= (1 - p_d)^{M-1} \text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] - (1 - p_d)^M \text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right], \end{aligned} \quad (\text{D7})$$

where $|0\rangle\langle 0|_k$ is the projector on the vacuum of the output mode k for polarizations P and P_\perp , as the detectors do not distinguish polarization, and $\rho_{\text{out}} = |\psi_{\text{out}}\rangle\langle \psi_{\text{out}}|$. We calculate both terms appearing in Eq. (D7). For the second term, we have

$$\begin{aligned} \text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] &= \prod_{k=0}^{M-1} \exp \left[- \left| \sqrt{\frac{\eta}{M}} \alpha \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 - \left| \sqrt{\frac{\eta}{M}} \alpha \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right] \\ &= \exp \left[-\frac{\eta}{M} \alpha^2 \sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right) \right]. \end{aligned} \quad (\text{D8})$$

We now focus on the sum over k in the last expression and use the fact that we fix the angles θ_i and ϕ_i as discussed above. The sum over k simplifies to

$$\begin{aligned} &\sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right) \\ &= \sum_{k=0}^{M-1} \left(\left| x_0 \cos \theta_0 + \cos \theta_1 e^{i\phi} \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 + \left| x_0 \sin \theta_0 + \sin \theta_1 e^{i\phi} \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 \right) \end{aligned}$$

$$\begin{aligned}
 &= \sum_{k=0}^{M-1} \left(x_0^2 \cos^2 \theta_0 + \cos^2 \theta_1 \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 + x_0^2 \sin^2 \theta_0 + \sin^2 \theta_1 \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 \right. \\
 &\quad \left. + 2x_0 \cos \theta_0 \cos \theta_1 \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} + 2x_0 \sin \theta_0 \sin \theta_1 \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} \right) \\
 &= \sum_{k=0}^{M-1} \left(1 + \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 + 2x_0 \cos \theta \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} \right), \tag{D9}
 \end{aligned}$$

where we use that $x_i = \pm 1$, $\cos^2 \theta_i + \sin^2 \theta_i = 1$ and $\cos \theta_0 \cos \theta_1 + \sin \theta_0 \sin \theta_1 = \cos(\theta_0 - \theta_1)$ and where we define $\theta := \theta_0 - \theta_1$. Consider the following lemma for the function $f_{i,k}$, which coincides with $f_{k,i}$ in Eq. (A6).

Lemma 1.—For $f_{k,i}$ as defined by (A6), it holds

$$\sum_{i=0}^{M-1} f_{k,i} = M \delta_{k,0}. \tag{D10}$$

Proof.—To show the result of the lemma we first recall that the function $f_{k,i}$ is given by

$$f_{k,i} = (-1)^{\vec{k} \cdot \vec{i}}, \tag{D11}$$

where \vec{k} and \vec{i} are the binary vectors of length s that represent the numbers k and i in binary representation. Then, the sum over i of $f_{k,i}$ can be recast as

$$\sum_{i=0}^{M-1} f_{k,i} = \sum_{\vec{i} \in \{0,1\}^s} (-1)^{\vec{k} \cdot \vec{i}} = \sum_{c=0}^{|\vec{k}|} (-1)^c \binom{|\vec{k}|}{c} 2^{s-|\vec{k}|}, \tag{D12}$$

where in the second equality we perform the sum over all the possible values c of $\vec{k} \cdot \vec{i}$ and count how many distinct vectors \vec{i} lead to the same scalar product $c = \vec{k} \cdot \vec{i}$. This number is given by the ways in which we can select c bits equal to one in \vec{k} (the binomial coefficient), which fixes the corresponding c bits in \vec{i} to be one and also fixes other $|\vec{k}| - c$ bits in \vec{i} to be zero since they correspond to the ones in \vec{k} that have not been selected. At this point, the vector \vec{i} is almost all fixed, except for the bits that correspond to the $s - |\vec{k}|$ zero bits in \vec{k} . Since such bits in \vec{i} can be arbitrary as they would not contribute to the scalar product, the total number of possibilities is given by $2^{s-|\vec{k}|}$.

Now, we can simplify the expression in Eq. (D12) as follows:

$$\sum_{i=0}^{M-1} f_{k,i} = \sum_{c=0}^{|\vec{k}|} (-1)^c \binom{|\vec{k}|}{c} 2^{s-|\vec{k}|} = 2^{s-|\vec{k}|} \sum_{c=0}^{|\vec{k}|} \binom{|\vec{k}|}{c} (-1)^c (1)^{|\vec{k}|-c} = 2^{s-|\vec{k}|} (1-1)^{|\vec{k}|} = M \delta_{k,0}, \tag{D13}$$

where we use the binomial formula in the third line and that $M = 2^s$ together with the definition of Kronecker δ in the last line. This concludes the proof. ■

By applying Lemma 3 in Eq. (D9), we can simplify the term with the cosines as follows:

$$\begin{aligned}
 \sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right) &= \sum_{k=0}^{M-1} \left(1 + \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 + 2x_0 \cos \theta \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} \right) \\
 &= \sum_{k=0}^{M-1} \left(1 + \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 \right) + 2x_0 \cos \theta \cos \phi \sum_{i=1}^{N-1} x_i M \delta_{i,0} \\
 &= \sum_{k=0}^{M-1} \left(1 + \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 \right) = M + \sum_{k=0}^{M-1} \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2, \quad (\text{D14})
 \end{aligned}$$

where the sum with the Kronecker $\delta_{i,0}$ is identically zero since the index i starts from one.

We now expand the square in the last expression and obtain

$$\begin{aligned}
 \sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right) &= M + \sum_{k=0}^{M-1} \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 \\
 &= M + \sum_{k=0}^{M-1} \sum_{i,i'=1}^{N-1} x_i x_{i'} f_{i,k} f_{i',k} = M + \sum_{i,i'=1}^{N-1} x_i x_{i'} \sum_{\vec{k} \in \{0,1\}^s} (-1)^{(\vec{i}+\vec{i}') \cdot \vec{k}}, \quad (\text{D15})
 \end{aligned}$$

where we remark that the result of Lemma 3 cannot be directly applied to the innermost sum since $(\vec{i} + \vec{i}')$ is not a binary vector. However, we can use the lemma to compute such a sum. In order to do so, we observe that the vector $(\vec{i} + \vec{i}')$ deviates from a binary vector only in the elements r where $i_r = i'_r = 1$, and we have $\vec{i} \cdot \vec{i}'$ many such elements. These elements do not contribute to the value of $(-1)^{(\vec{i}+\vec{i}') \cdot \vec{k}}$ regardless of the value of k_r . Hence, we can define shorter vectors $\vec{m} \in \{0, 1\}^{s-\vec{i} \cdot \vec{i}'}$ and $\vec{l} \in \{0, 1\}^{s-\vec{i} \cdot \vec{i}'}$ that correspond to the remaining $s - \vec{i} \cdot \vec{i}'$ elements of $\vec{i} + \vec{i}'$ and \vec{k} , respectively, where $i_r + i'_r \neq 2$. By definition, we have that $(-1)^{(\vec{i}+\vec{i}') \cdot \vec{k}} = (-1)^{\vec{m} \cdot \vec{l}}$. Now, in order to replace the sum over \vec{k} with a sum over \vec{l} , we must account for the fact that, for every fixed value of \vec{l} and hence of $(-1)^{\vec{m} \cdot \vec{l}}$, there are $2^{\vec{i} \cdot \vec{i}'}$ vectors \vec{k} such that $(-1)^{(\vec{i}+\vec{i}') \cdot \vec{k}} = (-1)^{\vec{m} \cdot \vec{l}}$. Therefore, we can recast the innermost sum in Eq. (D15) as follows:

$$\sum_{\vec{k} \in \{0,1\}^s} (-1)^{(\vec{i}+\vec{i}') \cdot \vec{k}} = 2^{\vec{i} \cdot \vec{i}'} \sum_{\vec{l} \in \{0,1\}^{s-\vec{i} \cdot \vec{i}'}} (-1)^{\vec{m} \cdot \vec{l}} = 2^{\vec{i} \cdot \vec{i}'} 2^{s-\vec{i} \cdot \vec{i}'} \delta_{\vec{m}, \vec{0}} = M \delta_{\vec{m}, \vec{0}} = M \delta_{\vec{i}, \vec{i}'}, \quad (\text{D16})$$

where in the second equality we used Lemma 3 since now \vec{m} is a binary vector and in the fourth equality we use the fact that the $\delta_{\vec{m}, \vec{0}}$ effectively implies that $\vec{i} = \vec{i}'$ over the whole set of s elements since \vec{m} is given by the elements of $\vec{i} + \vec{i}'$ corresponding to the positions where the two vectors are not both equal to one.

Thus, by using Eq. (D16) in Eq. (D15), we obtain

$$\begin{aligned}
 \sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right) &= M + M \sum_{i,i'=1}^{N-1} x_i x_{i'} \delta_{\vec{i}, \vec{i}'} \\
 &= M \left(1 + \sum_{i=1}^{N-1} x_i^2 \right) = MN, \quad (\text{D17})
 \end{aligned}$$

where we use the fact that $x_i = \pm 1$. Finally, by employing Eq. (D17) in Eq. (D8), we obtain

$$\text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] = e^{-N\eta\alpha^2}, \quad (\text{D18})$$

which concludes the calculation of the second trace in Eq. (D7).

We now move on to calculate the first trace in Eq. (D7). In a similar manner to Eq. (D8), we can write

$$\begin{aligned} \text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] &= \prod_{k \neq j} \exp \left[- \left| \sqrt{\frac{\eta}{M}} \alpha \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 - \left| \sqrt{\frac{\eta}{M}} \alpha \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right] \\ &= \exp \left[- \frac{\eta}{M} \alpha^2 \sum_{k \neq j} \left(\left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2 \right) \right] \\ &= \exp \left[- \frac{\eta}{M} \alpha^2 \sum_{k \neq j} C_k \right] = \exp \left[- \frac{\eta}{M} \alpha^2 \left(\sum_{k=0}^{M-1} C_k - C_j \right) \right] = e^{-N\eta\alpha^2} e^{(\eta/M)\alpha^2 C_j}, \end{aligned} \quad (\text{D19})$$

where in the third line we define

$$C_k := \left| \sum_{i=0}^{N-1} x_i f_{i,k} \cos \theta_i e^{i\phi_i} \right|^2 + \left| \sum_{i=0}^{N-1} x_i f_{i,k} \sin \theta_i e^{i\phi_i} \right|^2, \quad (\text{D20})$$

and we use Eq. (D18) in the last line. With analogous calculations to those leading to Eq. (D9), one can simplify C_j as follows:

$$C_j = 1 + \left| \sum_{i=1}^{N-1} x_i f_{i,j} \right|^2 + 2x_0 \cos \theta \cos \phi \sum_{i=1}^{N-1} x_i f_{i,j}. \quad (\text{D21})$$

We now recall that in the postprocessing of the protocol, party A_i flips their X -basis outcome, x_i , if $f_{i,j} = (-1)^{\vec{i}\vec{j}} = -1$. For this, we identify the sum $\sum_{i=1}^{N-1} x_i f_{i,j}$ in the last expression as the sum of the postprocessed X -basis outcomes of the parties (excluding A_0) and can label it as follows:

$$\sum_{i=1}^{N-1} x_i f_{i,j} =: S_{x_1, \dots, x_{N-1}}^j. \quad (\text{D22})$$

This allows us to recast C_j as follows:

$$C_j = 1 + (S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j x_0 \cos \theta \cos \phi. \quad (\text{D23})$$

By using the last expression in Eq. (D19), we obtain the final form of the first trace in Eq. (D7):

$$\begin{aligned} \text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] &= e^{-N\eta\alpha^2} e^{(\eta/M)\alpha^2 \left(1 + (S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j x_0 \cos \theta \cos \phi \right)} \\ &= e^{-(MN-1)\eta\alpha^2/M} e^{\eta\alpha^2 \left((S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j x_0 \cos \theta \cos \phi \right) / M}. \end{aligned} \quad (\text{D24})$$

Finally, by combining Eqs. (D18) and (D24) in Eq. (D7), we obtain the following expression for the probability that only detector D_j clicks, conditioned on the parties preparing coherent states $|x_0\alpha\rangle, \dots, |x_{N-1}\alpha\rangle$ in a KG round:

$$\begin{aligned} \text{Pr}(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{\text{KG}}) &= (1 - p_d)^{M-1} e^{-(MN-1)\eta\alpha^2/M} e^{\eta\alpha^2 \left((S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j x_0 \cos \theta \cos \phi \right) / M} \\ &\quad - (1 - p_d)^M e^{-N\eta\alpha^2}, \end{aligned} \quad (\text{D25})$$

where $S_{x_1, \dots, x_{N-1}}^j$ is given in Eq. (D22) and $\theta = \theta_0 - \theta_1$.

2. Computation of $\Pr(\Omega_j | R_{\text{KG}})$

We now calculate the probability that detector D_j clicks in a KG round, i.e.,

$$\begin{aligned} \Pr(\Omega_j | R_{\text{KG}}) &= \frac{1}{2^N} \sum_{(x_0, \dots, x_{N-1}) \in \{1, -1\}^N} \Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{\text{KG}}) \\ &= -(1 - p_d)^M e^{-N\eta\alpha^2} + \frac{(1 - p_d)^{M-1}}{2^N} e^{-(MN-1)\eta\alpha^2/M} \\ &\quad \times \sum_{(x_0, \dots, x_{N-1}) \in \{1, -1\}^N} e^{\eta\alpha^2 \left((S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j x_0 \cos \theta \cos \phi \right) / M}. \end{aligned} \tag{D26}$$

We denote the leftover sum in the last expression as Σ for brevity. Then, we can simplify it as follows:

$$\begin{aligned} \Sigma &= \sum_{(x_1, \dots, x_{N-1}) \in \{1, -1\}^{N-1}} \left(e^{\eta\alpha^2 \left((S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j \cos \theta \cos \phi \right) / M} + e^{\eta\alpha^2 \left((S_{x_1, \dots, x_{N-1}}^j)^2 - 2S_{x_1, \dots, x_{N-1}}^j \cos \theta \cos \phi \right) / M} \right) \\ &= \sum_{(x_1, \dots, x_{N-1}) \in \{1, -1\}^{N-1}} e^{\eta\alpha^2 (S_{x_1, \dots, x_{N-1}}^j)^2 / M} \left(e^{\eta\alpha^2 2S_{x_1, \dots, x_{N-1}}^j \cos \theta \cos \phi / M} + e^{-\eta\alpha^2 2S_{x_1, \dots, x_{N-1}}^j \cos \theta \cos \phi / M} \right) \\ &= 2 \sum_{(x_1, \dots, x_{N-1}) \in \{1, -1\}^{N-1}} e^{\eta\alpha^2 (S_{x_1, \dots, x_{N-1}}^j)^2 / M} \cosh \left(2 \frac{\eta\alpha^2}{M} S_{x_1, \dots, x_{N-1}}^j \cos \theta \cos \phi \right). \end{aligned} \tag{D27}$$

At this point, we define a vector $\vec{y} \in \{1, -1\}^{N-1}$ such that $y_i = x_i f_{i,j}$. Then, we can rewrite $S_{x_1, \dots, x_{N-1}}^j = \sum_i y_i$. Of note, since we sum over all possible vectors (x_1, \dots, x_{N-1}) , we reach all possible values for \vec{y} . This implies that we can recast the sum over (x_1, \dots, x_{N-1}) as a sum over all possible vectors \vec{y} . This has the consequence that the probability of detector D_j clicking is independent of j . With these considerations, we rewrite the last expression as follows:

$$\Sigma = 2 \sum_{\vec{y} \in \{1, -1\}^{N-1}} e^{\eta\alpha^2 (\sum_i y_i)^2 / M} \cosh \left(2 \frac{\eta\alpha^2}{M} \left(\sum_i y_i \right) \cos \theta \cos \phi \right). \tag{D28}$$

Now let us call k the number of ones in the vector \vec{y} . We have that $\sum_i y_i = k - (N - 1 - k) = 2k + 1 - N$. Since there are $\binom{N-1}{k}$ different vectors \vec{y} that have a fixed number k of ones, we can recast the last expression as follows:

$$\Sigma = 2 \sum_{k=0}^{N-1} \binom{N-1}{k} e^{\eta\alpha^2 (2k+1-N)^2 / M} \cosh \left(2 \frac{\eta\alpha^2}{M} (2k + 1 - N) \cos \theta \cos \phi \right). \tag{D29}$$

By inserting the last expression in Eq. (D26), we obtain the final expression for the probability that detector D_j clicks in a KG round:

$$\begin{aligned} \Pr(\Omega_j | R_{\text{KG}}) &= -(1 - p_d)^M e^{-N\eta\alpha^2} + \frac{(1 - p_d)^{M-1}}{2^{N-1}} e^{-(MN-1)\eta\alpha^2/M} \\ &\quad \times \sum_{k=0}^{N-1} \binom{N-1}{k} e^{\eta\alpha^2 (2k+1-N)^2 / M} \cosh \left(2 \frac{\eta\alpha^2}{M} (2k + 1 - N) \cos \theta \cos \phi \right), \end{aligned} \tag{D30}$$

where $\theta = \theta_0 - \theta_1$. As discussed above, the probability that a specific detector clicks is independent of j , as expected given our symmetric channel model.

3. Computation of \mathcal{Q}_{x_0, x_i}^j

The QBER is computed through Eq. (5), which we report here for clarity:

$$\mathcal{Q}_{x_0, x_i}^j = \sum_{x_0 \neq x_i f_{i,j}} \frac{\Pr(\Omega_j | x_0, x_i, R_{KG})}{4 \Pr(\Omega_j | R_{KG})}, \quad (\text{D31})$$

where the only quantity that still needs to be computed is $\Pr(\Omega_j | x_0, x_i, R_{KG})$. By definition, we have

$$\begin{aligned} \Pr(\Omega_j | x_0, x_i, R_{KG}) &= \frac{1}{2^{N-2}} \sum_{(x_1, \dots, \hat{x}_i, \dots, x_{N-1}) \in \{1, -1\}^{N-2}} \Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{KG}) \\ &= -(1-p_d)^M e^{-N\eta\alpha^2} + \frac{(1-p_d)^{M-1}}{2^{N-2}} e^{-(MN-1)\eta\alpha^2/M} \\ &\quad \times \sum_{(x_1, \dots, \hat{x}_i, \dots, x_{N-1}) \in \{1, -1\}^{N-2}} e^{\eta\alpha^2 \left((S_{x_1, \dots, x_{N-1}}^j)^2 + 2S_{x_1, \dots, x_{N-1}}^j x_0 \cos \theta \cos \phi \right) / M}, \end{aligned} \quad (\text{D32})$$

where $(x_1, \dots, \hat{x}_i, \dots, x_{N-1})$ are $(N-2)$ -dimensional vectors where the i th element is removed. Then, we can define a vector $\vec{y} \in \{1, -1\}^{N-1}$ with $y_l = x_l f_{l,j}$ for $l \neq i$ and $y_i = 0$, such that $S_{x_1, \dots, x_{N-1}}^j = \sum_l y_l + x_i f_{i,j}$. Since the sum in the last expression runs over all vectors $(x_1, \dots, \hat{x}_i, \dots, x_{N-1})$, we can reach all possible choices of \vec{y} , meaning that we can recast the sum as a sum over all possible choices of \vec{y} . With these considerations, we recast Eq. (D32) as follows:

$$\begin{aligned} \Pr(\Omega_j | x_0, x_i, R_{KG}) &= -(1-p_d)^M e^{-N\eta\alpha^2} + \frac{(1-p_d)^{M-1}}{2^{N-2}} e^{-(MN-1)\eta\alpha^2/M} \\ &\quad \times \sum_{\substack{\vec{y} \in \{1, -1\}^{N-1}: \\ y_i = 0}} e^{\eta\alpha^2 \left((\sum_l y_l + x_i f_{i,j})^2 + 2(\sum_l y_l + x_i f_{i,j}) x_0 \cos \theta \cos \phi \right) / M}. \end{aligned} \quad (\text{D33})$$

We label the sum as Σ' and focus on it

$$\begin{aligned} \Sigma' &= \sum_{\substack{\vec{y} \in \{1, -1\}^{N-1}: \\ y_i = 0}} e^{\eta\alpha^2 \left((\sum_l y_l)^2 + 1 + 2x_i f_{i,j} \sum_l y_l + 2x_i f_{i,j} x_0 \cos \theta \cos \phi + 2x_0 \cos \theta \cos \phi \sum_l y_l \right) / M} \\ &= e^{\eta\alpha^2 (1 + 2x_0 x_i f_{i,j} \cos \theta \cos \phi) / M} \sum_{\substack{\vec{y} \in \{1, -1\}^{N-1}: \\ y_i = 0}} e^{\eta\alpha^2 \left((\sum_l y_l)^2 + 2 \sum_l y_l (x_i f_{i,j} + x_0 \cos \theta \cos \phi) \right) / M}. \end{aligned} \quad (\text{D34})$$

By replicating the argument in the calculation of $\Pr(\Omega_j | R_{KG})$, we can replace the sum over \vec{y} with a sum over k , which is the number of ones in \vec{y} :

$$\Sigma' = e^{\eta\alpha^2 (1 + 2x_0 x_i f_{i,j} \cos \theta \cos \phi) / M} \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2 (2k+2-N)^2 / M} e^{2\eta\alpha^2 (2k+2-N) (x_i f_{i,j} + x_0 \cos \theta \cos \phi) / M}. \quad (\text{D35})$$

By inserting this in Eq. (D33), we obtain the final expression for the probability that detector D_j clicks, given that party A_0 (A_i) prepared coherent state $|x_0\alpha\rangle$ ($|x_i\alpha\rangle$):

$$\begin{aligned} \Pr(\Omega_j | x_0, x_i, R_{KG}) &= -(1-p_d)^M e^{-N\eta\alpha^2} + \frac{(1-p_d)^{M-1}}{2^{N-2}} e^{-(MN-2-2x_0 x_i f_{i,j} \cos \theta \cos \phi)\eta\alpha^2 / M} \\ &\quad \times \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2 (2k+2-N)^2 / M} e^{2\eta\alpha^2 (2k+2-N) (x_i f_{i,j} + x_0 \cos \theta \cos \phi) / M}. \end{aligned} \quad (\text{D36})$$

With Eq. (D36) we can finally compute the QBER as follows:

$$\begin{aligned}
 \mathcal{Q}_{X_0, X_i}^j &= \sum_{x_0 \neq x_i / i, j} \frac{\Pr(\Omega_j | x_0, x_i, R_{\text{KG}})}{4 \Pr(\Omega_j | R_{\text{KG}})} = \frac{-(1-p_d)^M e^{-N\eta\alpha^2}}{2 \Pr(\Omega_j | R_{\text{KG}})} + \frac{(1-p_d)^{M-1}}{2^N \Pr(\Omega_j | R_{\text{KG}})} e^{-(MN-2+2\cos\theta\cos\phi)\eta\alpha^2/M} \\
 &\quad \times \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2(2k+2-N)^2/M} \\
 &\quad \times \left(e^{2\eta\alpha^2(2k+2-N)(1-\cos\theta\cos\phi)/M} + e^{-2\eta\alpha^2(2k+2-N)(1-\cos\theta\cos\phi)/M} \right) \\
 &= \frac{-(1-p_d)^M e^{-N\eta\alpha^2}}{2 \Pr(\Omega_j | R_{\text{KG}})} + \frac{(1-p_d)^{M-1}}{2^{N-1} \Pr(\Omega_j | R_{\text{KG}})} e^{-(MN-2+2\cos\theta\cos\phi)\eta\alpha^2/M} \\
 &\quad \times \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2(2k+2-N)^2/M} \cosh\left(2\frac{\eta\alpha^2}{M}(2k+2-N)(1-\cos\theta\cos\phi)\right), \tag{D37}
 \end{aligned}$$

which is also independent of j ($\Pr(\Omega_j | R_{\text{KG}})$ is independent of j , see Eq. (D30)), as well as i , due to the symmetry of the considered noise model.

4. Computation of $\Pr(\Omega_j | \beta_0, \beta_1, \dots, \beta_{N-1})$

We now calculate the gains, i.e., the probability that only detector D_j clicks in a PE round where the parties prepared phase-randomized coherent states with intensities $\beta_0, \beta_1, \dots, \beta_{N-1}$. We recall that the state (1) sent by party A_i can be equivalently described as follows:

$$\rho_{a_i}(\beta_i) = \frac{1}{2\pi} \int_0^{2\pi} d\varphi_i |\sqrt{\beta_i} e^{i\varphi_i}\rangle \langle \sqrt{\beta_i} e^{i\varphi_i}|, \tag{D38}$$

where $\beta_i \in \mathcal{S}_i$. Thus, the state sent by all parties reads

$$\rho_{\text{in}} = \bigotimes_{i=0}^{N-1} \rho_{a_i}(\beta_i) = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \cdots d\varphi_{N-1} \bigotimes_{i=0}^{N-1} |\sqrt{\beta_i} e^{i\varphi_i}\rangle \langle \sqrt{\beta_i} e^{i\varphi_i}|. \tag{D39}$$

We now apply our channel model comprising a pure-loss channel and a polarization misalignment (we neglect the phase shift as the states are already phase randomized). After going through the lossy and noisy channel, ρ_{in} evolves to

$$\begin{aligned}
 \rho'_{\text{in}} &= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \cdots d\varphi_{N-1} \bigotimes_{i=0}^{N-1} |\cos\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}\rangle \langle \cos\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}|_P \\
 &\quad \otimes |-\sin\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}\rangle \langle -\sin\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}|_{P_\perp}. \tag{D40}
 \end{aligned}$$

The final step consists in evolving ρ'_{in} through the BBS network. We obtain the following state:

$$\begin{aligned}
 \rho_{\text{out}} &= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \cdots d\varphi_{N-1} \bigotimes_{k=0}^{M-1} \left| \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right\rangle \left\langle \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|_P \\
 &\quad \otimes \left| -\sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right\rangle \left\langle -\sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|_{P_\perp}, \tag{D41}
 \end{aligned}$$

which we remark is not anymore a product state of phase-randomized coherent states. Now, similarly to the calculation of $\Pr(\Omega_j | x_0, \dots, x_{N-1}, R_{KG})$, we can express each gain as follows:

$$\Pr(\Omega_j | \beta_0, \beta_1, \dots, \beta_{N-1}) = (1 - p_d)^{M-1} \text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] - (1 - p_d)^M \text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right], \quad (\text{D42})$$

where $|0\rangle\langle 0|_k$ is the projector on the vacuum of the output mode k for polarizations P and P_\perp , since the detectors do not distinguish polarization. We now evaluate the two terms in Eq. (D42). Let us begin with the second, i.e.,

$$\begin{aligned} \text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] &= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \dots d\varphi_{N-1} \\ &\times \prod_{k=0}^{M-1} \left| \langle 0 | \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \left| \langle 0 | -\sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \\ &= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \dots d\varphi_{N-1} \\ &\times \prod_{k=0}^{M-1} \exp \left[- \left| \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 - \left| \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \right] \\ &= \int_0^{2\pi} \frac{d\varphi_0 \dots d\varphi_{N-1}}{(2\pi)^N} \exp \left[-\frac{\eta}{M} \sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} f_{i,k} \cos \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \left| \sum_{i=0}^{N-1} f_{i,k} \sin \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \right) \right] \\ &\equiv \int_0^{2\pi} \frac{d\varphi_0 \dots d\varphi_{N-1}}{(2\pi)^N} e^{-\frac{\eta}{M} \sum_{k=0}^{M-1} C_k}. \end{aligned} \quad (\text{D43})$$

Let us now focus on the sum of the terms labeled C_k . By expanding the squares in C_k we obtain

$$\begin{aligned} \sum_{k=0}^{M-1} C_k &= \sum_{k=0}^{M-1} \left(\sum_{i=0}^{N-1} \left| f_{i,k} \cos \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \sum_{\substack{i,i'=0 \\ i \neq i'}}^{N-1} f_{i,k} f_{i',k} \cos \theta_i \cos \theta_{i'} \sqrt{\beta_i \beta_{i'}} e^{i(\varphi_i - \varphi_{i'})} \right. \\ &\quad \left. + \sum_{i=0}^{N-1} \left| f_{i,k} \sin \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \sum_{\substack{i,i'=0 \\ i \neq i'}}^{N-1} f_{i,k} f_{i',k} \sin \theta_i \sin \theta_{i'} \sqrt{\beta_i \beta_{i'}} e^{i(\varphi_i - \varphi_{i'})} \right) \\ &= \sum_{k=0}^{M-1} \left(\sum_{i=0}^{N-1} \cos^2 \theta_i \beta_i + 2 \sum_{\substack{i,i'=0 \\ i < i'}}^{N-1} f_{i,k} f_{i',k} \cos \theta_i \cos \theta_{i'} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right. \\ &\quad \left. + \sum_{i=0}^{N-1} \sin^2 \theta_i \beta_i + 2 \sum_{\substack{i,i'=0 \\ i < i'}}^{N-1} f_{i,k} f_{i',k} \sin \theta_i \sin \theta_{i'} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right). \end{aligned} \quad (\text{D44})$$

Now, we use the result in Eq. (D16) (derived from Lemma 3) to argue that

$$\begin{aligned} \sum_{k=0}^{M-1} f_{i,k} f_{i',k} &= \sum_{k=0}^{M-1} (-1)^{(\vec{i}+\vec{i}')\cdot\vec{k}} \\ &= M \delta_{\vec{i}\vec{i}'} \end{aligned} \tag{D45}$$

By applying this result in Eq. (D44), and by noting that \vec{i} and \vec{i}' must differ in the sums that involve them, we are left with

$$\sum_{k=0}^{M-1} C_k = \sum_{k=0}^{M-1} \left(\sum_{i=0}^{N-1} \beta_i \cos \theta_i^2 + \sum_{i=0}^{N-1} \beta_i \sin \theta_i^2 \right) = M \sum_{i=0}^{N-1} \beta_i \tag{D46}$$

By using this result in Eq. (D43), we can directly integrate over the phases and obtain the following expression for the second term in Eq. (D42):

$$\text{Tr} \left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] = e^{-\eta \sum_i \beta_i} \tag{D47}$$

Regarding the first term in Eq. (D42), we can express it as follows:

$$\begin{aligned} \text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] &= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \dots d\varphi_{N-1} e^{-\eta/M \sum_{k=0, k \neq j}^{M-1} C_k} \\ &= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \dots d\varphi_{N-1} e^{-\eta/M (\sum_{k=0}^{M-1} C_k - C_j)} \\ &= e^{-\eta \sum_i \beta_i} \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \dots d\varphi_{N-1} e^{\eta C_j / M} \end{aligned} \tag{D48}$$

Now we calculate the coefficient C_j by expanding its squares:

$$\begin{aligned} C_j &= \left| \sum_{i=0}^{N-1} f_{i,j} \cos \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \left| \sum_{i=0}^{N-1} f_{i,j} \sin \theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \\ &= \sum_{i=0}^{N-1} \beta_i + 2 \sum_{\substack{i,i'=0 \\ i < i'}}^{N-1} f_{i,j} f_{i',j} (\cos \theta_i \cos \theta_{i'} + \sin \theta_i \sin \theta_{i'}) \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \\ &= \sum_{i=0}^{N-1} \beta_i + 2 \sum_{\substack{i,i'=0 \\ i < i'}}^{N-1} f_{i,j} f_{i',j} \cos(\theta_i - \theta_{i'}) \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \end{aligned} \tag{D49}$$

Now we use the fact that $\theta_i = \theta_1$ for every $i \geq 1$. By splitting the second sum into two terms, where the first has $i = 0$ fixed and in the second $i \geq 1$, we obtain

$$C_j = \sum_{i=0}^{N-1} \beta_i + 2 \cos \theta \sum_{i=1}^{N-1} f_{i,j} \sqrt{\beta_0 \beta_i} \cos(\varphi_0 - \varphi_i) + 2 \sum_{\substack{i,i'=1 \\ i < i'}}^{N-1} f_{i,j} f_{i',j} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}), \tag{D50}$$

where $\theta = \theta_0 - \theta_1$. By using this expression in Eq. (D48), we obtain the following expression for the first term in Eq. (D42):

$$\text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] = e^{-\eta(1-1/M) \sum_i \beta_i} I_j(\beta_0, \dots, \beta_{N-1}), \tag{D51}$$

where we define the integral:

$$I_j(\beta_0, \dots, \beta_{N-1}) := \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \dots d\varphi_{N-1} \times \exp \left[\frac{2\eta}{M} \left(\cos \theta \sum_{i=1}^{N-1} f_{ij} \sqrt{\beta_0 \beta_i} \cos(\varphi_0 - \varphi_i) + \sum_{\substack{i,i'=1 \\ i < i'}}^{N-1} f_{ij} f_{i'j} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right) \right]. \quad (\text{D52})$$

By employing Eqs. (D51) and (D47) in Eq. (D42), we obtain the following compact expression for the gains:

$$\Pr(\Omega_j | \beta_0, \beta_1, \dots, \beta_{N-1}) = (1 - p_d)^{M-1} e^{-\eta(1-1/M) \sum_i \beta_i} I_j(\beta_0, \dots, \beta_{N-1}) - (1 - p_d)^M e^{-\eta \sum_i \beta_i}, \quad (\text{D53})$$

where $I_j(\beta_0, \dots, \beta_{N-1})$ is given in Eq. (D52).

Of note, due to our symmetric channel model, the gains are independent of which detector D_j clicks. To show this, we argue that the integral in Eq. (D52) is actually independent of j . To this aim, we label the function to be integrated in Eq. (D52) as follows:

$$F_j(\varphi_0, \dots, \varphi_{N-1}) := \exp \left[\frac{2\eta}{M} \left(\cos \theta \sum_{i=1}^{N-1} (-1)^{\vec{i} \cdot \vec{j}} \sqrt{\beta_0 \beta_i} \cos(\varphi_0 - \varphi_i) + \sum_{\substack{i,i'=1 \\ i < i'}}^{N-1} (-1)^{(\vec{i} + \vec{i}') \cdot \vec{j}} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right) \right] \quad (\text{D54})$$

and observe that this function is periodic in each variable φ_i , with period 2π . The only dependency of F_j on j comes from the ± 1 signs inside the sums. We can reabsorb such signs by defining alternative integration variables $\Phi_i := \varphi_i - \pi \cdot (\vec{i} \cdot \vec{j})$, which allow us to simplify the summands as follows:

$$(-1)^{\vec{i} \cdot \vec{j}} \cos(\varphi_0 - \varphi_i) = \cos(\Phi_0 - \Phi_i), \quad (\text{D55})$$

$$(-1)^{(\vec{i} + \vec{i}') \cdot \vec{j}} \cos(\varphi_i - \varphi_{i'}) = (-1)^{\vec{i} \cdot \vec{j} - \vec{i}' \cdot \vec{j}} \cos(\varphi_i - \varphi_{i'}) = \cos(\Phi_i - \Phi_{i'}). \quad (\text{D56})$$

Then, by performing the change of variable $\Phi_i := \varphi_i - \pi \cdot (\vec{i} \cdot \vec{j})$ in the integral and by using the fact that the function F_j is periodic in each variable, we obtain

$$I_j(\beta_0, \dots, \beta_{N-1}) = \frac{1}{(2\pi)^N} \int_{-\pi(\vec{i} \cdot \vec{j})}^{2\pi - \pi(\vec{i} \cdot \vec{j})} d\Phi_0 d\Phi_1 \dots d\Phi_{N-1} F_0(\Phi_0, \Phi_1, \dots, \Phi_{N-1}) = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\Phi_0 d\Phi_1 \dots d\Phi_{N-1} F_0(\Phi_0, \Phi_1, \dots, \Phi_{N-1}) = I_0(\beta_0, \dots, \beta_{N-1}), \quad (\text{D57})$$

which confirms that I_j is independent of j . The final formula for the gains is thus

$$\Pr(\Omega_j | \beta_0, \beta_1, \dots, \beta_{N-1}) = (1 - p_d)^{M-1} e^{-\eta(1-1/M) \sum_i \beta_i} I(\beta_0, \dots, \beta_{N-1}) - (1 - p_d)^M e^{-\eta \sum_i \beta_i}, \quad (\text{D58})$$

where the integral

$$I(\beta_0, \dots, \beta_{N-1}) = \int_0^{2\pi} \frac{d\varphi_0 \dots d\varphi_{N-1}}{(2\pi)^N} \exp \left[\frac{2\eta}{M} \left(\cos \theta \sum_{i=1}^{N-1} \sqrt{\beta_0 \beta_i} \cos(\varphi_0 - \varphi_i) + \sum_{\substack{i,i'=1 \\ i < i'}}^{N-1} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right) \right], \quad (\text{D59})$$

is evaluated numerically in our simulations. Note that we freely relabeled the variables in the integral back to φ_i .

5. Computation of $\Pr(\Omega_j | n_0, \dots, n_{N-1})$

Here we calculate the analytical expression of any yield $Y_{n_0, \dots, n_{N-1}}^j$, defined in Eq. (6) as the probability that detector D_j clicks given the hypothetical scenario in which party A_i sent exactly n_i photons.

We remark that in an experiment the parties cannot, in general, learn the exact value of each yield with the decoy-state analysis, but can derive upper bounds as shown in Appendix C. In the limit of an infinite number of decoy intensities, the yields' upper bounds would tend to the exact values computed here.

To evaluate $Y_{n_0, \dots, n_{N-1}}^j$, we consider the scenario in which the parties send the state $\bigotimes_{i=0}^{N-1} |n_i\rangle$, where $|n_i\rangle$ is a Fock state of n_i photons. The state can be written as

$$|\xi(n_0, \dots, n_{N-1})\rangle = \left(\prod_{i=0}^{N-1} \frac{(\hat{a}_i^\dagger)^{n_i}}{\sqrt{n_i!}} \right) |0\rangle, \quad (\text{D60})$$

where \hat{a}_i^\dagger is the creation operator of the optical mode of party A_i and $|0\rangle$ represents the vacuum state on all modes. We now introduce, step by step, the effect of all sources of noise and then apply the BBS network.

The lossy channel transforms each party's mode according to

$$\hat{a}_i^\dagger \rightarrow \sqrt{\eta} \hat{a}_i^\dagger + \sqrt{1-\eta} \hat{l}_i^\dagger, \quad (\text{D61})$$

where \hat{l}_i^\dagger is the creation operator of the loss mode of party A_i . The input state $|\xi\rangle$ is transformed as follows:

$$\begin{aligned} |\xi'(n_0, \dots, n_{N-1})\rangle &= \left(\prod_{i=0}^{N-1} \frac{(\sqrt{\eta} \hat{a}_i^\dagger + \sqrt{1-\eta} \hat{l}_i^\dagger)^{n_i}}{\sqrt{n_i!}} \right) |0\rangle \\ &= \left[\prod_{i=0}^{N-1} \left(\sum_{k_i=0}^{n_i} \binom{n_i}{k_i} \frac{\eta^{k_i/2} (1-\eta)^{(n_i-k_i)/2}}{\sqrt{n_i!}} (\hat{a}_i^\dagger)^{k_i} (\hat{l}_i^\dagger)^{n_i-k_i} \right) \right] |0\rangle \\ &= \sum_{k_0=0}^{n_0} \dots \sum_{k_{N-1}=0}^{n_{N-1}} \binom{n_0}{k_0} \dots \binom{n_{N-1}}{k_{N-1}} \frac{\eta^{\sum_i k_i/2} (1-\eta)^{\sum_i (n_i-k_i)/2}}{\sqrt{n_0! \dots n_{N-1}!}} \sqrt{(n_0-k_0)! \dots (n_{N-1}-k_{N-1})!} \\ &\quad \times \left[\prod_{i=0}^{N-1} (\hat{a}_i^\dagger)^{k_i} \right] |0\rangle_{a_0, \dots, a_{N-1}} \otimes |n_0-k_0\rangle_{l_0} \otimes \dots \otimes |n_{N-1}-k_{N-1}\rangle_{l_{N-1}}, \end{aligned} \quad (\text{D62})$$

where we just use the binomial expansion in the second line and where a_i and l_i are used to indicate the optical mode and the loss mode of party A_i , respectively.

We now note that the loss modes are not observed by the parties and thus need to be traced out. The density matrix $\rho' = |\xi'\rangle\langle\xi'|$ will thus have two sets of indices (k_0, \dots, k_{N-1}) and (k'_0, \dots, k'_{N-1}) . However, it is immediate to see from Eq. (D62) that tracing out the loss modes will impose the conditions $k_i = k'_i \forall i$. Thus we are left with the state

$$\begin{aligned} \rho' &= \sum_{k_0=0}^{n_0} \dots \sum_{k_{N-1}=0}^{n_{N-1}} \binom{n_0}{k_0}^2 \dots \binom{n_{N-1}}{k_{N-1}}^2 \frac{\eta^{\sum_i k_i} (1-\eta)^{\sum_i (n_i-k_i)} (n_0-k_0)! \dots (n_{N-1}-k_{N-1})!}{n_0! \dots n_{N-1}!} \\ &\quad \times \left[\prod_{i=0}^{N-1} (\hat{a}_i^\dagger)^{k_i} \right] |0\rangle\langle 0|_{a_0, \dots, a_{N-1}} \left[\prod_{i=0}^{N-1} (\hat{a}_i)^{k_i} \right] \\ &= \sum_{k_0=0}^{n_0} \dots \sum_{k_{N-1}=0}^{n_{N-1}} \binom{n_0}{k_0} \dots \binom{n_{N-1}}{k_{N-1}} \frac{\eta^{\sum_i k_i} (1-\eta)^{\sum_i (n_i-k_i)}}{k_0! \dots k_{N-1}!} \left[\prod_{i=0}^{N-1} (\hat{a}_i^\dagger)^{k_i} \right] |0\rangle\langle 0|_{a_0, \dots, a_{N-1}} \left[\prod_{i=0}^{N-1} (\hat{a}_i)^{k_i} \right], \end{aligned} \quad (\text{D63})$$

where we use the fact that $(n_i - k_i)!/n_i! = 1/\binom{n_i}{k_i} k_i!$ and where, from now on, for simplicity of notation we neglect the explicit dependence of the state on n_0, \dots, n_{N-1} .

We now introduce the polarization misalignment, while we skip the phase misalignment since its effect cancels out on tensor products of Fock states. The polarization misalignment acts on the creation operators of each mode as follows:

$$\hat{a}_i^\dagger \rightarrow \cos \theta_i \hat{a}_{i,P}^\dagger - \sin \theta_i \hat{a}_{i,\perp}^\dagger, \quad (\text{D64})$$

where we recall that in our channel model we set $\theta_i = \theta_1$ for $i \geq 1$, i.e., we introduce only a misalignment between the reference party A_0 and the other parties. For simplicity of notation we omit the label P and consider the polarization P to be the input polarization and label the orthogonal polarization with \perp . By applying the above transformation to the creation operators in Eq. (D63) and by using again the binomial expansion we obtain

$$\begin{aligned} \prod_{i=0}^{N-1} \left(\cos \theta_i \hat{a}_i^\dagger - \sin \theta_i \hat{a}_{i,\perp}^\dagger \right)^{k_i} &= \prod_{i=0}^{N-1} \left(\sum_{l_i=0}^{k_i} (-1)^{k_i-l_i} \binom{k_i}{l_i} (\cos \theta_i)^{l_i} (\sin \theta_i)^{k_i-l_i} (\hat{a}_i^\dagger)^{l_i} (\hat{a}_{i,\perp}^\dagger)^{k_i-l_i} \right) \\ &= \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} (-1)^{\sum_i (k_i-l_i)} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} (\cos \theta_0)^{l_0} \\ &\quad \times (\sin \theta_0)^{k_0-l_0} (\cos \theta_1)^{\sum_{i=1}^{N-1} l_i} (\sin \theta_1)^{\sum_{i=1}^{N-1} (k_i-l_i)} \left[\prod_{i=0}^{N-1} (\hat{a}_i^\dagger)^{l_i} (\hat{a}_{i,\perp}^\dagger)^{k_i-l_i} \right]. \end{aligned} \quad (\text{D65})$$

By using this expression in Eq. (D63), we obtain

$$\begin{aligned} \rho'' &= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} \sum_{l'_0=0}^{k_0} \cdots \sum_{l'_{N-1}=0}^{k_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \binom{k_0}{l'_0} \cdots \binom{k_{N-1}}{l'_{N-1}} \\ &\quad \times (-1)^{\sum_i (2k_i-l_i-l'_i)} \frac{\eta^{\sum_i k_i} (1-\eta)^{\sum_i (n_i-k_i)}}{k_0! \cdots k_{N-1}!} \times (\cos \theta_0)^{l_0+l'_0} (\sin \theta_0)^{2k_0-l_0-l'_0} (\cos \theta_1)^{\sum_{i=1}^{N-1} (l_i+l'_i)} (\sin \theta_1)^{\sum_{i=1}^{N-1} (2k_i-l_i-l'_i)} \\ &\quad \times \left[\prod_{i=0}^{N-1} (\hat{a}_i^\dagger)^{l_i} (\hat{a}_{i,\perp}^\dagger)^{k_i-l_i} \right] |0\rangle \langle 0|_{a_0, \dots, a_{N-1}, a_{0,\perp}, \dots, a_{N-1,\perp}} \left[\prod_{i=0}^{N-1} (\hat{a}_i)^{l'_i} (\hat{a}_{i,\perp})^{k_i-l'_i} \right]. \end{aligned} \quad (\text{D66})$$

We now let the state evolve through the optical setup of the BBS network. The resulting transformation of the incoming creation operators is given in Eq. (3), as proved in Appendix A. This brings us to the following state of the output modes in the BBS network:

$$\begin{aligned} \rho_{\text{out}} &= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} \sum_{l'_0=0}^{k_0} \cdots \sum_{l'_{N-1}=0}^{k_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \binom{k_0}{l'_0} \cdots \binom{k_{N-1}}{l'_{N-1}} \\ &\quad \times (-1)^{\sum_i (2k_i-l_i-l'_i)} \frac{\eta^{\sum_i k_i} (1-\eta)^{\sum_i (n_i-k_i)}}{k_0! \cdots k_{N-1}!} (\cos \theta_0)^{l_0+l'_0} (\sin \theta_0)^{2k_0-l_0-l'_0} (\cos \theta_1)^{\sum_{i=1}^{N-1} (l_i+l'_i)} (\sin \theta_1)^{\sum_{i=1}^{N-1} (2k_i-l_i-l'_i)} \\ &\quad \times \left[\prod_{i=0}^{N-1} \left(\frac{1}{\sqrt{M}} \sum_{s=0}^{M-1} (-1)^{\bar{s} \cdot \bar{i}} \hat{a}_s^\dagger \right)^{l_i} \left(\frac{1}{\sqrt{M}} \sum_{s'=0}^{M-1} (-1)^{\bar{s}' \cdot \bar{i}} \hat{a}_{s',\perp}^\dagger \right)^{k_i-l_i} \right] |0\rangle \langle 0|_{d_0, \dots, d_{N-1}, d_{0,\perp}, \dots, d_{N-1,\perp}} \\ &\quad \times \left[\prod_{i=0}^{N-1} \left(\frac{1}{\sqrt{M}} \sum_{q=0}^{M-1} (-1)^{\bar{q} \cdot \bar{i}} \hat{a}_q \right)^{l'_i} \left(\frac{1}{\sqrt{M}} \sum_{q'=0}^{M-1} (-1)^{\bar{q}' \cdot \bar{i}} \hat{a}_{q',\perp} \right)^{k_i-l'_i} \right]. \end{aligned} \quad (\text{D67})$$

From the definition of yields, $Y_{n_0, \dots, n_{N-1}}^j = \Pr(\Omega_j | n_0, \dots, n_{N-1})$, we can express them as follows by including dark counts (each detector has a probability p_d of a dark count):

$$Y_{n_0, \dots, n_{N-1}}^j = (1-p_d)^{M-1} \text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{r \neq j}^{M-1} |0\rangle \langle 0|_r \right] - (1-p_d)^M \text{Tr} \left[\rho_{\text{out}} \bigotimes_{r=0}^{M-1} |0\rangle \langle 0|_r \right], \quad (\text{D68})$$

where the identity operator and the projector on the vacuum are defined on both modes of polarization, since the detectors cannot distinguish them. We note that calculating the second trace in Eq. (D68) is trivial: projecting all modes onto the vacuum forces all indexes to be equal to zero, thus yielding the result:

$$\text{Tr} \left[\rho_{\text{out}} \bigotimes_{r=0}^{M-1} |0\rangle\langle 0|_r \right] = (1 - \eta)^{\sum_i n_i}. \tag{D69}$$

In order to calculate the first trace in Eq. (D68), we would need to expand the sums over the detectors' creation modes using multinomial expansions. However, since we need to project onto the vacuum state in all modes except modes d_j and $d_{j,\perp}$, this operation will force all the terms in the multinomial expansion to vanish, except for the terms containing \hat{d}_j or $\hat{d}_{j,\perp}$. Therefore, the reduced state of ρ_{out} after projecting onto the vacuum all modes except the j th mode, $\rho_{\text{out}}^{(j)} := \langle 0_1, \dots, 0_{j-1}, 0_{j+1}, \dots, 0_{M-1} | \rho_{\text{out}} | 0_1, \dots, 0_{j-1}, 0_{j+1}, \dots, 0_{M-1} \rangle$, reads

$$\begin{aligned} \rho_{\text{out}}^{(j)} &= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \cdots \binom{k_{N-1}}{l'_{N-1}} \\ &\times (-1)^{\sum_i (2k_i - l_i - l'_i)} \frac{\eta^{\sum_i k_i} (1 - \eta)^{\sum_i (n_i - k_i)}}{k_0! \cdots k_{N-1}!} (\cos \theta_0)^{l_0 + l'_0} (\sin \theta_0)^{2k_0 - l_0 - l'_0} (\cos \theta_1)^{\sum_{i=1}^{N-1} (l_i + l'_i)} (\sin \theta_1)^{\sum_{i=1}^{N-1} (2k_i - l_i - l'_i)} \\ &\times \left[\prod_{i=0}^{N-1} \left(\frac{(-1)^{\bar{j} \cdot i}}{\sqrt{M}} \right)^{k_i} (\hat{d}_j^\dagger)^{l_i} (\hat{d}_{j,\perp}^\dagger)^{k_i - l_i} \right] |0\rangle\langle 0|_{d_j, d_{j,\perp}} \left[\prod_{i=0}^{N-1} \left(\frac{(-1)^{\bar{j} \cdot i}}{\sqrt{M}} \right)^{k_i} (\hat{d}_j)^{l'_i} (\hat{d}_{j,\perp})^{k_i - l'_i} \right] \\ &= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} \sum_{l'_0=0}^{k_0} \cdots \sum_{l'_{N-1}=0}^{k_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \cdots \binom{k_{N-1}}{l'_{N-1}} \\ &\times (-1)^{\sum_i (2k_i - l_i - l'_i)} \frac{\eta^{\sum_i k_i} (1 - \eta)^{\sum_i (n_i - k_i)}}{M^{\sum_i k_i} k_0! \cdots k_{N-1}!} (\cos \theta_0)^{l_0 + l'_0} (\sin \theta_0)^{2k_0 - l_0 - l'_0} (\cos \theta_1)^{\sum_{i=1}^{N-1} (l_i + l'_i)} (\sin \theta_1)^{\sum_{i=1}^{N-1} (2k_i - l_i - l'_i)} \\ &\times \left[(\hat{d}_j^\dagger)^{\sum_i l_i} (\hat{d}_{j,\perp}^\dagger)^{\sum_i (k_i - l_i)} \right] |0\rangle\langle 0|_{d_j, d_{j,\perp}} \left[(\hat{d}_j)^{\sum_i l'_i} (\hat{d}_{j,\perp})^{\sum_i (k_i - l'_i)} \right], \tag{D70} \end{aligned}$$

where we use the fact that $\left((-1)^{\bar{j} \cdot i} \right)^{2 \sum_i k_i} = 1$. We observe that, as expected, the yields do not depend on j , i.e., on the detector that clicked, due to our symmetric channel model.

We can now compute the first trace in Eq. (D68) by simply taking the trace of $\rho_{\text{out}}^{(j)}$. We note that this forces the identity $\sum_i l_i = \sum_i l'_i$ on the indexes, allowing us to obtain the following expression:

$$\text{Tr} \left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{r \neq j}^{M-1} |0\rangle\langle 0|_r \right] = \text{Tr}[\rho_{\text{out}}^{(j)}] = \mathcal{Q}(n_0, \dots, n_{N-1}), \tag{D71}$$

where we define

$$\begin{aligned} \mathcal{Q}(n_0, \dots, n_{N-1}) &= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{(l_0, \dots, l_{N-1}, l'_0, \dots, l'_{N-1}) \in \mathcal{L}(k_0, \dots, k_{N-1})} \\ &\times \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \binom{k_0}{l'_0} \cdots \binom{k_{N-1}}{l'_{N-1}} \\ &\times \frac{\eta^{\sum_i k_i} (1 - \eta)^{\sum_i (n_i - k_i)}}{M^{\sum_i k_i} k_0! \cdots k_{N-1}!} (\cos \theta_0)^{l_0 + l'_0} (\sin \theta_0)^{2k_0 - l_0 - l'_0} \\ &\times (\cos \theta_1)^{\sum_{i=1}^{N-1} (l_i + l'_i)} (\sin \theta_1)^{\sum_{i=1}^{N-1} (2k_i - l_i - l'_i)} \left(\sum_i l_i \right)! \left(\sum_i (k_i - l_i) \right)!, \tag{D72} \end{aligned}$$

where the summation set is defined as

$$\mathcal{L}(k_0, \dots, k_{N-1}) := \left\{ (l_0, \dots, l_{N-1}, l'_0, \dots, l'_{N-1}) : 0 \leq l_i \leq k_i, 0 \leq l'_i \leq k_i, \sum_{i=0}^{N-1} l_i = \sum_{i=0}^{N-1} l'_i \right\}. \quad (\text{D73})$$

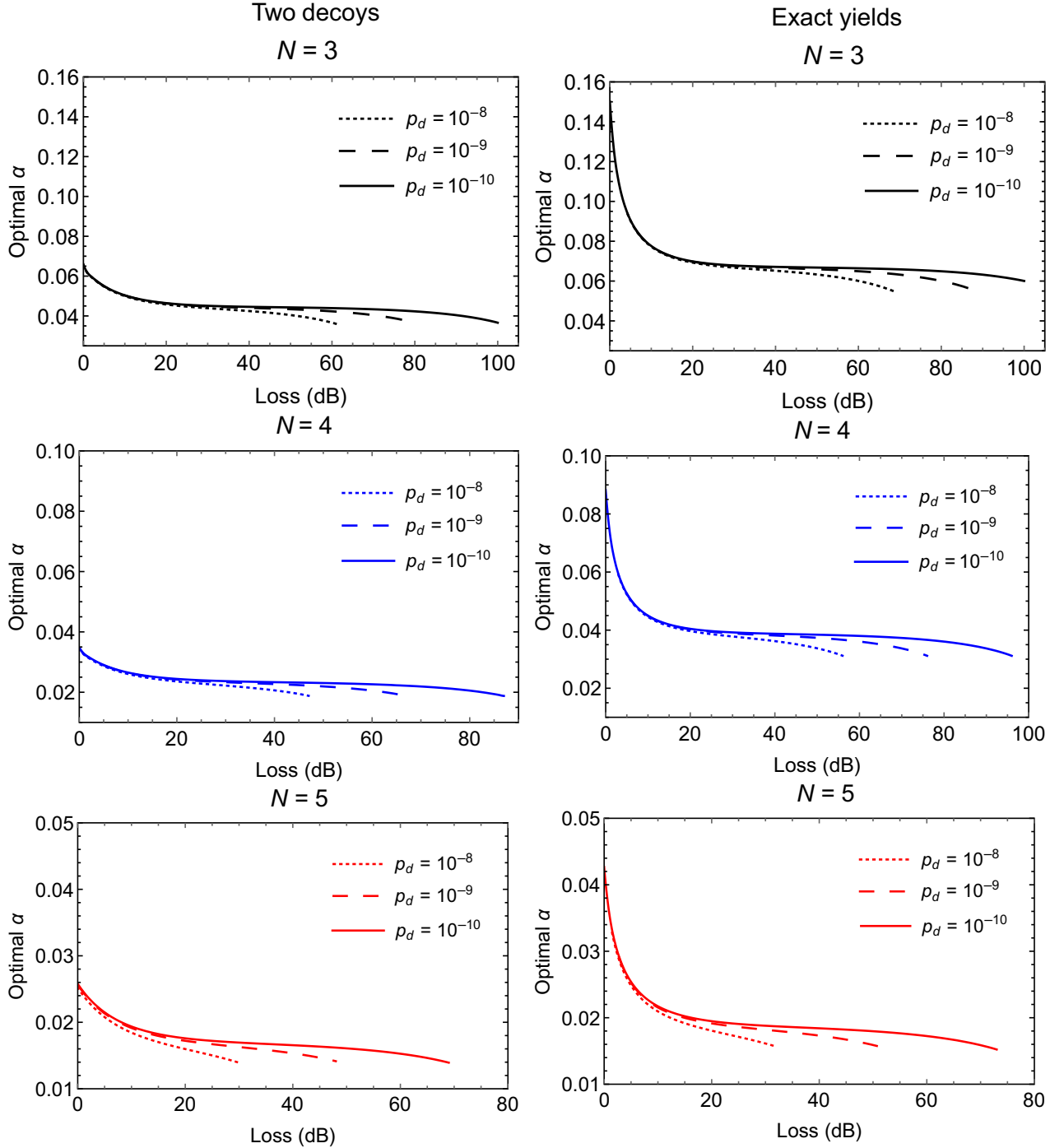


FIG. 5. The optimal value of the signal amplitude (α) that maximizes the key rate plotted in Fig. 4, for different values of the dark-count probability (p_d) and number of parties (N). On the left, the key rate is computed by using the analytical bounds on the yields (34) in the phase error rate bound (7), while the plots on the right use the exact expressions of the yields for our channel model (D74). We observe that a tighter bound on the yields allows for a higher value of α and leads to a higher key rate (see Fig. 4).

By using Eqs. (D69) and (D71) in Eq. (D68), we obtain the final expression for the yields in our channel model:

$$Y_{n_0, \dots, n_{N-1}}^j = (1 - p_d)^{M-1} Q(n_0, \dots, n_{N-1}) - (1 - p_d)^M (1 - \eta)^{\sum_i n_i}, \quad (\text{D74})$$

where $Q(n_0, \dots, n_{N-1})$ is defined in Eq. (D72) and we emphasize once again that the yields are independent of j .

APPENDIX E: NUMERICAL SIMULATIONS

In this Appendix we provide more details about the numerical simulations presented in Sec. V of the paper.

In our simulations, we set a polarization and a phase misalignment between the reference party A_0 and each other party of 2%. This means that the parameters θ_i and ϕ_i , introduced in Appendix D to describe the polarization rotation and the phase mismatch of party A_i , are set to $\phi_0 = 0$, $\phi_{i \geq 1} = \phi$, $\theta_{i \geq 1} = \theta_1$, and $\phi = \theta_0 - \theta_1 = \arcsin \sqrt{0.02}$. We compute the protocol's key rate for three values of p_d , i.e., the probability of a dark count in a given detector, namely, $p_d = 10^{-8}$, 10^{-9} , and 10^{-10} .

As for the decoy-state analysis, we consider two decoy intensities for each party, β_0 and β_1 , and use the analytical bounds derived in Sec. IV to compute the upper bound (7) on the phase error rate. The decoy intensity β_0 is fixed to $\beta_0 = 0.5$, which we verify is a close-to-optimal value for all loss parameters, while $\beta_1 = 0$ is optimal. In Sec. V we also plot the key rate in the case in which the exact value of the yields is known, which corresponds to the limit where the parties have an infinite number of decoy intensities. The exact values of the yields are computed for our channel model in Appendix D and are reported in Eq. (D74). We then replaced the exact yields Y_0, \dots, Y_{N-1} in the phase error rate bound (7), in place of the yields' bounds $\bar{Y}_0, \dots, \bar{Y}_{N-1}$.

The key rates in Fig. 4 are optimized over the signal amplitude α for all values of loss and is computed for $N = 3, 4$, and 5 parties. In Fig. 5 we provide the optimal values of α for every loss, both when we use the yields bounds obtained with two decoys and when we use the exact expressions of the yields from the channel model. By comparing the optimal values of α in the two cases, we deduce that tighter bounds on the yields would allow for a higher optimal value of α . This is explained by the fact that having tighter bounds on the yields in the phase error rate bound (7) allows the yields' coefficients in that expression to grow, i.e., α to grow, without increasing the phase error rate bound. In turn, greater values of α can increase the key rate due to a higher chance of having a detector click [see Fig. 4(b)]. Therefore, we deduce that increasing the number of decoy intensities used by each party would lead to better yields' bounds and hence to a significantly improved key rate.

In order to reduce the number of yields that are nontrivially bounded in Eq. (7), we remark that the polarization and phase angles θ_i and ϕ_i are the same for all parties except for reference party A_0 . Moreover, the signal and decoy intensities are the same for all parties as well as the losses. Therefore, the channel model is symmetric under the permutation of parties A_1, A_2, \dots, A_{N-1} . This implies, in particular, that the yields in Eq. (7) satisfy

$$Y_{n_0, n_1, \dots, n_{N-1}} = Y_{n_0, \sigma(n_1, \dots, n_{N-1})}, \quad (\text{E1})$$

where $\sigma(n_1, \dots, n_{N-1})$ represents a permutation of the indexes n_1, \dots, n_{N-1} . The permutational symmetry of the yields in our channel model implies that, in computing the phase error rate bound (7) for a cutoff $\bar{n} = 4$ (above which every yield is bounded by one), we need only to bound the following yields for $N = 3$: $Y_{0,0,0}$, $Y_{2,0,0}$, $Y_{0,2,0}$, $Y_{4,0,0}$, $Y_{0,4,0}$, $Y_{1,1,0}$, $Y_{0,1,1}$, $Y_{2,2,0}$, $Y_{0,2,2}$, $Y_{1,3,0}$, $Y_{0,1,3}$, $Y_{1,1,2}$.

Similarly, for $N = 4$ we bound only the yields: $Y_{0,0,0,0}$, $Y_{2,0,0,0}$, $Y_{4,0,0,0}$, $Y_{0,4,0,0}$, $Y_{1,1,0,0}$, $Y_{0,1,1,0}$, $Y_{2,2,0,0}$, $Y_{0,2,2,0}$, $Y_{1,3,0,0}$, $Y_{0,1,3,0}$, $Y_{1,1,2,0}$, $Y_{0,1,1,2}$, $Y_{1,1,1,1}$.

And for $N = 5$ we bound only the yields: $Y_{0,0,0,0,0}$, $Y_{2,0,0,0,0}$, $Y_{4,0,0,0,0}$, $Y_{0,4,0,0,0}$, $Y_{1,1,0,0,0}$, $Y_{0,1,1,0,0}$, $Y_{2,2,0,0,0}$, $Y_{0,2,2,0,0}$, $Y_{1,3,0,0,0}$, $Y_{0,1,3,0,0}$, $Y_{1,1,2,0,0}$, $Y_{0,1,1,2,0}$, $Y_{1,1,1,1,0}$, $Y_{0,1,1,1,1}$.

-
- [1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
 - [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [3] K. Chen and H. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, *Quantum Inf. Comput.* **7**, 689 (2007).
 - [4] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, *New J. Phys.* **19**, 093012 (2017).
 - [5] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, *New J. Phys.* **20**, 113014 (2018).
 - [6] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Modular network for high-rate quantum conferencing, *Commun. Phys.* **2**, 118 (2019).
 - [7] Z. Zhang, R. Shi, and Y. Guo, Multipartite continuous variable quantum conferencing network with entanglement in the middle, *Appl. Sci.* **8**, 1312 (2018).
 - [8] S. Zhao, P. Zeng, W.-F. Cao, X.-Y. Xu, Y.-Z. Zhen, X. Ma, L. Li, N.-L. Liu, and K. Chen, Phase-Matching Quantum Cryptographic Conferencing, *Phys. Rev. Appl.* **14**, 024010 (2020).

- [9] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, *Adv. Quantum Technol.* **3**, 2000025 (2020).
- [10] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, *Sci. Adv.* **7**, eabe0395 (2021).
- [11] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi, Experimental network advantage for quantum conference key agreement, *ArXiv:2207.01643* (2022).
- [12] F. Hahn, J. de Jong, and A. Pappa, Anonymous Quantum Conference Key Agreement, *PRX Quantum* **1**, 020325 (2020).
- [13] F. Grasselli, G. Murta, J. de Jong, F. Hahn, H. Kampermann, and A. Pappa, Secure Anonymous Conferencing in Quantum Networks, *PRX Quantum* **3**, 040306 (2022).
- [14] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz, Experimental anonymous conference key agreement using linear cluster states, *ArXiv:quant-ph/2207.09487* (2022).
- [15] 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* **557**, 400 (2018).
- [16] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, *Phys. Rev. X* **8**, 031043 (2018).
- [17] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, *npj Quantum Inf.* **5**, 64 (2019).
- [18] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, *Phys. Rev. A* **98**, 062323 (2018).
- [19] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-Field Quantum Key Distribution Without Phase Postselection, *Phys. Rev. Appl.* **11**, 034053 (2019).
- [20] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [21] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).
- [22] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and Reverse Secret-Key Capacities of a Quantum Channel, *Phys. Rev. Lett.* **102**, 050503 (2009).
- [23] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nat. Photonics* **13**, 334 (2019).
- [24] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution Through Sending or Not Sending, *Phys. Rev. Lett.* **123**, 100505 (2019).
- [25] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System, *Phys. Rev. X* **9**, 021046 (2019).
- [26] X.-T. Fang, *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, *Nat. Photonics* **14**, 422 (2020).
- [27] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [28] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, *Nat. Photonics* **15**, 530 (2021).
- [29] H. Liu, *et al.*, Field Test of Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending over 428 km, *Phys. Rev. Lett.* **126**, 250502 (2021).
- [30] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, *Nat. Photonics* **15**, 570 (2021).
- [31] C. Clivati, A. Meda, S. Donadello, S. Virzi, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni, and D. Calonico, Coherent phase transfer for real-world twin-field quantum key distribution, *Nat. Commun.* **13**, 157 (2022).
- [32] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [33] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing, *Phys. Rev. Lett.* **128**, 180502 (2022).
- [34] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, *New J. Phys.* **21**, 123002 (2019).
- [35] X.-Y. Cao, Y.-S. Lu, Z. Li, J. Gu, H.-L. Yin, and Z.-B. Chen, High key rate quantum conference key agreement with unconditional security, *IEEE Access* **9**, 128870 (2021).
- [36] X.-Y. Cao, J. Gu, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, Coherent one-way quantum conference key agreement based on twin field, *New J. Phys.* **23**, 043002 (2021).
- [37] J.-L. Bai, Y.-M. Xie, Z. Li, H.-L. Yin, and Z.-B. Chen, Post-matching quantum conference key agreement, *Opt. Express* **30**, 28865 (2022).
- [38] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, *Phys. Rev. A* **62**, 062314 (2000).
- [39] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [40] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [41] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).

- [42] S. Pirandola, General upper bound for conferencing keys in arbitrary quantum networks, *IET Quantum Commun.* **1**, 22 (2020).
- [43] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, *Nat. Phys.* **6**, 659 (2010).
- [44] Note that we can assume, without loss of generality, that there is only one Kraus operator for each announcement Ω_j . Indeed, if there were more, the eavesdropper would be able to distinguish which operator acted on the optical modes with an ancillary classical flag. The flag would be part of the side information E , allowing the expansion of the entropy $H(X_0|E)_{\Omega_j}$ over each value of the flag, which coincides with the scenario of having only one Kraus operator.
- [45] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).
- [46] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, *NPJ Quantum Inf.* **7**, 22 (2021).
- [47] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference, *PRX Quantum* **3**, 020315 (2022).
- [48] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, *Nat. Commun.* **13**, 3903 (2022).
- [49] F. Grasselli, Á. Navarrete, and M. Curty, Asymmetric twin-field quantum key distribution, *New J. Phys.* **21**, 113032 (2019).
- [50] C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, and Z.-B. Chen, Breaking universal limitations on quantum conference key agreement without quantum memory, *ArXiv:2212.05226* (2022).
- [51] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, *Quantum* **1**, 14 (2017).