Device-independent Quantum Key Distribution and the Role of Bell Nonlocality

Inaugural-Dissertation

submitted in partial fulfillment of the requirements
for the degree of

Dr. rer. nat.

in the Faculty of Mathematics and Natural Sciences
at the Heinrich-Heine-Universität Düsseldorf

presented by

Timo Holz
from Dudweiler

Düsseldorf, November 2019

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

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

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

Date of the oral examination: 13.12.2019

Declaration of Authorship

Ich versichere an Eides statt, dass die Dissertation von mir selbstständig und ohne unzulässige fremde Hilfe unter Beachtung der "Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Universität Düsseldorf" erstellt worden ist.

Signed

Date

To my family

"I think I can safely say that nobody understands quantum mechanics."

Richard P. Feynman, 1964

Abstract

Quantum entanglement is a unique property of quantum particles. It can correlate them in such a way, that further correlations to an additional unwanted party is prevented. This renders quantum theory as the prime candidate to implement a secure distribution of an encryption key. Quantum key distribution (QKD) is dedicated to this task. A striking feature of correlations in a statistical experiment is, that they can, in principle, always be approximated. Even more so, correlations can be obtained without a detailed knowledge about the underlying physical process that generated the experimental data. This no-characterization approach is at the heart of the device-independent (DI) paradigm. Here, Bell inequalities are an imperative tool to detect nonlocal correlations, which are necessary for a DI secret key.

One central subject of this thesis is multipartite DIQKD and the implications of Bell nonlocality in this context. Any DIQKD protocol involves test rounds in which the violation of a Bell inequality is checked. For multipartite DIQKD, however, not all Bell inequalities are suitable. We identify the crucial properties a Bell test requires to be a viable option. In this light, a published protocol for multipartite DIQKD is examined. We establish an incompatibility which is inherent to the proposed Bell test in combination with the required quantum states. This leads us to the conclusion, that the proposed protocol necessarily aborts. In a subsequent work, we develop a family of multipartite Bell inequalities, specifically tailored to the task of DI conference key agreement (CKA). Several features of this Bell inequality are analytically characterized. In addition, we prove its usefulness for the purposes of DICKA. To this end, semidefinite programming techniques are employed and extended to the multipartite scenario which allows us to quantify asymptotic DI conference key rates.

In a second part, we explore the challenges of implementing (bipartite) long-distance DIQKD with quantum repeaters. For two repeater protocols, we describe how experimental parameters manifest themselves in DI secret-key rates. In doing so, we shed light on the fundamental differences between the usual and the DI scenario and we benchmark the threshold requirements of quantum devices to make profitable DI secret-key rates feasible. Finally, we develop a general method to describe in a non-DI setting the propagation of an important class of errors through quantum circuits in arbitrary dimensions. With this, we discuss the potential of error-corrected quantum repeaters to overcome fundamental point-to-point limitations.

Zusammenfassung

Quantenverschränkung ist eine bemerkenswerte Eigenschaft von Quantenteilchen, die eine derart starke Korrelation zwischen ihnen erlaubt, sodass eine weitere Korrelation zu einer unerwünschten dritten Partei ausgeschlossen werden kann. Die Quantentheorie ist daher der optimale Rahmen, um eine sichere Übertragung eines kryptographischen Schlüssels zu implementieren. Dies ist die zentrale Aufgabe der Quantenschlüsselverteilung (QKD). Ein wichtiges Merkmal von Korrelationen in einem statistischen Experiment ist, dass diese prinzipiell immer zugänglich sind und beliebig genau approximiert werden können. Insbesondere ist hierfür ein genaues Verständnis des physikalischen Ablaufs, der die Messdaten generiert, nicht erforderlich. Dieser Ansatz steckt im Kern des apparateunabhängigen (DI) Paradigmas. Bell Ungleichungen sind in diesem Kontext unverzichtbar, wegen ihrer Fähigkeit nichtlokale Korrelationen detektieren zu können, die für einen DI sicheren Schlüssel notwendig sind.

Ein zentrales Thema dieser Dissertation ist die multipartite apparateunabhängige Quantenschlüsselverteilung (DIQKD) und die Implikationen von Bell Nichtlokalität in diesem Kontext. In jedem DIQKD Protokoll wird die Verletzung einer Bell Ungleichung in Testrunden geprüft. Für multipartite DIQKD ist jedoch nicht jede Bell Ungleichung geeignet. Wir identifizieren entscheidende Merkmale, die ein Belltest aufweisen muss, um eine gangbare Option für DIQKD darzustellen. Vor diesem Hintergrund untersuchen wir ein publiziertes Protokoll für multipartite DIQKD. Wir etablieren eine, dem vorgeschlagenen Belltest inhärente, Inkompatibilität mit den für QKD notwendigen Quantenzuständen. Dies führt uns zu der Schlussfolgerung, dass das Protokoll zwangsläufig abbrechen muss. Darauf aufbauend entwickeln wir speziell für multipartite DIQKD eine Familie von Bell Ungleichungen. Verschiedene Eigenschaften dieser Bell Ungleichung werden analytisch beschrieben. Wir stellen außerdem deren Verwertbarkeit für multipartite DIQKD unter Beweis. Zu diesem Zweck, nutzen wir semidefinite Programmierung, erweitert auf mehrere Parteien, und quantifizieren DI Konferenzschlüsselraten.

In einem zweiten Themenkomplex erforschen wir die Möglichkeit (bipartite) DIQKD über große Distanzen mittels Quantenrepeater zu realisieren. Wir beschreiben für zwei Quantenrepeatermodelle, wie sich typische experimentelle Parameter in den DI Schlüsselraten manifestieren. In dieser systematischen Analyse arbeiten

wir fundamentale Unterschiede zwischen dem apparateabhängigem (DD) und dem DI Szenario heraus. Darüber hinaus setzen wir den Maßstab für die Mindestanforderung an die Qualität der Quantenapparate, um profitable DI Schlüsselraten zu erhalten. Schließlich entwickeln wir, in dem DD Szenario und für beliebige Dimensionen, ein allgemeines Verfahren zur Beschreibung der Propagation einer wichtigen Fehlerklasse durch den Quantenrepeater. Ausgestattet mit diesem Werkzeug untersuchen wir das Potential von fehlerkorrigierten Quantenrepeatern um fundamentale Grenzen von Punkt-zu-Punkt Verbindungen zu überschreiten.

Acknowledgements

Before we delve into the contents of this thesis, I want to express my gratitude to many people who helped me on my way, directly or indirectly. So let me give credit where credit is due.

First, I would like to thank my supervisor Dagmar Bruß, for giving me the opportunity to become the scientist I am today. I greatly participated from her experience and her analytical way of thinking. I really enjoyed the kind and productive environment at her institute.

No less thanks are due to Hermann Kampermann, my co-supervisor and mentor. I am greatly indebted to his scientific acumen and, a posteriori, I acknowledge him constantly pushing me to render my thoughts more clearly. His input proved to be invaluable at many instances, thereby improving the scientific content of this manuscript.

Many thanks to all of my colleagues, Carlo Liorni, Daniel Miller, Federico Grasselli, Giulio Gianfelici, Gláucia Murta, Lukas Tendick, Sarnava Datta, Thomas Wagner, our IT administrator Jens Bremer, and all remaining members of the Institute for Theoretical Physics III. In particular, I acknowledge the help of Daniel Miller, Federico Grasselli, Carlo Liorni, and Lukas Tendick, who proofread parts of this thesis. I also want to express my gratitude to Felix Bischof, whose visits to my office were welcomed opportunities for procrastination.

Besides academia, my deepest gratitude lies with my family, Jürgen, Dagmar, and Marco Holz, without whom none of this would have been possible. I will always be grateful for their unconditional support. I want to emphasize how proud I am of my parents, for achieving so much, starting from so little.

I also appreciate the feedback on the introduction of this manuscript provided by Niamh Farrell and Ruwen Hollenbach.

Last but not least, my sincerest thanks to Isabell Geimer, who helped improving the grammar in this thesis. More importantly though, I thank her for her support and for making my life so much more enjoyable.

Contents

List of Figures

Chapter 1

Introduction

Quantum cryptography emerged in the early 1980s [Wie83] as one of the cornerstones of quantum information science. The central idea in quantum cryptography is to use the laws of quantum mechanics for the purposes of secrecy. To exploit quantum theory to its full potential for quantum cryptographic applications, a profound theoretical understanding of quantum correlations and their implications is required. So-called *Bell inequalities* [Bel64a] are an integral part of this foundational research.

Arguably the most important subfield of quantum cryptography is *quantum key distribution* (QKD) which was born in 1984 with the famous BB84 protocol [BB84]. It is dedicated to the task of distributing a secure encryption key to the honest parties who wish to communicate. Quantum mechanics offers a unique way to achieve this, by employing intrinsic features of quantum particles such as *entanglement*.

Since BB84, a variety of QKD protocols have been published [Eke91, Ben92, Bru98]. Although pioneering work, a common flaw of these protocols is that they have extreme demands on their physical implementation which in general cannot be realized. Any experimental deviation which is not accounted for in the theoretical description potentially allows a malicious eavesdropper to break the security of the QKD scheme.

This calls for a new standard of security which is independent of the exact internal workings of the quantum devices that are required for QKD. Surprisingly, quantum mechanics provides such a *device-independent* (DI) way to certify the security of a cryptographic protocol. Security is established by means of certain classical input-output correlations [MY98] which serve as a witness for the integrity of the data. Bell inequalities are indispensable for a DI security.

Quantum key distribution becomes meaningful if it can be realized in a large-scale quantum network including multiple parties. However, quantum correlations which grant the aforementioned benefits are fragile and easily disturbed by the influence of the environment or by quantum operations. A straightforward amplification or repetition of the quantum signal in the classical sense is fundamentally prevented by the laws of quantum mechanics. Hence, a more sophisticated approach in the form of *quantum repeaters* [BDCZ98] is required, inter alia, to realize long-distance QKD.

This thesis aims at a concise and self-contained presentation of our research in multipartite DIQKD, the role of Bell nonlocality therein, and the prospects of its implementation in a quantum repeater network. To this end, our manuscript exhibits the following logical structure.

In Chap. 2 we introduce basic notions of many concepts in quantum information theory and the required mathematical tools.

Chapter 3 is devoted to Bell nonlocality and Bell inequalities. We thoroughly introduce the best known representative of Bell inequalities and discuss its generalizations. Multipartite Bell inequalities are of particular interest to us. We go on to discuss these in more detail, including supplemental results which were not explicitly contained in previously published work. In addition, we will review numerical tools required for a further characterization of quantum correlations and explicitly apply them to a Bell inequality we developed.

An introduction to QKD is provided in Chap. 4. This serves two purposes. First, we require the fundamental concepts that allow the secure distribution of an encryption key, and the BB84 protocol allows a rather intuitive way to get familiar with them. Second, some notions of QKD need to be refined and adjusted in the multipartite setting, which we also address in this chapter.

Bell inequalities and QKD lay the foundations for DIQKD, which is the subject of Chap. 5. The DI security of quantum cryptographic protocols was extensively investigated in recent years. We give a brief survey of the development and then provide an in-depth review of one of the most central results which is relevant for this thesis. In the subsequent section, we address the extension to multipartite DIQKD. Here, two proposals are investigated from which only the second is a viable option. We explain in detail why the first approach cannot succeed and provide additional information not included in our publication. The chapter concludes with a short discussion of state-of-the-art DIQKD experiments.

A survey of the quantum repeater concept is provided in Chap. 6. First, we explain the fundamental limitation faced by point-to-point quantum communication. Afterwards, we introduce the original quantum repeater protocol and put it into the context of QKD. An alternative quantum repeater based on error-correction is the subject of the subsequent section.

A brief summary of our main results can be found in Chap. 7.

We conclude with Chap. 8 and give an outlook for future research based on our work.

The original articles that constitute the main content of our research are attached in Appendices A to E.

Chapter 2

Quantum Mechanics and Linear Algebra

Quantum theory [Pla00] dictates the behavior of nature at the smallest scales of length and energy, with laws that are comparatively simple, but generally perceived as counterintuitive. Predictions of quantum theory, however, are in striking accordance with experimental observations, thus witnessing its superiority over the classical formulation.

In this chapter, we provide the essential mathematical tools needed for a precise description of many quantum mechanical concepts. The postulates of quantum mechanics are introduced alongside the required elements of linear algebra. Inspiration was taken from a variety of literature, most importantly though from Refs. [NC10, KLM07, CTDL77] and [Fis75].

2.1. The State Space and the Dirac Notation

In this thesis, we exclusively consider discrete quantum systems with a finite number $d \in \mathbb{N}$ of inherent degrees of freedom. There are numerous quantum systems fulfilling this requirement, such as an atom and its energetic excitations, an electron and its spin, or a photon and its polarization. The following statement offers a mathematical way to describe the *state* of a quantum system.

Postulate 1. *At each instant of time t, the state of a physical system is defined by an element $|\psi(t)\rangle$ of a state space $\mathcal{H}$.*

In 1939, Dirac [Dir39] introduced the notation $|\psi(t)\rangle$ for a state space element. The state space $\mathcal{H}$ is a finite dimensional vector space over the field $\mathbb{C}$ of complex numbers that is supplemented with an *inner product*, denoted by $\langle\cdot|\cdot\rangle$, i.e., $\mathcal{H}$ is a *Hilbert space*. Note that the identification of the state space with the mathematical notion of a vector space, already has profound implications, namely that a linear combination or a *superposition* of elements of $\mathcal{H}$ again represent a quantum state. To rigorously define the inner product of the Hilbert space $\mathcal{H}$, we introduce the *dual* version of $\mathcal{H}$.

Definition 2.1 (Dual Space)**.** *Let $\mathcal{H}$ be a Hilbert space over the field $\mathbb{C}$. The dual space $\mathcal{H}^*$ is the vector space of all linear maps $\mathcal{H} \to \mathbb{C}$.*

Elements of the dual space $\mathcal{H}^*$ are denoted by $\langle\varphi|$. They act onto $|\psi\rangle \in \mathcal{H}$ according to $\langle\varphi| : |\psi\rangle \mapsto \langle\varphi|\,\psi\rangle \in \mathbb{C}$, i.e., they map the state to a complex scalar – the inner product $\langle\varphi|\,\psi\rangle$ of the states $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$. The standard inner product in vector spaces over the complex field $\mathbb{C}$ is a *sesquilinear form*, i.e., it fulfills

$$\langle\varphi|\,\alpha\psi_1 + \beta\psi_2\rangle = \alpha\langle\varphi\,|\psi_1\rangle + \beta\langle\varphi\,|\psi_2\rangle\,, \tag{2.1a}$$

$$\langle\alpha\varphi_1 + \beta\varphi_2|\,\psi\rangle = \alpha^*\langle\varphi_1\,|\psi\rangle + \beta^*\langle\varphi_2\,|\psi\rangle\,, \tag{2.1b}$$

for all $|\psi_i\rangle, |\psi\rangle \in \mathcal{H}$, $\langle\varphi|, \langle\varphi_i| \in \mathcal{H}^*$, and $\alpha, \beta \in \mathbb{C}$, where α^* denotes the complex conjugation of α. The inner product induces a *norm* $\|\cdot\|$ on $\mathcal{H}$, via $\|\psi\| \coloneqq \sqrt{\langle\psi|\,\psi\rangle}$ and we call states with $\|\psi\| = 1$ *normalized*. Furthermore, a sense of relative orientation between states is provided by the inner product, that is, states with $\langle\varphi|\,\psi\rangle = 0$ are *orthogonal* to each other. This leads us to:

Definition 2.2 ((Orthonormal) Basis)**.** *Let $\mathcal{H}$ be a d-dimensional Hilbert space. A set $\{|b_i\rangle\}_{i=1}^d =: \mathcal{B} \subset \mathcal{H}$ of linear independent vectors is called a basis of $\mathcal{H}$, if every element $|\psi\rangle \in \mathcal{H}$ can be written as a (unique) linear combination of elements of $\mathcal{B}$, i.e.,*

$$|\psi\rangle = \sum_{i=1}^{d} c_i\,|b_i\rangle\,, \quad \textit{with} \quad c_i \coloneqq \langle b_i|\,\psi\rangle \in \mathbb{C}. \tag{2.2}$$

The basis $\mathcal{B}$ is called orthonormal, if its elements are of unit length and they are pairwise orthogonal, i.e., if $\langle b_i|\,b_j\rangle = \delta_{i,j}$.

Here, $\delta_{i,j}$ denotes the Kronecker delta which is equal to one for $i = j$ and zero otherwise. Often, the orthonormal basis of choice is the so-called *computational basis*, with elements $\{|k\rangle\}_{k=0}^{d-1}$. Two orthonormal bases $\{|b_i\rangle\}_{i=1}^d, \{|b'_j\rangle\}_{j=1}^d$ of $\mathcal{H}$ are *mutually unbiased* if $|\langle b_i|\,b'_j\rangle|^2 = \frac{1}{d}$ for all i, j.

2.2. Linear Operators

To describe the manipulation of a quantum state we define:

Definition 2.3 (Linear Operator)**.** *A linear operator on a Hilbert space $\mathcal{H}$ is a linear map $M : \mathcal{H} \to \mathcal{H}, |\psi\rangle \mapsto M\,|\psi\rangle$.*

In Dirac notation we can write certain linear operators via the *dyadic product* as $|\psi\rangle\langle\varphi|$. Such an operator maps the state $|\chi\rangle \in \mathcal{H}$ to $\langle\varphi|\,\chi\rangle\,|\psi\rangle \in \mathcal{H}$. The set of all linear operators on $\mathcal{H}$ form again a vector space, which we denote with $\mathcal{L}(\mathcal{H})$. Consider a d-dimensional Hilbert space with an orthonormal basis $\{|b_i\rangle\}_{i=1}^d$. Via the *resolution of the identity* property, $\mathbb{1} = \sum_i |b_i\rangle\langle b_i|$, we can represent every linear operator $M \in \mathcal{L}(\mathcal{H})$ as

$$M = \sum_{i,j=1}^{d} M_{i,j}\,|b_i\rangle\langle b_j|\,, \quad \text{with} \quad M_{i,j} = \langle b_i|M|b_j\rangle\,. \tag{2.3}$$

Definition 2.4 (Eigenvalue, Eigenstate)**.** *Let $M \in \mathcal{L}(\mathcal{H})$. A scalar $m \in \mathbb{C}$ is eigenvalue of M if there exists a $|\psi\rangle \in \mathcal{H}$ with $|\psi\rangle \neq \mathbf{0}$, such that*

$$M|\psi\rangle = m|\psi\rangle, \tag{2.4}$$

and $|\psi\rangle$ is eigenstate of M to eigenvalue m. The set of all eigenvalues of M is called spectrum of M, denoted by $\sigma(M)$.

Of particular importance for quantum mechanics are *self-adjoint* or *Hermitian* operators. To introduce them, we need the notion of *Hermitian conjugation*. That is, to each operator $M \in \mathcal{L}(\mathcal{H})$, there exists a unique operator $M^\dagger \in \mathcal{L}(\mathcal{H}^*)$ that fulfills $(\langle\varphi|M|\psi\rangle)^* = \langle\psi|M^\dagger|\varphi\rangle$ for all $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$. Hermitian operators satisfy $M^\dagger = M$.

Lemma 2.5 (Spectrum of Hermitian Operators)**.** *Let $M \in \mathcal{L}(\mathcal{H})$ be a self-adjoint operator. Then, $\sigma(M) \subset \mathbb{R}$.*

Proof. Let $|\psi\rangle$ be a (normalized) eigenstate of M to eigenvalue m. Therefore,

$$m = \langle\psi|(m|\psi\rangle) = \langle\psi|M|\psi\rangle = \langle\psi|M^\dagger|\psi\rangle = (\langle\psi|m^*)|\psi\rangle = m^*.$$

■

Theorem 2.6 (Spectral Theorem)**.** *Let $\mathcal{H}$ be a Hilbert space of finite dimension d and $M \in \mathcal{L}(\mathcal{H})$ a Hermitian operator. Then, there exists an orthonormal basis of $\mathcal{H}$ that consists of eigenstates of M.*

Proof. Let $M \in \mathbb{C}^{d\times d}$ be the matrix representation of a self-adjoint operator. Since $\mathbb{C}$ is algebraically closed, the characteristic polynomial of M can be decomposed into linear factors of its eigenvalues m_i which are real due to Lemma 2.5. The rest of the proof can be done via induction, where the case $d = 0$ is trivial. For $d \geqslant 1$, there exists a normalized eigenstate $|\psi_1\rangle$ of M to eigenvalue m_1. Let $\mathcal{W} \coloneqq \{|\varphi\rangle \in \mathcal{H} \mid \langle\psi_1|\varphi\rangle = 0\}$. For all $|\varphi\rangle \in \mathcal{W}$, it holds

$$\langle\psi_1|(M|\varphi\rangle) = \left(\langle\psi_1|M^\dagger\right)|\varphi\rangle = m_1\langle\psi_1|\varphi\rangle = 0, \tag{2.5}$$

i.e., $M|\varphi\rangle \in \mathcal{W}$. By induction base, there exists a orthonormal basis of $\mathcal{W}$ that consists of $(d-1)$ eigenstates of M, which together with the state $|\psi_1\rangle$ yields the orthonormal basis of $\mathcal{H}$. ■

The condition of finite dimension in Theorem 2.6 is crucial. In infinite dimensional Hilbert spaces, only the eigenstates of particular Hermitian operators, so-called *observables*, form an eigenbasis of $\mathcal{H}$. Observables are key ingredients for quantum measurements, which will be further discussed in Sec. 2.4.

2.3. Density Operator Formalism

Often, a more convenient description of quantum states is provided by the *density operator* formalism. We call a density operator w.r.t. a fixed basis a *density matrix*. A quantum source which provides with probability p_i the quantum state $|\psi_i\rangle$ motivates the definition of quantum states in terms of a statistical mixture.

Definition 2.7 (Density Operator)**.** *Let* $\{|\psi_i\rangle\}_{i=1}^n$ *be a set of quantum states and* $\{p_i\}_{i=1}^n$ *a probability distribution, i.e.,* $\sum_{i=1}^n p_i = 1$ *and* $p_i \in [0,1]$ *for all* i*. The operator*

$$\rho = \sum_{i=1}^{n} p_i \, |\psi_i\rangle\langle\psi_i| \tag{2.6}$$

is called a mixed state if $p_i < 1$ *for all* i*. We call* ρ *a pure state if there exists one index* i' *for which* $p_{i'} = 1$*.*

To further characterize density operators, we introduce the *trace* function of a matrix M, which is defined as the sum of its diagonal elements, i.e., for a basis $\{|b_i\rangle\}_i$ the trace of M is given by $\mathrm{tr}\,(M) \coloneqq \sum_{i=1}^d \langle b_i| M |b_i\rangle$ which is independent of the particular choice of the basis. Density operators fulfill the following properties:

(i) Density operators are self-adjoint operators, i.e., $\rho^\dagger = \rho$.
(ii) The trace of density operators is $\mathrm{tr}\,(\rho) = 1$. Moreover, $\mathrm{tr}\left(\rho^2\right) = 1$ if and only if ρ is a pure state.
(iii) They are *positive semidefinite*, i.e., $\langle\psi|\,\rho\,|\psi\rangle \geqslant 0 \quad \forall \quad |\psi\rangle \in \mathcal{H}$, denoted by $\rho \geqslant 0$.

2.3.1. The Quantum Bit and the Bloch Sphere

The most simple, yet nontrivial states are of dimension $d = 2$. Commonly, the two degrees of freedom are labeled with $|0\rangle, |1\rangle \in \mathcal{H}_2$. Such quantum states represent the fundamental unit of quantum information, hence the name *quantum bit* or *qubit*. A general qubit state can thus be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{with} \quad |\alpha|^2 + |\beta|^2 = 1, \quad \alpha, \beta \in \mathbb{C}. \tag{2.7}$$

Quantum states which only differ by a global phase are indistinguishable, thus physically equivalent, and we can take α to be real without loss of generality. A parametrization in spherical coordinates then turns Eq. (2.7) into

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle\,, \quad \text{with} \quad 0 \leqslant \theta \leqslant \pi, \quad 0 \leqslant \phi < 2\pi. \tag{2.8}$$

We now identify the parameters θ, ϕ with the polar θ and azimuthal angle ϕ in a unit vector in spherical coordinates, i.e., $\boldsymbol{e}_{\phi,\theta} = (\sin(\theta)\cos(\phi), \sin(\theta)\sin(\phi), \cos(\theta))^T$. The vector $\boldsymbol{e}_{\phi,\theta}$ defines for $\phi \in [0, 2\pi)$ and $\theta \in [0, \pi]$ the surface of a sphere, embedded in the $\mathbb{R}^3$ and thus allows for $\theta \in (0, \pi)$ a unique mapping of a pure qubit state $|\psi\rangle$ with a point on the surface of this *Bloch sphere*. This is visualized in Fig. 2.1.

In 1927, Wolfgang Pauli introduced the *Pauli matrices* to describe the spin of an electron [Pau27], which only has two different spin-degrees of freedom and thus represents a qubit quantum system. The Pauli matrices in the computational basis $\{|0\rangle = \begin{pmatrix}1 & 0\end{pmatrix}^T, |1\rangle = \begin{pmatrix}0 & 1\end{pmatrix}^T\}$ are given by

$$\sigma_x \equiv \sigma_1 = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \quad \sigma_y \equiv \sigma_2 = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, \quad \sigma_z \equiv \sigma_3 = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}. \tag{2.9}$$

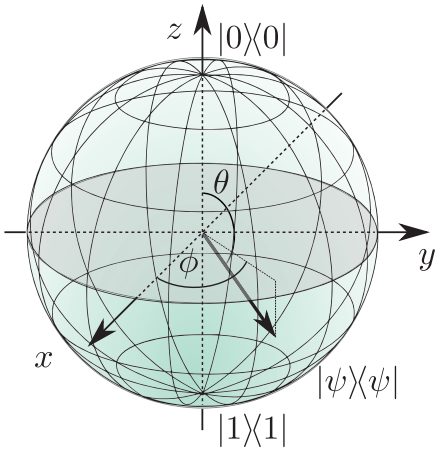

Figure 2.1: Any pure qubit state corresponds to a point of the surface of the Bloch sphere. The depicted general qubit state $|\psi\rangle$ according to Eq. (2.8) is shown for some angles θ and ϕ. For $\theta = 0$ ($\theta = \pi$) and arbitrary ϕ, the state $|\psi\rangle$ marks the north (south) pole of the sphere and corresponds to the pure state $|0\rangle$ ($|1\rangle$).

They are Hermitian, traceless operators with eigenvalues ± 1 and satisfy the relation

$$\sigma_i \sigma_j = \delta_{i,j} \mathbb{1} + \sum_{k=1}^{3} \epsilon_{i,j,k} \sigma_k . \tag{2.10}$$

Here, $\epsilon_{i,j,k}$ denotes the *Levi-Civita symbol* which is $+1$ (-1) if the triple (i, j, k) is a cyclic (anticyclic) permutation of $(1, 2, 3)$, and 0 otherwise.

The set $\{\sigma_i\}_{i=1}^{3}$ of Pauli matrices is a basis for all Hermitian, traceless matrices on a two-dimensional Hilbert space. Together with the identity matrix $\mathbb{1}$, any qubit state ρ can be expressed according to

$$\rho = \frac{\boldsymbol{s}^T \boldsymbol{\sigma} + \mathbb{1}}{2}, \quad \text{with} \quad \|\boldsymbol{s}\| \leqslant 1, \;\; \boldsymbol{\sigma} \coloneqq (\sigma_x, \sigma_y, \sigma_z)^T , \tag{2.11}$$

where $\boldsymbol{s}$ is the *Bloch vector* of ρ. Recalling property (ii) of density operators, one can identify the interior of the Bloch sphere with mixed states. The *completely mixed* state $\frac{1}{2}\mathbb{1}$ has $\boldsymbol{s} = \mathbf{0}$ and is thus located at the center of the Bloch sphere.

2.3.2. The Quantum Dit

The qubit concept can be generalized to a *quantum dit* or *qudit*. Here, the quantum system has a discrete and finite number $d \geqslant 2$ of inherent degrees of freedom, with labels according to the computation basis $\{|k\rangle\}_{k=0}^{d-1}$. One can introduce a Pauli basis for all linear operators on a d-dimensional Hilbert space. This basis , $\{X^r Z^s\}_{r,s=0}^{d-1}$, consists of d^2 independent operators and follows from [Got99]

$$X \coloneqq \sum_{k=0}^{d-1} |k \oplus 1\rangle\langle k| \quad \text{and} \quad Z \coloneqq \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k| , \tag{2.12}$$

where $\omega \coloneqq e^{\frac{2\pi i}{d}}$ and $\oplus$ denotes the addition modulo d. The generalized Pauli operators $X^r Z^s$ are traceless for all $r, s \in \{0, \ldots, d-1\}$. In contrast to their two dimensional counterparts, however, they are *not* self-adjoint.

2.4. Quantum Measurements

To extract information from a physical system, some sort of interaction is required. Here, we explain how a quantum measurement is described, which measurement results are possible, and how the measurement itself affects the quantum system.

Postulate 2. *A quantum measurement of a physical quantity of a system in quantum state ρ is described by a set of measurement operators $\{M_m\}_m \in \mathcal{L}(\mathcal{H})$, satisfying the completeness relation $\sum_m M_m^\dagger M_m = \mathbb{1}$. A possible measurement outcome m is measured with probability*

$$p(m) = tr\left(M_m^\dagger M_m \rho\right) \tag{2.13}$$

and the state of the system after the measurement is

$$\rho_m = \frac{1}{tr\left(M_m^\dagger M_m \rho\right)} M_m \rho M_m^\dagger. \tag{2.14}$$

In *projective measurements* the measurement operators M_m correspond to *projectors* P_m with the defining properties $P_m^2 = P_m$ and $P_m^\dagger = P_m$. The operators P_m form the spectral decomposition of the observable that is measured, i.e., $M = \sum_m m P_m$.

To get familiar with the concept of a projective measurement, consider a quantum source that randomly generates a pure state from an orthonormal set $\{|\psi_k\rangle\}_{k=1}^n$. In order to reliably identify which state is produced, define the projective measurement operators $P_m \coloneqq |\psi_m\rangle\langle\psi_m|$ for $m \in \{1, \ldots, n\}$ and $P_0 \coloneqq \mathbb{1} - \sum_{m=1}^n P_m$. Given the state $|\psi_k\rangle$, we find outcome m with probability $p(m) = \mathrm{tr}\left(P_m |\psi_k\rangle\langle\psi_k|\right) = \delta_{k,m}$, which allows us to distinguish the states with certainty.

The situation is different for non-orthogonal states, in which case there exists *no* set of measurement operators that provides a reliable way to distinguish these states. For an heuristic way to comprehend this statement suppose that the quantum source distributes either $|\psi\rangle$ or $|\varphi\rangle$. Because of $\langle\varphi|\,\psi\rangle \neq 0$, we can decompose the state

$$|\varphi\rangle = c_\perp |\psi_\perp\rangle + c_\parallel |\psi_\parallel\rangle, \qquad \text{with} \quad |c_\perp|^2 + |c_\parallel|^2 = 1, \tag{2.15}$$

into a nontrivial linear combination of states $|\psi_\perp\rangle$ and $|\psi_\parallel\rangle$ that are orthogonal and parallel to $|\psi\rangle$, respectively. Suppose the source provides the state $|\varphi\rangle$ on which we perform a measurement. Depending on the result we make a guess which state was produced by the source. But because of $\langle\varphi|\,\psi\rangle \neq 0$ we measure outcome m_ψ (based on which we infer that $|\psi\rangle$ was measured) with probability $|c_\parallel|^2 \neq 0$. Hence, we cannot deterministically distinguish the states $|\psi\rangle$ and $|\varphi\rangle$.

The task above is related to *unambiguous state discrimination* [Iva87]. As argued, no measurements can reliably differentiate between quantum states with a nonzero overlap. With general quantum measurements, however, a misidentification as above can be avoided. The corresponding measurement operators $E_m \coloneqq M_m^\dagger M_m \geqslant 0$ are *POVM elements* and the set $\{E_m\}_m$ is called POVM, an acronym for *positive operator-valued measure*. Note that POVM measurements include projective measurements, that is, for $M_m = P_m$ with $P_k P_m = \delta_{k,m} P_m$ we find $E_m = P_m$.

Importantly, any POVM measurement on a Hilbert space $\mathcal{H}$ of dimension d can be expressed as a projective measurement on a Hilbert space $\mathcal{H}'$ of dimension $d' \geqslant d$, which is the essence of the so-called *Naimark extension* [DJR05, Per06].

2.5. Composition of Quantum Systems

So far, we only considered a single quantum system. The extension to multiple quantum systems is achieved via the *tensor* or *Kronecker product*.

Postulate 3. *The state space of a composite system is given by the tensor product of the state spaces of the components, i.e., $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.*

For a state of $\mathcal{H}_{\mathrm{AB}}$ we equivalently write $|\psi_{\mathrm{A}}\rangle \otimes |\psi_{\mathrm{B}}\rangle = |\psi_{\mathrm{A}}\rangle |\psi_{\mathrm{B}}\rangle = |\psi_{\mathrm{A}}, \psi_{\mathrm{B}}\rangle$. Note that not all elements of $\mathcal{H}_{\mathrm{AB}}$ can be written in product form. For all $|\psi_{\mathrm{A}_i}\rangle \in \mathcal{H}_{\mathrm{A}}, |\psi_{\mathrm{B}_j}\rangle \in \mathcal{H}_{\mathrm{B}}, \alpha_i, \beta_j \in \mathbb{C}$, the tensor product is further characterized by

$$\Big(\sum_{i=1}^{d_{\mathrm{A}}} \alpha_i |\psi_{\mathrm{A}_i}\rangle\Big) \otimes \Big(\sum_{j=1}^{d_{\mathrm{B}}} \beta_j |\psi_{\mathrm{B}_j}\rangle\Big) = \sum_{i,j=1}^{d_{\mathrm{A}}, d_{\mathrm{B}}} \alpha_i \beta_j |\psi_{\mathrm{A}_i}, \psi_{\mathrm{B}_j}\rangle. \tag{2.16}$$

Any two orthonormal bases $\{|a_i\rangle\}_{i=1}^{d_{\mathrm{A}}}$, $\{|b_j\rangle\}_{j=1}^{d_{\mathrm{B}}}$ for $\mathcal{H}_{\mathrm{A}}$, $\mathcal{H}_{\mathrm{B}}$, give rise to an orthonormal basis $\{|a_i, b_j\rangle\}_{i,j}$ of the composite Hilbert space $\mathcal{H}_{\mathrm{AB}}$. However, the following theorem tells us, i.a., that we can always find a pair of orthonormal bases such that all cross terms $|a_i, b_j\rangle$ with $i \neq j$ vanish in the representation of $|\psi_{\mathrm{AB}}\rangle \in \mathcal{H}_{\mathrm{AB}}$.

Theorem 2.8 (Schmidt Decomposition)**.** *Let $|\psi_{AB}\rangle \in \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. There exists an orthonormal basis $\{|a_i\rangle\}_{i=1}^{d_A}$ for $\mathcal{H}_A$ and $\{|b_j\rangle\}_{j=1}^{d_B}$ for $\mathcal{H}_B$ and a set of nonnegative number $\{p_i\}$ such that*

$$|\psi_{AB}\rangle = \sum_{i=1}^{\min\{d_A, d_B\}} \sqrt{p_i}\, |a_i, b_i\rangle\,. \tag{2.17}$$

Proof. Let $\{|\bar{a}_i\rangle\}_{i=1}^{d_{\mathrm{A}}}, \{|\bar{b}_j\rangle\}_{j=1}^{d_{\mathrm{B}}}$ be an orthonormal basis for $\mathcal{H}_{\mathrm{A}}, \mathcal{H}_{\mathrm{B}}$, respectively. Thus, we can write

$$|\psi_{\mathrm{AB}}\rangle = \sum_{i,j} \bar{a}_i \bar{b}_j \,|\bar{a}_i, \bar{b}_j\rangle = \sum_{i,j} c_{i,j}\, |\bar{a}_i, \bar{b}_j\rangle\,, \tag{2.18}$$

where we identified $\bar{a}_i \bar{b}_j$ with the entry $c_{i,j}$ of a coefficient matrix $C \in \mathbb{C}^{d_\mathrm{A} \times d_\mathrm{B}}$. According to the *singular value decomposition*, any complex matrix can be decomposed as $C = UDV^\dagger$, with unitary matrices $U \in \mathbb{C}^{d_\mathrm{A} \times d_\mathrm{A}}$, $V \in \mathbb{C}^{d_\mathrm{B} \times d_\mathrm{B}}$, and a diagonal matrix $D \in \mathbb{C}^{d_\mathrm{A} \times d_\mathrm{B}}$ with nonnegative entries $d_{k,k} \in \mathbb{R}$. With $d \coloneqq \min\{d_\mathrm{A}, d_\mathrm{B}\}$, we obtain

$$|\psi_{\mathrm{AB}}\rangle = \sum_{k=1}^{d} \sum_{i,j} u_{i,k} d_{k,k} v^*_{k,j} \left|\bar{a}_i, \bar{b}_j\right\rangle = \sum_{k=1}^{d} d_{k,k} \left|a_k, b_k\right\rangle , \tag{2.19}$$

where in the last step we defined $|a_k\rangle \coloneqq \sum_i u_{i,k} \left|\bar{a}_i\right\rangle$, $|b_k\rangle \coloneqq \sum_j v^*_{k,j} \left|\bar{b}_j\right\rangle$. Orthonormality of the *Schmidt basis* is guaranteed by the unitarity of U and V. Finally, as $d_{k,k}$ are nonnegative and real, we may identify them with $\sqrt{p_k}$. ∎

Given a state ρ_{AB} of a composite system, a natural question that arises is how the state of the respective subsystems $\rho_\mathrm{A}, \rho_\mathrm{B}$ can be accessed. To answer this question, we require an additional tool.

Definition 2.9 (Partial Trace)**.** *Let ρ_{AB} be the state of a system composed of two Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ with basis $\{|a_i\rangle\}_{i=1}^{d_A}, \{|b_j\rangle\}_{j=1}^{d_B}$, respectively. The partial trace over subsystem B is defined by*

$$tr_B\left(\rho_{AB}\right) \coloneqq \sum_{i,i'=1}^{d_A} \sum_{j=1}^{d_B} \langle a_i, b_j| \, \rho_{AB} \, |a_{i'}, b_j\rangle \, |a_i\rangle\langle a_{i'}| \, , \tag{2.20}$$

which yields the reduced density operator $\rho_A \coloneqq tr_B\left(\rho_{AB}\right)$ of subsystem A.

Consider a pure two-qubit state $\rho_{\mathrm{AB}} = |\phi^+\rangle\langle\phi^+|$, with $|\phi^+\rangle \coloneqq \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$. The reduced density matrix of system A is given by

$$\rho_\mathrm{A} = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) = \frac{1}{2}\mathbb{1} . \tag{2.21}$$

Hence, the partial trace of a pure state can result in a completely mixed state. This example leads us to a general statement regarding the inverse transformation.

Proposition 2.10 (Purification)**.** *Consider a system A and an auxiliary system X with associated Hilbert spaces $\mathcal{H}_A, \mathcal{H}_X$, respectively. Let ρ_A be a state on system A. Then, there exists a pure state $|\psi_{AX}\rangle \in \mathcal{H}_{AX}$, called the purification of ρ_A, such that*

$$tr_X\left(|\psi_{AX}\rangle\langle\psi_{AX}|\right) = \rho_A . \tag{2.22}$$

Proof. Let $\{|a_i\rangle\}_{i=1}^{d}$ be an orthonormal basis of $\mathcal{H}_\mathrm{A}$ that admits the spectral decomposition $\rho_\mathrm{A} = \sum_i p_i |a_i\rangle\langle a_i|$. Take an additional Hilbert space $\mathcal{H}_X$ of equal dimension with orthonormal basis $\{|x_i\rangle\}_{i=1}^{d}$ and define the state

$$|\psi_{\mathrm{AX}}\rangle \coloneqq \sum_i \sqrt{p_i} \left|a_i, x_i\right\rangle . \tag{2.23}$$

The partial trace over the auxiliary system reveals

$$\begin{aligned} \mathrm{tr}_\mathrm{X}\left(|\psi_{\mathrm{AX}}\rangle\langle\psi_{\mathrm{AX}}|\right) &= \sum_{i,j} \sqrt{p_i p_j} \, |a_i\rangle\langle a_j| \, \mathrm{tr}\left(|x_i\rangle\langle x_j|\right) \\ &= \sum_i p_i \, |a_i\rangle\langle a_i| = \rho_\mathrm{A} . \end{aligned} \tag{2.24}$$

Hence, the state $|\psi_{\mathrm{AX}}\rangle$ is indeed the purification of ρ_A. ∎

2.5.1. Entanglement and Separability

The consideration of multiple quantum systems allows us to introduce one of the most intriguing and puzzling features of quantum mechanics.

Definition 2.11 (Entanglement, Separability)**.** *A mixed quantum state ρ_{AB} is called separable, if there exists a convex combination of pure product states $|\psi_i, \varphi_i\rangle\langle\psi_i, \varphi_i|$, with $|\psi_i\rangle, |\varphi_i\rangle \in \mathcal{H}_A, \mathcal{H}_B$, respectively, such that*

$$\rho_{AB} = \sum_i p_i \, |\psi_i, \varphi_i\rangle\langle\psi_i, \varphi_i| \, . \tag{2.25}$$

Otherwise, ρ_{AB} is called entangled.

A famous example of bipartite qubit entangled states are the *Bell states*

$$|\phi^{\pm}\rangle \coloneqq \frac{1}{\sqrt{2}} \left(|00\rangle \pm |11\rangle\right) \quad \text{and} \quad |\psi^{\pm}\rangle \coloneqq \frac{1}{\sqrt{2}} \left(|01\rangle \pm |10\rangle\right) . \tag{2.26}$$

For more than two parties, the terminology of entanglement and separability has to be refined. Consider multiple parties, labeled according to the index set $\mathcal{I} \coloneqq \{1, \ldots, n\}$. A *partition* of $\mathcal{I}$ is a set $\{\mathcal{I}_i\}_i$ of disjoint subset $\mathcal{I}_i \subseteq \mathcal{I}$ such that $\mathcal{I} = \dot{\bigcup}_i \mathcal{I}_i$. A state is called separable w.r.t. to the partition $\{\mathcal{I}_i\}_i$ if it is of the form

$$\rho = \sum_j p_j \bigotimes_i \rho_{j,\mathcal{I}_i} . \tag{2.27}$$

If every index subset $\mathcal{I}_i$ contains exactly one label, ρ is called *fully separable* and every state which cannot be expressed as a convex combination of a fully separable states is entangled. A state is *biseparable* if the partition contains only two subsets $\mathcal{I}_i$ and *genuinely multipartite entangled* states cannot be decomposed into a sum of biseparable states. The pure n-qubit Greenberger-Horne-Zeilinger (GHZ) state [GHZ89]

$$|\mathrm{GHZ}_n\rangle \coloneqq \frac{1}{\sqrt{2}} \left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right) , \tag{2.28}$$

is an example for a genuinely multipartite entangled state.

2.6. Quantum Channels

The defining property of a *unitary operator* $U \in \mathcal{L}(\mathcal{H})$ is $U^\dagger = U^{-1}$. They are required to describe the time evolution of a *closed* quantum system, i.e., a system that is perfectly isolated from the environment.

Postulate 4. *The time evolution of a closed quantum system initialized in state $|\psi(t_0)\rangle$ is described by a unitary operator $U(t, t_0)$, that is, $|\psi(t)\rangle = U(t, t_0) \, |\psi(t_0)\rangle$.*

However, in reality there is always an interaction of the quantum system with its environment and we speak of an *open* quantum system. Postulate 4 can be employed to describe the dynamics of an open system, if we consider the environment as part of the quantum system. Let $\{|e_i\rangle\}_i$ be an orthonormal basis of the Hilbert space $\mathcal{H}_\mathrm{E}$ associated to the environment, which is in a pure state $|e_0\rangle$ at some initial time.[1] Assume that the state of the total system can be prepared in a product state $\rho \otimes |e_0\rangle\langle e_0|$. The quantum dynamics of the total system is governed by a unitary operator U. After this evolution, we trace out the degrees of freedom of the environment and obtain,

$$\mathcal{E}(\rho) \coloneqq \sum_i \langle e_i| U\left(\rho \otimes |e_0\rangle\langle e_0|\right) U^\dagger |e_i\rangle = \sum_i K_i \rho K_i^\dagger, \tag{2.29}$$

the *operator-sum representation of the quantum operation* $\mathcal{E}$ with the *Kraus operators* $K_i \coloneqq \langle e_i| U |e_0\rangle$ for all i. To make the notion of quantum operations more precise, let us define:

Definition 2.12 ((Completely) Postitive Map)**.** *Let $\mathcal{H}$ be a Hilbert space. A linear map $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}), M \mapsto \mathcal{E}(M)$ is a positive map, if $\mathcal{E}(M) \geqslant 0$ for all $M \geqslant 0$. Beyond that, $\mathcal{E}$ is a completely positive map if $(id_X \otimes \mathcal{E})(M) \geqslant 0$ for all $M \geqslant 0$, where id_X denotes the identity map on an additional system $\mathcal{H}_X$ of arbitrary dimension.*

For quantum mechanics, we require $\mathcal{E}$ to be a completely positive (CP) map. This stronger notion ensures the positivity of the state after operations performed on subsystems. A quantum operation $\mathcal{E}$ is *trace-preserving* (TP) if $\mathrm{tr}(\mathcal{E}(M)) = \mathrm{tr}(M)$ for all $M \in \mathcal{L}(\mathcal{H})$. In terms of Kraus operators, $\mathcal{E}$ is TP if and only if $\sum_i K_i^\dagger K_i = \mathbb{1}$, which follows immediately from

$$\mathrm{tr}\Big(\mathcal{E}(M)\Big) = \sum_i \mathrm{tr}\Big(K_i M K_i^\dagger\Big) = \mathrm{tr}\Big(\sum_i K_i^\dagger K_i M\Big), \tag{2.30}$$

where we used linearity of the trace function and its invariance under cyclic permutation. Quantum channels or quantum operations are CPTP maps that map an input state ρ to an output state $\mathcal{E}(\rho)$.

2.6.1. Depolarizing Noise

To make quantum operations more accessible, consider as an example the operator-sum representation of the *depolarizing* noise channel $\mathcal{E}_\mathrm{depol}$, that affects a qubit system. The Kraus operators are given by [NC10]

$$K_0 = \sqrt{1 - \frac{3p}{4}}\mathbb{1} \quad \text{and} \quad K_i = \frac{\sqrt{p}}{2}\sigma_i \quad \text{for } i \in \{1,2,3\}, \tag{2.31}$$

where $p \in [0,1]$ denotes the *noise parameter*. The Pauli matrices are Hermitian and square to the identity, hence the completeness relation $\sum_{i=0}^3 K_i^\dagger K_i = \mathbb{1}$ is satisfied.

[1] As we did not specify the dimension of $\mathcal{H}_\mathrm{E}$, it is not restrictive to assume that the environment is initialized in a pure state $|e_0\rangle$, cf. Prop. 2.10.

Consider the pure, equally weighted qubit state $|+\rangle \coloneqq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, corrupted by $\mathcal{E}_{\text{depol}}$. A straightforward calculation shows

$$\begin{aligned}\mathcal{E}_{\text{depol}}(|+\rangle\langle+|) &= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) + \frac{1-p}{2}(|0\rangle\langle 1| + |1\rangle\langle 0|) \\ &= \frac{1}{2}\begin{pmatrix} 1 & 1-p \\ 1-p & 1 \end{pmatrix}. \end{aligned} \tag{2.32}$$

The depolarizing noise affects the off-diagonal elements and for maximal noise $p = 1$, the state becomes the completely mixed state $\frac{1}{2}\mathbb{1}$.

2.7. Elements of Information Theory

We conclude this chapter with some fundamental definitions and notions for information processing tasks. We follow Ref. [NC10] and define:

Definition 2.13 (Shannon Entropy [Sha48])**.** *Let $\boldsymbol{p} \coloneqq \{p_i\}_i$ be a probability distribution for a random variable $\mathcal{X}$ with possible values $\{x_i\}_i$. The Shannon entropy of $\mathcal{X}$ (or of $\boldsymbol{p}$) is defined by*

$$H(\mathcal{X}) \equiv H(\boldsymbol{p}) \coloneqq -\sum_i p_i \log_2(p_i). \tag{2.33}$$

The Shannon entropy measures the average amount of uncertainty inherent to random variable $\mathcal{X}$. We write

$$h(p) \coloneqq -p\log_2(p) - (1-p)\log_2(1-p) \tag{2.34}$$

for a binary-valued random variable $\mathcal{X}$ and call h the *binary entropy*. For two random variables $\mathcal{X}$ and $\mathcal{Y}$, with values $\{x_i\}_i$ and $\{y_j\}_j$ governed by a joint probability distribution $\{p(x_i, y_j)\}_{i,j}$, we define the *joint* and *conditional* entropy,

$$H(\mathcal{X},\mathcal{Y}) \coloneqq -\sum_{i,j} p(x_i,y_j)\log_2 p(x_i,y_j) \quad \text{and} \tag{2.35a}$$

$$H(\mathcal{X}|\mathcal{Y}) \coloneqq H(\mathcal{X},\mathcal{Y}) - H(\mathcal{Y}), \tag{2.35b}$$

respectively. The conditional Shannon entropy quantifies the average amount of uncertainty of the value of $\mathcal{X}$, conditioned on the information one has about the value of $\mathcal{Y}$. This becomes meaningful, if the random variables are *correlated*.

Definition 2.14 (Correlation)**.** *Let $\mathcal{X}, \mathcal{Y}$ be two random variables with possible values $\{x_i\}_i, \{y_j\}_j$, respectively, governed by a joint probability distribution $\{p(x_i, y_j)\}_{i,j}$. The random variables $\mathcal{X}$ and $\mathcal{Y}$ are called uncorrelated if and only if all joint probabilities factorize into a product of their respective marginal probabilities, that is,*

$$p(x_i, y_j) = p(x_i)\,p(y_j) \quad \forall i, j. \tag{2.36}$$

Otherwise, they are correlated.

A quantifier of the average amount of information one can obtain about $\mathcal{X}$ based on the knowledge about $\mathcal{Y}$ and vice versa is the *mutual information*

$$H(\mathcal{X}:\mathcal{Y}) \coloneqq H(\mathcal{X}) + H(\mathcal{Y}) - H(\mathcal{X},\mathcal{Y}) = H(\mathcal{X}) - H(\mathcal{X}|\mathcal{Y}). \tag{2.37}$$

The maximization of the mutual information $H(\mathcal{X}:\mathcal{Y})$ over all possible ways to infer $\mathcal{X}$ from $\mathcal{Y}$ is called *accessible information*. Interestingly, the accessible information is fundamentally different in classical and in quantum information theory. To make this statement more formal, let us define the quantum version of the Shannon entropy.

Definition 2.15 (Von Neumann Entropy)**.** *Let ρ be a density matrix. The Von Neumann entropy is defined as*

$$S(\rho) \coloneqq -tr(\rho \log_2(\rho)), \tag{2.38}$$

which becomes $S(\rho) = -\sum_i \lambda_i \log_2(\lambda_i)$, with the spectral decomposition of ρ.

Now consider two parties, Alice and Eve, and suppose Alice has a random variable $\mathcal{X}$ with values $\{x_i\}_{i=1}^d$ according to a probability distribution $\{p_i\}_{i=1}^d$. Eve's task is to access the value x_i of $\mathcal{X}$, guided by Alice who sends a (possibly mixed) state drawn from a set $\{\rho_i\}_{i=1}^d$ according to $\{p_i\}_{i=1}^d$. Eve performs a measurement described by POVM elements $\{E_v\}_v$ on the states she receives and obtains results $\{v_j\}_j$ from $\mathcal{V}$. In general, she cannot perfectly distinguish between the states ρ_i. For any measurement, her accessible information is upper bounded by the *Holevo quantity* $\chi(\mathcal{X}:\mathcal{V})$ [Hol73], that is,

$$H(\mathcal{X}:\mathcal{V}) \leqslant \chi(\mathcal{X}:\mathcal{V}) \coloneqq S(\rho) - \sum_{i=1}^{d} p_i S(\rho_i), \tag{2.39}$$

where $\rho = \sum_i p_i \rho_i$. If $\rho = \frac{1}{d}\sum_{i=1}^d |i\rangle\langle i|$ is a completely mixed state of orthogonal states $|i\rangle$, Eve can obtain maximal information. In this case, her accessible information saturates the Holevo bound (2.39). The Von Neumann entropy of a pure state vanishes and it is maximal for completely mixed state, hence

$$\chi(\mathcal{X}:\mathcal{V}) = S\left(\sum_{i=1}^{d} \frac{1}{d} |i\rangle\langle i|\right) - \sum_{i=1}^{d} \frac{1}{d} S(|i\rangle\langle i|) = \log_2(d). \tag{2.40}$$

Quantum communication with orthogonal states is classical in the sense that they can be perfectly distinguished. However, the fact that the quantum accessible information can be *smaller* than the information prepared by Alice, literally invites us to exploit quantum mechanics for cryptographic tasks.

Chapter 3

Bell Nonlocality and Bell Inequalities

Bell's theorem [Bel64b], in its essence, states that any physical theory incorporating *local hidden variables* – entities hidden from the grasp of quantum mechanics which determine the properties of nature – is in discord with the predictions of quantum mechanics.

Local-hidden-variable (LHV) theories are based on profound assumptions in classical physics. Beyond the axiom of *free will*, an LHV theory postulates [EPR35]:

Locality. An event can only be causally affected by events which lie in the interior of its past light cone.

Realism. Properties in nature exist independent of our understanding and observation. The value of any measurable quantity of a physical system is well defined, independent of measurements.

Via these assumptions, Bell derived inequalities consisting of correlator functions which are bounded in any LHV theory [Bel64a]. A violation of such bounds by any type of correlations unambiguously proves the *nonclassical* nature of them. Quantum theory allows for such correlations and therefore contradicts at least one of the assumptions of an LHV theory. In principle, it is justified to abandon either one of them and there is no general consensus up to this day, see for instance [Leg08, GG99]. However, we (and the majority of quantum information scientists) opt to drop the locality assumption and speak of the *nonlocality* of quantum theory. The merit of Bell inequalities lies in their ability to identify nonlocal correlations in a mathematically precise fashion.

We open this chapter with Sec. 3.1 which surveys the best known example of Bell inequalities, the Clauser-Horne-Shimony-Holt (CHSH) inequality [CHSH69]. Afterwards, we briefly discuss the general Bell setting and review generalizations of the CHSH case in Sec. 3.2. We primarily focus on multipartite Bell inequalities of which we discuss two examples in Sec. 3.3. Section 3.4 outlines experimental realizations of Bell inequality violation. In Sec. 3.5 we discuss different types of correlation. We will learn that the description of the set of quantum correlations is a nontrivial task. To this end, we require a numerical tool which is the subject of Sec. 3.6.

3.1. The CHSH Inequality and the Tsirelson Bound

Let us consider the most simple, yet nontrivial Bell inequality [CHSH69]. The CHSH inequality is of particular importance, as for example the vast majority of quantum cryptographic tasks that rely on a Bell inequality violation, is either tailored to or depends on the CHSH inequality [Eke91, HHH96, ABG+07, AMPS16]. We thus want to pay particular attention to this Bell setup and properly introduce it.

A rather intuitive access to this Bell inequality is provided in terms of a game that two parties play [BCP+14]. The rules of this game are simple. An unbiased third party, the referee, sends binary values $x \in \{0,1\}$ and $y \in \{0,1\}$ to Alice and Bob, respectively, which are chosen uniformly at random. After receiving the bit values, Alice and Bob have to answer to the referee a binary value $a \in \{0,1\}$ and $b \in \{0,1\}$. The two parties win one round of this game if and only if

$$a \oplus b = x \cdot y, \tag{3.1}$$

where $\oplus$ denotes the addition modulo 2. The task of Alice and Bob is to maximize their winning probability p^{win}. There is no communication allowed during the game, but they can agree on a strategy before the game starts. The truth table, Table 3.1, reveals, that the best strategy is to always answer both 0 (or 1), which maximizes their winning probability, that is, $p^{\text{win}}_{\text{max}} = \frac{3}{4}$ and thus $p^{\text{lose}}_{\text{min}} = \frac{1}{4}$.

Table 3.1: The truth table of the CHSH game.

x	y	$x \cdot y$	$a_x \oplus b_y$
0	0	0	$a_0 \oplus b_0$
0	1	0	$a_0 \oplus b_1$
1	0	0	$a_1 \oplus b_0$
1	1	1	$a_1 \oplus b_1$

Let us move away from the *deterministic* strategy where Alice and Bob always output the same value. The expectation value $E(a_x, b_y) \coloneqq P(a = b|x,y) - P(a \neq b|x,y)$ is the difference between the probability that Alice and Bob answer the same value and the probability that their values are unequal, conditioned on the inputs x and y. We are now in the position to formulate the CHSH inequality:

$$\mathcal{B}_{\text{CHSH}} \coloneqq |E(a_0,b_0) + E(a_1,b_0) + E(a_0,b_1) - E(a_1,b_1)| \leqslant 2, \tag{3.2}$$

where the upper bound corresponds to $4\left(p^{\text{win}}_{\text{max}} - p^{\text{lose}}_{\text{min}}\right) = 2$ which is called the *classical* or *local bound*. In any LHV model, the CHSH value $\mathcal{B}_{\text{CHSH}}$ cannot exceed this bound, in contrast to correlations of quantum origin as we will show in the following.

Let Alice and Bob measure two dichotomic observables A_x and B_y with eigenvalues ± 1 for $x, y \in \{0,1\}$ and spectral decomposition

$$A_x = A^+_x - A^-_x \quad \text{and} \quad B_y = B^+_y - B^-_y. \tag{3.3}$$

Here, $A_x^{\pm}, B_y^{\pm}$ denote the rank-1 projectors onto the respective eigenstates. Depending on the inputs x and y, a measurement of a quantum system in state ρ is implemented. The conditional probability that their outcomes coincide and mismatch are given by

$$P(a = b|x,y) = \mathrm{tr}\left(A_x^{\pm} \otimes B_y^{\pm} \rho\right) \quad \text{and} \quad P(a \neq b|x,y) = \mathrm{tr}\left(A_x^{\pm} \otimes B_y^{\mp} \rho\right), \tag{3.4}$$

respectively. Therefore, we can write $E(a_x, b_y) = \mathrm{tr}(A_x \otimes B_y \rho) = \langle A_x \otimes B_y \rangle_\rho$. Now let $\rho = |\phi^+\rangle\langle\phi^+|$ be the pure Bell state in Eq. (2.26) and

$$A_0 = \sigma_z, \quad A_1 = \sigma_x, \quad B_0 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}, \quad \text{and} \quad B_1 = \frac{\sigma_z - \sigma_x}{\sqrt{2}}, \tag{3.5}$$

be the observables of Alice and Bob. A straightforward calculation shows that the Bell value for the CHSH inequality (3.2) is $\mathcal{B}_{\mathrm{CHSH}} = 4\frac{1}{\sqrt{2}} = 2\sqrt{2}$, which violates the classical bound and thus demonstrates the nonlocality of quantum correlations.

The maximum Bell value attainable with quantum correlations for a specific Bell setting is the *Tsirelson bound* [Tsi80]. This brings us to the following theorem, which we present here without proof.

Theorem 3.1 (Tsirelson [Tsi80])**.** *Let $\{A_x\}_{x=0}^{\alpha-1}$ and $\{B_y\}_{y=0}^{\beta-1}$ be two sets of observables with eigenvalues in $[-1,1]$. Then, for any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ there exist real normalized vectors $\{\boldsymbol{v}_x\}_{x=0}^{\alpha-1}, \{\boldsymbol{w}_y\}_{y=0}^{\beta-1} \in \mathbb{R}^{\alpha+\beta}$, such that*

$$\langle A_x B_y \rangle_{|\psi\rangle} = \boldsymbol{v}_x^T \boldsymbol{w}_y \quad \forall \; x \in \{0,\dots,\alpha-1\}, y \in \{0,\dots,\beta-1\}. \tag{3.6}$$

This theorem allowed Tsirelson to prove that the maximum quantum value for the CHSH inequality is $2\sqrt{2}$. We verify this via the method presented in [EKB13]. As $\alpha = \beta = 2$, there exist unit vectors $\boldsymbol{v}_0, \boldsymbol{v}_1, \boldsymbol{w}_0, \boldsymbol{w}_1 \in \mathbb{R}^4$, which we write into $\boldsymbol{V} = (\boldsymbol{v}_0, \boldsymbol{v}_1)^T$ and $\boldsymbol{W} = (\boldsymbol{w}_0, \boldsymbol{w}_1)^T$, such that

$$\mathcal{B}_{\mathrm{CHSH}} = \sum_{x,y=0}^{1} (-1)^{x\cdot y} \langle A_x B_y \rangle_{|\psi\rangle} = \sum_{x,y=0}^{1} (-1)^{x\cdot y} \boldsymbol{v}_x^T \boldsymbol{w}_y = \boldsymbol{V}^T G \boldsymbol{W}, \tag{3.7}$$

where $G \coloneqq \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \mathbb{1}^4$. An upper bound on Eq. (3.7) is established by

$$\boldsymbol{V}^T G \boldsymbol{W} \leqslant \left|\boldsymbol{V}^T G \boldsymbol{W}\right| \leqslant |\boldsymbol{V}| \, \|G\|_\infty \, |\boldsymbol{W}| = 2\sqrt{2}. \tag{3.8}$$

In the last step, we used $|\boldsymbol{V}| = |\boldsymbol{W}| = \sqrt{2}$ which follows from the normalization of $\boldsymbol{v}_i$ and $\boldsymbol{w}_j$. We also introduced the *spectral norm* $\|\cdot\|_\infty$ which is the largest singular value of a matrix. As G is hermitian, its singular values are given by absolute value of its eigenvalues, which are either $\sqrt{2}$ or $-\sqrt{2}$. Hence, $\|G\|_\infty = \sqrt{2}$. The bound in Eq. (3.8) is tight, as we already discussed an example with Bell value $2\sqrt{2}$, cf. Eq. (3.5).

3.2. General Bell Setting

Since their discovery, Bell inequalities are at forefront of foundational research regarding quantum mechanics and quantum correlations. It is thus useful to develop new Bell inequalities and employ them not only for purposes of quantum information tasks, but also to gain a deeper and more profound understanding about the implications of quantum mechanics. To ease notation, we consider a *symmetric* Bell setting, where each party measures m different k-valued observables and we denote such a Bell inequality as (n, m, k)-Bell inequality [BBB$^+$12]. Furthermore, *full-correlation Bell inequalities* are inequalities that exclusively consist of full-correlation functions, i.e, k-valued functions that include all n parties, and where all k values can, in principle, be attained, in particular for a fixed measurement settings. Full-correlation $(n, m, 2)$-Bell inequalities are so-called *CHSH-type inequalities*. Figure 3.1 illustrates a general symmetric (n, m, k)-Bell setup.

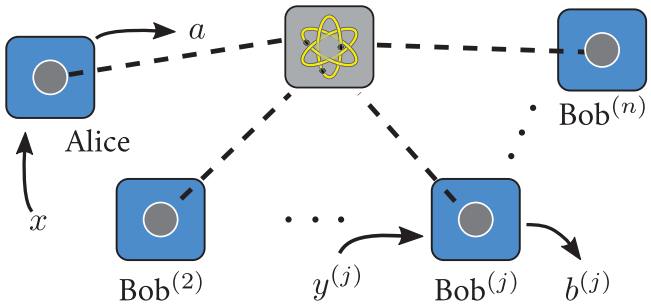

Figure 3.1: A generic symmetric Bell setting consisting of n parties called Alice and Bob$^{(j)}$ for $j \in \{2, \ldots, n\}$. A quantum source repeatedly distributes a state to all parties, which perform measurements on their share of the global state specified by an input $x, y^{(j)} \in \{0, \ldots, m-1\}$. Each measurement yields one of k different results $a, b^{(j)} \in \{0, \ldots, k-1\}$. After many repetitions, a correlator function such as the conditional probability $P\big(a, b^{(2)}, \ldots, b^{(n)} \big| x, y^{(2)}, \ldots, y^{(n)}\big)$ can be estimated.

Generalizations of the CHSH inequality were achieved into full-correlation Bell inequalities for multiple parties $(n, 2, 2)$ [WW01], multiple inputs $(2, m, 2)$ [Pea70, BC90], multiple outputs $(2, 2, k)$ [CGL$^+$02], and the $(2, m, k)$ case [BKP06]. A unified full-correlation (n, m, k)-Bell expression is introduced in [BBB$^+$12], which reproduces the aforementioned generalizations.

Regarding the derivation of the Tsirelson bound of a Bell inequality, we want to stress that the approaches of Tsirelson [Tsi80] and the ones presented in Refs. [Weh06, EKB13] are only applicable to bipartite CHSH-type inequalities. Beyond that, little is known. For arbitrary Bell inequalities, there is no general methodology that yields a tight analytical Tsirelson bound. It was only achieved in some cases as for example in [WW01] for $n \geqslant 2$ and in [SAT$^+$17] for $m \geqslant 2, k \geqslant 2$. Numerically, however, one can establish an upper bound on the Tsirelson bound, which we discuss in Sec. 3.6.

3.3. Two Examples for Multipartite Bell Inequalities

Primarily, we focus on multipartite Bell inequalities with two binary observables on each site. Here, we discuss two important examples: The Mermin-Ardehali-Belinskiĭ -Klyshko (MABK) inequality [Mer90, Ard92, BK93] and the Parity-CHSH inequality [RMW19].

3.3.1. MABK Inequality

The MABK inequality is a rather straightforward generalization of the CHSH inequality (3.2) to the multipartite case. To introduce them, we label the n parties Paul$^{(j)}$ for $j \in \{1, \ldots, n\}$ and define [RMW18]:

Definition 3.2 (MABK Operator)**.** *Let $P_i^{(j)}$ for $i \in \{0, 1\}$ be dichotomic observables of party $j \in \{1, \ldots, n\}$. By recursion, the MABK operator is defined via*

$$M_2 \coloneqq \frac{1}{2}\left[P_0^{(1)} \otimes \left(P_0^{(2)} + P_1^{(2)}\right) + P_1^{(1)} \otimes \left(P_0^{(2)} - P_1^{(2)}\right)\right], \tag{3.9a}$$

$$M_n \coloneqq \frac{1}{2}\left[M_{n-1} \otimes \left(P_0^{(n)} + P_1^{(n)}\right) + \overline{M}_{n-1} \otimes \left(P_0^{(n)} - P_1^{(n)}\right)\right] \quad \forall \; n \geqslant 3, \tag{3.9b}$$

where $\overline{M}_{n-1}$ is obtained from M_{n-1} by inverting the measurement input of all observables, i.e., by replacing $P_0^{(j)}$ with $P_1^{(j)}$ and vice versa for all $j \in \{1, \ldots, n-1\}$.

Note the CHSH structure in the recursive definition in Eqs. (3.9). Via the MABK operator, we obtain the MABK inequality for $n \geqslant 2$,

$$\mathcal{M}_n \coloneqq \left|\mathrm{tr}\left(M_n \rho\right)\right| \leqslant 2^{\frac{m-1}{2}} \quad \forall \; m \in \{1, \ldots, n\}, \tag{3.10}$$

where m denotes the maximum cardinality of parties which are entangled via the state ρ [WW00]. Hence, a Bell value above the bound $2^{\frac{m-1}{2}}$ certifies entanglement of at least m parties. The classical bound corresponds to $m = 1$, which cannot be exceeded by fully separable states. On the other hand, $m = n$ leads to the Tsirelson bound and for $m = n - 1$ the MABK inequality represents a *Svetlichny inequality* [Sve87], which can only be violated by genuinely multipartite entangled states.

As an instructive example, let us consider the 3-MABK inequality

$$\frac{1}{2}\left|\left\langle A_0 B_0^{(2)} B_1^{(3)}\right\rangle + \left\langle A_0 B_1^{(2)} B_0^{(3)}\right\rangle + \left\langle A_1 B_0^{(2)} B_0^{(3)}\right\rangle - \left\langle A_1 B_1^{(2)} B_1^{(3)}\right\rangle\right| \leqslant 1 \leqslant \sqrt{2} \leqslant 2, \tag{3.11}$$

where we renamed the three parties Alice, Bob$^{(2)}$, and Bob$^{(3)}$. The bounds 1, $\sqrt{2}$, and 2 are the classical, the Svetlichny, and the Tsirelson bound, respectively. The Tsirelson bound can be saturated with the 3-GHZ state, cf. Eq. (2.28), with measurement observables that *have* to be chosen in the σ_x-σ_y plane of the Bloch sphere. One choice that saturates the Tsirelson bound is given by

$$A_0 = \sigma_x = B_0^{(2)} = B_1^{(3)} \quad \text{and} \quad A_1 = \sigma_y = B_1^{(2)} = -B_0^{(3)}. \tag{3.12}$$

Due to structure of the MABK test, the optimal measurements cannot contain contributions in σ_z direction. Let us make this more precise and consider the pure 3-GHZ state $\chi_3 = |\mathrm{GHZ}_3\rangle\langle\mathrm{GHZ}_3|$, which is given by

$$\chi_3 = \frac{1}{2^3}\left(\mathbb{1}^{\otimes 3} + \sigma_z\sigma_z\mathbb{1} + \sigma_z\mathbb{1}\sigma_z + \mathbb{1}\sigma_z\sigma_z + \sigma_x^{\otimes 3} - \sigma_x\sigma_y\sigma_y - \sigma_y\sigma_x\sigma_y - \sigma_y\sigma_y\sigma_x\right), \tag{3.13}$$

a normalized sum of products of Pauli operators. The *weight* of such operators is the number of nontrivial Pauli operators it contains. Now take $A_0 = \sigma_z$ and consider the correlator $\langle A_0 B^{(2)}_{y^{(2)}} B^{(3)}_{y^{(3)}}\rangle_{\chi_3}$, where

$$B^{(j)}_{y^{(j)}} \coloneqq \boldsymbol{\beta}^{(j)T}_{y^{(j)}}\boldsymbol{\sigma} = \sum_{i=1}^{3} \beta^{(j)}_{y^{(j)},i}\sigma_i\,, \quad \text{with} \qquad \left\|\boldsymbol{\beta}^{(j)}_{y^{(j)}}\right\| = 1, \quad j \in \{2,3\}, \tag{3.14}$$

are general qubit observables. Due to the Pauli product relation (2.10), operators in the χ_3 state, Eq. (3.13), with full Pauli weight lead to either σ_y or σ_x on Alice's site. Both operators are traceless and hence the respective contribution to the expectation value vanishes. Likewise, every contribution of operators with non-full Pauli weight in Eq. (3.13) vanishes, because at least one Pauli operator remains in the full-correlator. In total, we find $\langle A_0 B^{(2)}_{y^{(2)}} B^{(3)}_{y^{(3)}}\rangle_{\chi_3} = 0$, which prevents the 3-MABK value in Eq. (3.11) from exceeding the classical bound. We can make a stronger statement for general Bell inequalities with qubit measurements:

Remark 3.3. *Full-correlator expressions in any Bell inequality with an odd number of parties that contain at least one observable equal to σ_z vanish, given the n-GHZ state is measured.*

Consequently, odd-partite, full-correlation Bell inequalities cannot be maximally violated via σ_z measurements on the n-GHZ state. In Ref. [HMKB19], App. C, we discuss this property in full depth for the MABK inequality. Based on these results we developed in Ref. [HKB19], App. E, a genuine multipartite Bell inequality which can be maximally violated with Pauli-σ_z measurements. Furthermore, it contains the Parity-CHSH inequality as a subclass, which we introduce in the following section.

3.3.2. Parity-CHSH Inequality

In Ref. [RMW19], the Parity-CHSH inequality is introduced in terms of a nonlocal game. To put this inequality into perspective and identify it as a subclass of our Bell inequality, we establish here the actual inequality in terms of expectation values. The rules of the game are similar to the CHSH case in Sec. 3.1. A referee sends inputs to Alice and all Bobs. However, all Bobs except the first one only receive one input. All parties report a binary value to the referee. They win the game if and only if

$$a \oplus b^{(2)} = x \cdot \left(y^{(2)} \oplus \bar{b}\right), \quad \text{where} \quad \bar{b} \coloneqq \bigoplus_{j=3}^{n} b^{(j)}. \tag{3.15}$$

For $\bar{b} = 0$, the game is identical to the CHSH game, cf. Ref [RMW19]. For $\bar{b} = 1$, however, it is not clear how to exactly phrase the game in terms of expectation values. To develop this, let us consider the tripartite case with a third party Bob$^{(3)}$ and let $\bar{b} = b^{(3)} = 1$. According to Eq. (3.15), the parties win the game if they announce $a = b^{(2)}$ for $(x, y^{(2)}) \in \{(0,0),(0,1),(1,1)\}$. Because of $\bar{b} = 1$, the input pair $(x, y^{(2)}) = (1,0)$ plays the role of the $(1,1)$ input in the CHSH game, cf. Table 3.1. The 3-Parity-CHSH inequality can thus be written as two CHSH inequalities for Alice and Bob$^{(2)}$, conditioned on different measurement results of the third party. In terms of qubit observables, the 3-Parity-CHSH operator is given by

$$\left[\sum_{x,y^{(2)}=0}^{1} (-1)^{x\cdot y^{(2)}} A_x B^{(2)}_{y^{(2)}}\right] B^{(3)+} + \left[\sum_{x,y^{(2)}=0}^{1} (-1)^{x\cdot (y^{(2)}\oplus 1)} A_x B^{(2)}_{y^{(2)}}\right] B^{(3)-}, \tag{3.16}$$

where $B^{(3)\pm}$ denotes the projector on the ± 1 eigenstate of observable $B^{(3)}$, and the measurement results are relabeled according to $+1 \to 0$ and $-1 \to 1$. The expression (3.16) can be simplified with $B^{(3)\pm} = \frac{\mathbb{1}\pm B^{(3)}}{2}$. This leads us to

$$\mathcal{B}^{(3)}_{\text{Parity}} \coloneqq \left\langle A_1 \left(B^{(2)}_0 - B^{(2)}_1\right) B^{(3)} \right\rangle + \left\langle A_0 \left(B^{(2)}_0 + B^{(2)}_1\right)\right\rangle \leqslant 2 \leqslant 2\sqrt{2}, \tag{3.17}$$

which is the Parity-CHSH inequality for $n = 3$ parties. From here on, the generalization to n parties is straightforward. We define:

Definition 3.4 (Parity-CHSH Inequality)**.** *Let $A_x, B^{(2)}_{y^{(2)}}$, and $B^{(j)}$ for $x, y^{(2)} \in \{0,1\}$ and $j \in \{3,\dots,n\}$ be binary observables. The Parity-CHSH inequality is defined as*

$$\mathcal{B}^{(n)}_{\textit{Parity}} \coloneqq \left\langle A_1 \frac{B^{(2)}_0 + B^{(2)}_1}{2} \bigotimes_{j=3}^{n} B^{(j)} \right\rangle - \left\langle A_0 \frac{B^{(2)}_0 - B^{(2)}_1}{2} \right\rangle \leqslant 1 \leqslant \sqrt{2}, \tag{3.18}$$

for all $n \geqslant 2$, with classical bound 1 and Tsirelson bound $\sqrt{2}$.

Note that we substituted $A_0 \to -A_0$ and $B^{(2)}_1 \to -B^{(2)}_1$, which merely represents a relabeling of measurement results, and we divided the inequality by two. These changes allow a straightforward identification of the Parity-CHSH inequality as a subclass of the Bell inequality in Ref. [HKB19], App. E.

In summary, the multipartite Parity-CHSH game corresponds to two bipartite CHSH games, for $\bar{b} \in \{0,1\}$. In terms of expectation values, this translates to a slight modification of the CHSH inequality (3.2). The Parity-CHSH inequality (3.18) maintains the core of the original CHSH inequality and nonlocality can be certified by an effective bipartite Bell test, depending on the measurement results of the other parties.

3.4. On the Experimental Violation of Bell Inequalities

To unequivocally falsify LHV models as an accurate description of nature, a *loophole-free* experimental demonstration of a Bell inequality violation is needed. Loopholes are rather subtle obstacles which could, in principle, explain the nonlocality of correlations within a classical model [Pea70]. Two important loopholes are the detection and the locality loophole, which are open in a Bell test with detectors of insufficient efficiencies and Bell tests where measurement events are not spacelike separated. See Ref. [BCP+14] for a thorough discussion. In order to close loopholes, the experimental demands increase, as meticulous timing and highly efficient devices are required. Because of this, loophole-free Bell tests of high statistical relevance were performed only recently [HBD+15] and [GVW+15], where the violation of a Bell inequality via entangled electron spins and entangled photons, respectively, is reported.
However, many experiments with less strict regulations regarding loopholes and on various platforms were performed. All of them substantiate the nonlocal nature of quantum theory. For example, Refs. [FC72, AGR82, CMA+13] and [RKM+01] demonstrated a Bell inequality violation via entangled photons and trapped ions, respectively. The latter can be read-out with high efficiency and is thus robust with respect to the detection loophole. Furthermore, genuine multipartite nonlocality via an MABK inequality violation is reported in Refs. [PBD+00, ZYC+03, EMSF+14] with photonic three- or fourpartite GHZ state.

3.5. Classical, No-signaling, and Quantum Correlations

Generally, we categorize the different types of correlations according to their origin. We follow Ref. [BCP+14] and consider a bipartite Bell setting in which Alice and Bob perform measurements specified by inputs $x, y \in \{0, \dots, m-1\}$ and outputs $a, b \in \{0, \dots, k-1\}$. The Bell setting is completely characterized by the set $\boldsymbol{P} \coloneqq \{P(a,b|x,y)\}_{a,b,x,y}$ of all joint conditional probabilities which we refer to as a *behavior*. For a fixed Bell setting, a behavior defines a subspace $\mathcal{C} \subset \mathbb{R}^{m^2k^2}$. A behavior is a set of probabilities. Thus, first constraints on the boundaries of $\mathcal{C}$ are imposed by the conditions of positivity $P(a,b|x,y) \geqslant 0$ and normalization $\sum_{a,b=0}^{k-1} P(a,b|x,y) = 1$ for all x, y. For more specific statements, the origin of correlations are decisive for the boundaries of $\mathcal{C}$. We distinguish between classical, no-signaling, and quantum correlations, see also Fig. 3.2.

(i) Classical. Correlations of classical origin form a convex polytope $\mathcal{P}$ [Pit89], that is, the convex hull of a finite number of extremal points $\boldsymbol{v}_i \in \mathbb{R}^{m^2k^2}$, so-called *vertices*, which correspond to all possible deterministic assignments of outputs to inputs. Every classical behaviour can thus be written as

$$\boldsymbol{P}_{\text{cl}} = \sum_i \lambda_i \boldsymbol{v}_i, \quad \text{with} \quad \sum_i \lambda_i = 1, \quad \lambda_i \geqslant 0 \ \ \forall\ i. \tag{3.19}$$

Conversely, every behavior which admits no such decomposition is nonlocal and violates at least one Bell inequality.

(ii) No-signaling. In a spacelike separated setup, superluminal communication cannot be achieved between Alice and Bob. In terms of correlations this can be expressed by the no-signaling constraints [Tsi80, PR94],

$$\sum_{b=0}^{k-1} P(a,b|x,y) = P(a|x) \quad \forall a,x,y \quad \text{and} \tag{3.20a}$$

$$\sum_{a=0}^{k-1} P(a,b|x,y) = P(b|y) \quad \forall b,x,y, \tag{3.20b}$$

which state that the marginal probability distribution of Alice is independent of Bob's input y and vice versa. The set of all correlations satisfying the no-signaling constraints form a convex polytope $\mathcal{N}$.

(iii) Quantum. A behavior is quantum if there exist a quantum state ρ_{AB} and measurement operators $\{E_{a|x}\}_{a,x}$ and $\{E_{b|y}\}_{b,y}$ which describe the performed measurement in the sense of the measurement postulate 2. We will make this more precise in the subsequent section. The set of all quantum behaviors forms a convex set $\mathcal{Q}$, but it is *not* a polytope. The boundaries of $\mathcal{Q}$ are still unknown in spite of analytical efforts to describe it [PPK+09, FSA+13].

See Fig. 3.2 and the caption of it for a visualization and further explanations.

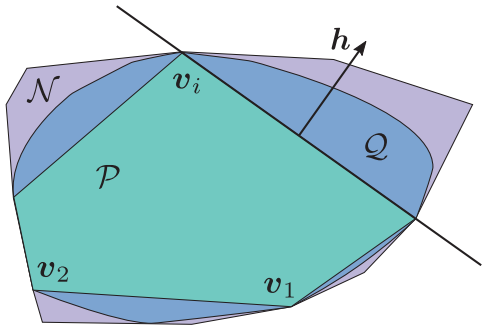

Figure 3.2: A graphical representation of a two-dimensional section of the no-signaling polytope $\mathcal{N}$, the convex quantum set $\mathcal{Q}$, and the classical polytope $\mathcal{P}$, adapted from [BCP+14]. Note the strict inclusions $\mathcal{P} \subset \mathcal{Q} \subset \mathcal{N}$. The boundaries of the classical polytope sharply separate local and quantum correlations and therefore represent tight Bell inequalities in terms of probabilities. Hyperplanes, defined by a normal vector $\boldsymbol{h}$, thus represent Bell inequalities.

3.6. A Numerical Tool: Hierarchy of Semidefinite Programs

In this section, we introduce a powerful and extremely versatile numerical method to describe the set of quantum correlations $\mathcal{Q}$, the Navascués-Pironio-Acín (NPA) hier-

archy [NPA07, NPA08]. Applications for this numerical toolbox are manifold, most notably it allows to upper bound the Tsirelon bound of an arbitrary Bell inequality and, as we will see in Chap. 5, it allows us to bound the information an eavesdropper has access to.

3.6.1. Introduction to Semidefinite Programming

First, we require the basics of semidefinite programming (SDP) for which we closely follow [NPA08, VB96]. In SDPs a linear objective function is optimized over convex constraint functions and it can be formulated as

$$\begin{aligned} &\text{maximize} && \operatorname{tr}(F_0 Z), && \text{(3.21a)}\\ &\text{subject to} && \operatorname{tr}(F_i Z) = c_i, \quad \forall i \in \{1,\dots,s\}, && \text{(3.21b)}\\ & && Z \geqslant 0, \end{aligned}$$

which is known as the *primal problem*. The problem variable is the Hermitian matrix $Z \in \mathbb{C}^{r\times r}$ and the problem parameters or problem data are the Hermitian matrices F_0, $F_i \in \mathbb{C}^{r\times r}$ and scalars c_i. The variable Z is *primal feasible* if $\operatorname{tr}(F_i Z) = c_i$ for all $i \in \{1,\dots,s\}$ and $Z \geqslant 0$. It is *strictly primal feasible* if $Z > 0$ instead of $Z \geqslant 0$.

Every primal problem has its *dual*, which is a minimization of a linear function of $\boldsymbol{x} = (x_1,\dots,x_s)^T$ subject to constraints stipulated by an affine combination of F_i,

$$\begin{aligned} &\text{minimize} && \boldsymbol{c}^T \boldsymbol{x}, && \text{(3.22a)}\\ &\text{subject to} && F(\boldsymbol{x}) \coloneqq \sum_{i=1}^{s} x_i F_i - F_0 \geqslant 0. && \text{(3.22b)} \end{aligned}$$

The variable $\boldsymbol{x}$ is *dual feasible* if $F(\boldsymbol{x}) \geqslant 0$ and *strictly dual feasible* if $F(\boldsymbol{x}) > 0$.

The solution of the dual problem provides useful bounds on the optimal value for the primal solution and vice versa. To see this, define the optimal primal and dual solutions

$$p^* \coloneqq \sup\{\operatorname{tr}(F_0 Z) \mid Z \geqslant 0,\ \operatorname{tr}(F_i Z) = c_i\ \forall i \in \{1,\dots,s\}\} \quad \text{and} \tag{3.23a}$$

$$d^* \coloneqq \inf\{\boldsymbol{c}^T \boldsymbol{x} \mid F(\boldsymbol{x}) \geqslant 0\}. \tag{3.23b}$$

Let Z and x be primal and dual feasible, respectively. Then,

$$\boldsymbol{c}^T \boldsymbol{x} - \operatorname{tr}(F_0 Z) = \sum_{i=1}^{m} \operatorname{tr}(F_i Z)\, x_i - \operatorname{tr}(F_0 Z) = \operatorname{tr}(F(x) Z) \geqslant 0 \tag{3.24}$$

and therefore $p^* \leqslant d^*$, which proves the *weak duality* between the primal and dual problem. For *strong duality* $p^* = d^*$, the existence of a strictly feasible primal point Z or dual point $\boldsymbol{x}$ is a sufficient condition [VB96].

Semidefinite programs represent a vast generalization of linear programs, while remaining efficiently solvable, in part due to the duality discussed above. Importantly, a hierarchy of SDPs can approximate the solution of polynomial optimization problems. This makes the transition to the NPA hierarchy.

3.6.2. The Navascués-Pironio-Acín Hierarchy

The question Refs. [NPA07, NPA08] address is the following: Given a behavior $\boldsymbol{P}$, do there exist local measurement operators and a quantum state that reproduce the behavior $\boldsymbol{P}$, i.e., is the behavior of quantum origin? Instead of directly seeking a quantum realization for a given behavior, which in full generality is a difficult task, in part because the dimensions of the quantum system can be unbounded, a family of weaker conditions is considered. Each condition represents a *level* of the NPA hierarchy that can be formulated as an SDP. Any behavior that satisfies the conditions in *all* levels is necessarily of quantum origin. Conversely, if a condition is not fulfilled, we can rule out the quantum origin of the behavior.

Let $|\psi\rangle \in \mathcal{H}$ be a pure state and $\{E_{a|x}\}_{a,x}$, $\{E_{b|y}\}_{b,y}$ be sets of projective measurement operators for Alice and Bob, respectively. A quantum behavior is a set of conditional probabilities

$$\boldsymbol{P} = \{P(a,b|x,y)\}_{a,b,x,y}, \quad \text{such that} \quad P(a,b|x,y) = \langle\psi| E_{a|x} \otimes E_{b|y} |\psi\rangle \tag{3.25}$$

for all a, b, x, y. As we did not specify the dimension of $\mathcal{H}$, we can assume the state to be pure and the measurements to be projective, recalling the purification and the Naimark extension in Chap. 2.

Let further $\mathcal{O} \coloneqq \{O_1, \ldots, O_r\}$ be a set of r operators O_i, which contains all projectors $E_{a|x}, E_{b|y}$ and (depending on the level of the hierarchy) additionally some linear combinations of finite products of these projectors. By construction, $\Gamma_{ij} \coloneqq \langle\psi| O_i^\dagger O_j |\psi\rangle$ is a linear function of probabilities $P(a,b|x,y)$. All coefficients Γ_{ij} form the *moment matrix* $\Gamma \in \mathbb{C}^{r\times r}$ associated to the set $\mathcal{O}$. If $\boldsymbol{P}$ is a quantum behavior, Γ fulfills:

(i) The moment matrix is positive semidefinite, i.e., $\Gamma \succcurlyeq 0$.
(ii) The entries Γ_{ij} fulfill a set of linear equalities that depend on the behavior $\boldsymbol{P}$, cf. the SDP constraints (3.28b).
(iii) The behavior $\boldsymbol{P}$ defines a subset of entries Γ_{ij}.

For a given unspecified behavior $\boldsymbol{P}$, the existence of such a moment matrix Γ is a necessary condition for the behavior to be of quantum origin.

Consider the CHSH setting as an example, see also [NPA07]. Let $|\psi\rangle$ be a quantum state and define the set

$$\mathcal{O} \coloneqq \{E_{a|x}, E_{b|y}\}_{a,b,x,y\in\{0,1\}}, \tag{3.26}$$

which contains all projective measurement operators $E_{a|x}, E_{b|y}$. The behavior $\boldsymbol{P}$ consists of 2^4 conditional probabilities $P(a,b|x,y)$. A necessary condition for this set of probabilities to admit a quantum representation, is the existence of real symmetric and positive semidefinite moment matrix $\Gamma \succcurlyeq 0$ of the form

$$\Gamma = \begin{pmatrix} Q & P \\ P^T & R \end{pmatrix}, \quad \text{with} \quad Q, R, P \in \mathbb{R}^{4\times 4}. \tag{3.27}$$

As argued, entries of the moment matrix Γ are probabilities, where the submatrix P contains all 2^4 probabilities $P(a,b|x,y)$. The submatrices Q and R are ordered such that the diagonal entries are the marginal probabilities for Alice and Bob, respectively. That is, for $x = x'$ the elements of Q are $Q_{a,a'} = \delta_{a,a'} P(a|x)$. For $x \neq x'$ and $a = a'$, the entries of Q are undetermined as they correspond to non-commuting measurements on the same subsystem, which cannot be measured simultaneously. If $\boldsymbol{P}$ is a quantum behavior, however, one can add a value $\langle\psi| E_{a|x} E_{a'|x'} |\psi\rangle$ to this entry, such that $\Gamma \geqslant 0$. The same arguments hold for R. An SDP checks if it is possible to complete Γ in this way.

Going back to the general discussion, we call a moment matrix Γ that fulfills properties (i) to (iii) a *certificate* associated to $\mathcal{O}$. The existence of such a certificate can be verified by the solution of the SDP [NPA08]

$$\begin{aligned} \text{maximize} \quad & \nu, && \text{(3.28a)} \\ \text{subject to} \quad & \operatorname{tr}(F_i \Gamma) = g_i(\boldsymbol{P}), \quad \forall i \in \{1,\dots,s\}, && \text{(3.28b)} \\ & \Gamma - \nu \mathbb{1} \geqslant 0, \end{aligned}$$

where Eq. (3.28b) is the set of linear constraints mentioned in item (ii) above. If a certificate Γ exists, the SDP (3.28) finds a positive solution $\nu \geqslant 0$. On the other hand, a negative solution $\nu < 0$ identifies the behavior as nonquantum.

Now let $\mathcal{O}_q$ contain operators that are nontrivial products of at most q of the projectors $E_{a|x}$ and $E_{b|y}$. The set of behaviors $\{\boldsymbol{P}_q\}$, for which a *certificate of order* q in terms of the moment matrix Γ^q associated to $\mathcal{O}_q$ exists, defines a subspace $\mathcal{Q}_q$ of the probability space that contains $\mathcal{Q}$. The SDPs which check for the existence of a certificate Γ^c for $c \in \{1,\dots,q\}$ give rise to the sequence $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \cdots \supseteq \mathcal{Q}_q$ of outer approximations of the true quantum set $\mathcal{Q}$. The limit of approximations becomes $\lim_{q\to\infty} \mathcal{Q}_q = \mathcal{Q}$ and we can state the main result of Ref. [NPA08].

Theorem 3.5. *Let $\boldsymbol{P}$ be a behavior such that there exists a certificate Γ^q of order q for all $q \geqslant 1$. Then $\boldsymbol{P} \in \mathcal{Q}$.*

See Ref. [NPA08] for the proof and Fig. 3.3 for a graphical representation of the NPA hierarchy.

The certificates of order q impose with increasing hierarchy level q stronger conditions on the behavior $\boldsymbol{P}$ to not be identified as nonquantum. In other words, if there exists a certificate of order q for a behavior $\boldsymbol{P}$, then there necessarily exists a certificate of order q' for all $q' < q$. As the numerical resources increase with the hierarchy level, the canonical way to search for a certificate of a given behavior $\boldsymbol{P}$ is to start with the first level and proceed in increasing order in the hierarchy. Fortunately, the numerical calculations often converge already at a low hierarchy level and the computation can be aborted if a desired numerical precision is achieved. Within this precision, the quantumness of a given behavior is then certified.

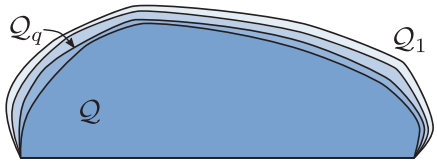

Figure 3.3: Illustration of the working principle of the NPA hierarchy, adapted from [BCP+14]. The set $\mathcal{Q}_q$ contains all behaviors $\{\boldsymbol{P}_q\}$ for which a certificate of order q exists. With increasing hierarchy level q, the approximation of the set of true quantum correlations $\mathcal{Q}$ becomes better, hence the inclusion $\mathcal{Q}_1 \supseteq \ldots \mathcal{Q}_q \supseteq \ldots \mathcal{Q}$. The better description of $\mathcal{Q}$ comes at the expense of an increased demand for numerical resources.

A Bound on the Tsirelson Bound

As an application, we now use the NPA hierarchy to upper bound the Tsirelson bound of the genuine multipartite Bell inequality we introduced in Ref. [HKB19], App. E, for $n = 3$ parties. The inequality is given by

$$\frac{1}{4}\left\langle A_1\left(B_0^{(2)}+B_1^{(2)}\right)\left(B_0^{(3)}+B_1^{(3)}\right)\right\rangle - \frac{1}{2}\left\langle A_0\left(B_0^{(2)}-B_1^{(2)}\right)+A_0\left(B_0^{(3)}-B_1^{(3)}\right)\right\rangle - \frac{1}{4}\left\langle\left(B_0^{(2)}-B_1^{(2)}\right)\left(B_0^{(3)}-B_1^{(3)}\right)\right\rangle \leqslant 1, \quad (3.29)$$

with classical upper bound 1. We are interested in an approximation of the Tsirelson bound of inequality (3.29) from above. As the NPA hierarchy optimizes over behaviors $\{\boldsymbol{P}\}$, we first translate the correlator inequality (3.29) into a Bell inequality of conditional probabilities to make the arguments more transparent. Via the spectral decomposition $A_x = A_x^+ - A_x^-$ and the completeness relation $\mathbb{1} = A_x^+ + A_x^-$ (and likewise for the Bobs), we can relate the correlators to the joint conditional +1-outcome probabilities according to:

$$\begin{aligned}\left\langle A_x B^{(2)}_{y^{(2)}} B^{(3)}_{y^{(3)}}\right\rangle_\rho &= \mathrm{tr}\left(\left(2A_x^+ - \mathbb{1}\right)\left(2B^{(2)+}_{y^{(2)}} - \mathbb{1}\right)\left(2B^{(3)+}_{y^{(3)}} - \mathbb{1}\right)\right) \quad (3.30)\\ &= 8P^{+++}_{xy^{(2)}y^{(3)}} - 4\left(P^{++}_{xy^{(2)}} + P^{++}_{xy^{(3)}} + P^{++}_{y^{(2)}y^{(3)}}\right)\\ &\quad + 2\left(P^{+}_{x} + P^{+}_{y^{(2)}} + P^{+}_{y^{(3)}}\right) - 1.\end{aligned}$$

Here, we introduced the shorthand notation

$$P^{+++}_{xy^{(2)}y^{(3)}} \coloneqq P\left(a = b^{(2)} = b^{(3)} = +1 \,\middle|\, x, y^{(2)}, y^{(3)}\right) \quad (3.31)$$

and likewise for all other probabilities. Similarly, one can relate the two-party correlators to the +1-outcome probabilities. A substitution of the correlators in the Bell

inequality (3.29) with the corresponding probabilities leads us to:

$$\begin{aligned} 1 \geqslant \mathcal{B}_P^{(3)} \coloneqq & P_{100}^{+++} + P_{110}^{+++} + P_{101}^{+++} + P_{111}^{+++} + P_{x=1}^{+} + P_{y^{(2)}=0}^{+} + P_{y^{(3)}=0}^{+} \\ & - \sum_{x,y^{(2)}=0}^{1} (-1)^{(x\oplus 1)\cdot y^{(2)}} P_{xy^{(2)}}^{++} - \sum_{x,y^{(3)}=0}^{1} (-1)^{(x\oplus 1)\cdot y^{(3)}} P_{xy^{(3)}}^{++} \\ & - P_{y^{(2)}=0,y^{(3)}=0}^{++} - P_{y^{(2)}=1,y^{(3)}=1}^{++}. \end{aligned} \tag{3.32}$$

The objective function $\mathcal{B}_P^{(3)}$ is maximized by the NPA hierarchy. Note, however, that $\mathcal{B}_P^{(3)}$ is maximized over all behaviors $\{\boldsymbol{P}\}$ which are compatible with quantum correlations at a fixed level, that is, w.r.t. all possible projective measurement operators $E_{+|x}, E_{+|y^{(2)}}, E_{+|y^{(3)}}$ and all quantum states $|\psi\rangle$ that lead to a behavior $\boldsymbol{P}$ for which a certificate of a fixed order exists. The maximization converges sufficiently well at the second level and an upper bound on the Tsirelson bound for inequality (3.32) is $g_{\text{NPA}}^{P} \approx 1.25$. This translates to the bound $g_{\text{NPA}} \approx 1.5$ in the correlator inequality (3.29). One can straightforwardly verify that the pure 3-GHZ state together with the measurement observables

$$A_0 = \sigma_z, \qquad B_0^{(j)} = \frac{\sqrt{3}}{2}\sigma_x - \frac{1}{2}\sigma_z, \qquad \text{and} \tag{3.33a}$$

$$A_1 = \sigma_x, \qquad B_1^{(j)} = \frac{\sqrt{3}}{2}\sigma_x + \frac{1}{2}\sigma_z \qquad \forall\ j \in \{2,3\}, \tag{3.33b}$$

yield 1.5 as a quantum value. Hence, we proved within numerical precision that the (tight) Tsirelson bound of inequality (3.29) is given by $g_{\text{qm}} = 1.5$.

Chapter 4

An Introduction to Quantum Key Distribution

Classical cryptography can only guarantee security of a protocol, if one assumes that the eavesdropper Eve has access to limited computational resources. Security is thus based on the computational hardness of certain mathematical problems. A famous example is the RSA encryption [RSA78], which exploits that the factorization of large numbers into primes (presumably) cannot be done in polynomial time on a classical computer.[1] In contrast, the security of quantum key distribution (QKD) is based on intrinsic and fundamental properties of quantum particles.

This chapter is designed to give an introduction to QKD and the concepts are mainly adapted from [SBPC+09, PAB+19]. To this end, we start with Sec. 4.1 in which we describe the one-time-pad encryption and prove the no-cloning theorem. Afterwards, in Sec. 4.2, we discuss the BB84 protocol in detail, as it represents the origin of (bipartite) QKD. Section 4.3 reviews an extension of QKD to multiple parties, so-called *conference key agreement*. Finally, in Sec. 4.4 we reevaluate fundamental assumptions upon which the security of QKD is built. This makes the semantic transition to Chap. 5.

4.1. One-time-pad Encryption and No-cloning Theorem

Let us consider two parties, called Alice and Bob as usual. Alice, the sender, wants to transmit a message $\boldsymbol{m}$ to the receiver Bob in a secure fashion. They can use the one-time-pad encryption [Mil82, Ver26], which is unconditionally secure under mild assumptions, that is, it provides security against an eavesdropper with unlimited computational power. The one-time pad is provably optimal in terms of required key length [Sha49]. See Fig.4.1 for a visualization and further explanations. To enable secure communication via this encryption scheme, a secure way to distribute the key $\boldsymbol{k}$ is required. This is the ultimate task of QKD.

[1] Currently, the largest integer that was factorized into prime numbers, is a 232-digit number which requires about 2000 years of computational time on a single core [KAF+10].

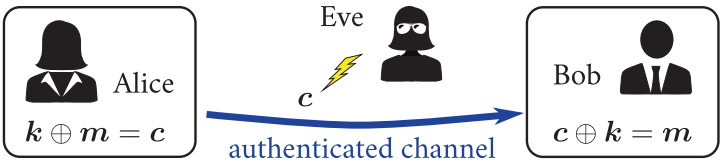

Figure 4.1: Sketch of the one-time-pad encryption. Alice and Bob are located in isolated laboratories and they can communicate via an authenticated channel. To encrypt a message $\boldsymbol{m}$ in a binary alphabet, Alice adds to $\boldsymbol{m}$ a random bit string $\boldsymbol{k}$, the key, which is of equal length as the message $\boldsymbol{m}$. This yields the cipher text $\boldsymbol{c}$, which she publicly sends via the channel to the receiver Bob. He holds a copy of the key $\boldsymbol{k}$ that was securely distributed beforehand. To recover the message $\boldsymbol{m}$, Bob adds the key $\boldsymbol{k}$ to the cipher text $\boldsymbol{c}$. Eve has full access to the cipher text $\boldsymbol{c}$, but she cannot decrypt it, because every message is equally probable from her point of view.

The following theorem describes one feature of quantum particles that allows the security of QKD protocols.

Theorem 4.1 (No-cloning [WZ82])**.** *It is not possible to perfectly clone an unknown quantum state.*

Proof. We follow [NC10] and prove this theorem by contradiction. Let $|\psi\rangle, |\varphi\rangle$ be two unknown quantum states, i.e., in general $|\psi\rangle \neq |\varphi\rangle$ and $\langle\psi|\varphi\rangle \neq 0$ holds. A unitary operator U determines the cloning procedure for $|\psi\rangle$ and $|\varphi\rangle$, which copies the states into some auxiliary state $|x\rangle$, hence

$$U|\psi\rangle|x\rangle = |\psi\rangle|\psi\rangle \quad \text{and} \quad U|\varphi\rangle|x\rangle = |\varphi\rangle|\varphi\rangle\,. \tag{4.1}$$

As $U^\dagger U = \mathbb{1}$ and $|x\rangle$ is normalized, the inner product of Eqs. (4.1) yields

$$\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2\,, \tag{4.2}$$

which is only true for $|\psi\rangle = |\varphi\rangle$ and $\langle\varphi|\psi\rangle = 0$. ∎

Quantum mechanics provides another way to guarantee security in a QKD protocol, which is the *monogamy* of entanglement [CKW00, Ter04]. That is, given ρ_{AB} is maximally entangled, it cannot be correlated to a third party. This strong form of correlation certifies security in the Ekert protocol [Eke91], which was the first entanglement-based proposal for QKD. Beyond that, monogamy of entanglement is at the heart of security in the device-independent formulation of QKD, which we thoroughly discuss in Chap. 5.

4.2. The BB84 Protocol

According to the no-cloning Theorem 4.1, we prevent the eavesdropper from perfectly cloning the quantum states by encoding the quantum information into non-

orthogonal states. This leads us to the BB84 protocol [BB84]. In its original version, the polarization of photons was used for encoding. The key distribution was a *prepare-and-measure* scheme, which we describe in the following. For now, let us neglect the effect of noise and assume that there is no eavesdropper present. The BB84 protocol consists of the following steps:

(i) Alice prepares with a single-photon source and polarizers a sequence of $2n$ signals. Each signal is a quantum state, chosen randomly from the set

$$\left\{ |{\rightarrow}\rangle\,,\ |{\uparrow}\rangle\,,\ |{\nearrow}\rangle = \frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle + |{\uparrow}\rangle\right),\ |{\searrow}\rangle = \frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle - |{\uparrow}\rangle\right) \right\}, \tag{4.3}$$

which she sends to Bob via a quantum channel.

(ii) Bob receives the states and measures them by a proper alignment of his polarizers either in the $Z \coloneqq \{|{\rightarrow}\rangle\,, |{\uparrow}\rangle\}$ or in the $X \coloneqq \{|{\nearrow}\rangle\,, |{\searrow}\rangle\}$ basis. They agree to code the bit 0 in the non-orthogonal states $|{\uparrow}\rangle$ and $|{\nearrow}\rangle$, whereas the bit 1 is coded in the non-orthogonal states $|{\rightarrow}\rangle$ and $|{\searrow}\rangle$.

(iii) After the quantum communication, Alice and Bob publicly compare their basis choice in each round. Given their choices are in discord, they discard the corresponding bit value. In the absence of noise (and perfect quantum devices), this *sifting* leads to identical keys of approximately n bits.

In Table 4.1, we give an example for a sequence in the BB84 protocol.

Table 4.1: In each round Alice and Bob choose randomly Z or X. If they choose the same basis, their results are perfectly correlated. In rounds where their basis choice does not coincide, Bob measures either 0 or 1 with equal probability, because the Z and X bases are mutually unbiased, recall Sec. 2.1. These instances are indicated by "?" and they are discarded in the sifting phase of the protocol.

Alice's Basis	X	Z	Z	Z	X	Z	X	Z	Z	Z	Z	X	X
State	$\nearrow$	$\rightarrow$	$\uparrow$	$\uparrow$	$\searrow$	$\rightarrow$	$\searrow$	$\rightarrow$	$\uparrow$	$\rightarrow$	$\uparrow$	$\nearrow$	$\searrow$
Bob's Basis	X	X	Z	Z	X	X	Z	Z	X	X	Z	X	Z
Result	0	?	0	0	1	?	?	1	?	?	0	0	?
Sifted Key	0		0	0	1			1			0	0	

A straightforward eavesdropping strategy is the *intercept-resend attack*, in which Eve randomly chooses the X or Z basis in each round as well. As Eve cannot perfectly clone non-orthogonal states, she needs to perform a measurement to obtain information. By doing so, she necessarily introduces errors in rounds where her choice is in discord with the choice of Alice. In the absence of noise, the disturbance by Eve manifests itself in measurement results for Bob (who is waiting for a signal), which can only be explained by the interaction of a third party. However, on average, Eve

guesses the correct basis in half of the measurement rounds, in which case she obtains full information without revealing her presence.

4.2.1. Entanglement-based BB84

In the entanglement-based version of the BB84 protocol [BBM92], Alice is in control of a quantum source and both parties hold measurement devices with two inputs, $x, y \in \{0, 1\}$ associated to the observables $A_0 = B_0 = \sigma_z$ and $A_1 = B_1 = \sigma_x$.

(i) In each round, the parties perform the following steps:
State preparation. Alice prepares the Bell state $|\phi^+\rangle$ and sends one qubit to Bob.
Measurements. Alice and Bob choose the inputs $x, y \in \{0, 1\}$ uniformly at random. If their choice coincides, they obtain perfectly correlated measurement results. For $x \neq y$, however, their measurement results are uncorrelated.

(ii) *Parameter estimation.* The parties publicly communicate the list of their input choices and perform the sifting procedure. A small subset of measurement outcomes for the input pairs $(x, y) \in \{(0, 0), (1, 1)\}$ is also announced. Alice and Bob check for a disturbance by Eve via the estimation of the *quantum bit error rate* (QBER)

$$Q_z \coloneqq P\left(a \neq b | x = y = 0\right) \quad \text{and} \quad Q_x \coloneqq P\left(a \neq b | x = y = 1\right), \tag{4.4}$$

which is the probability that they obtain different outcomes conditioned on a fixed measurement input. The remaining signals constitute the *raw key*.

(iii) *Classical postprocessing.* Alice and Bob evaluate their data and perform an *error-correction* protocol, which removes the discrepancies in their raw key. The final step is *privacy amplification*, which eliminates Eve's knowledge about the raw key, see Ref. [RK05, SBPC$^+$09] for details. At the end of the classical postprocessing, Alice and Bob successfully established a common and secure key.

In general, the measurement rounds in a QKD protocol can be divided in two types, raw key generation and parameter estimation, where the latter is used much less frequently [LCA05]. For key generation, the parties are inclined to use measurements and quantum states that lead to highly correlated measurement results. The data from the parameter estimation rounds are evaluated to quantify the amount of error-correction information and to bound the knowledge of Eve about the raw key. We will make these notions more precise in the following section.

4.2.2. Asymptotic Secret-Key Rate

A central task in QKD is to quantify the *secret-key rate*, which is the number of secure bits the parties can establish per time unit. This figure of merit depends on a variety of parameters, such as errors introduced by quantum devices and by the eavesdropper. Beyond that, it depends on the very structure of the QKD protocol, as well as on the number of rounds performed in the protocol. The *finite size* effects are discussed in Ref. [Ren08, SR08]. Throughout this thesis, however, we focus on the asymptotic

limit of infinitely long keys. In this case the secret-key rate has to be understood as the fraction of secure bits per time unit.

Let us calculate the asymptotic secret-key rate for the BB84 protocol. Assuming *one-way* classical postprocessing, the starting point is a lower bound known as the *Devetak-Winter rate* [DW05]

$$\begin{aligned} r &\geqslant H(A:B) - \chi(A:E) \\ &= H(A:B) - \Big(S(\rho_{\mathrm{E}}) - \sum_{a=\pm 1} P(a) S(\rho_{\mathrm{E}|a}) \Big), \end{aligned} \tag{4.5}$$

which is the difference between the mutual information $H(A:B)$, Eq. (2.37), (between Alice and Bob) and the Holevo quantity $\chi(A:E)$, Eq. (2.39), (between Alice and Eve). The reduced state $\rho_{\mathrm{E}} = \sum_a P(a) S(\rho_{\mathrm{E}|a})$ of Eve is a mixture of states $\rho_{\mathrm{E}|a}$, conditioned on the value of Alice's signal. The Devetak-Winter rate has the following interpretation: The mutual information describes the amount of information shared by Alice and Bob. Due to the action of Eve, this information is only partially secure, which is why the Holevo quantity, an upper bound on Eve's accessible information, is subtracted. In this worst-case scenario, the security of the remaining information is ensured.

For the BB84 protocol it holds, recalling the QBER Q_z in Eq. (4.4):

$$P(a,b) = \frac{Q_z}{2} \quad \text{for } a \neq b \quad \text{and} \quad P(a,b) = \frac{1-Q_z}{2} \quad \text{for } a = b, \tag{4.6}$$

and the marginal probability distributions are uniform, i.e., $P(a) = P(b) = \frac{1}{2}$ for all $a, b \in \{\pm 1\}$ and thus $H(A) = H(B) = \log_2(2) = 1$. With this, we can quantify the mutual information in terms of the parameter Q_z,

$$\begin{aligned} H(A:B) &= 2 + \sum_{a,b \text{ s.t. } a=b} P(a,b) \log_2 P(a,b) + \sum_{a,b \text{ s.t. } a\neq b} P(a,b) \log_2 P(a,b) \\ &= 2 + (1-Q_z)\left(\log_2(1-Q_z) - 1\right) + Q_z\left(\log_2 Q_z - 1\right) \\ &= 1 - h(Q_z), \end{aligned} \tag{4.7}$$

with the binary entropy h, Eq. (2.34). Intuitively, the mutual information is reduced by the rate of which mismatching measurement results occur.

For the calculation of the Holevo quantity, we follow Refs. [KGR05, RGK05]. Due to the symmetry of the BB84 protocol, it is not restrictive to assume that the final state Alice and Bob share is Bell diagonal. That is, $\rho_{\mathrm{AB}} = \sum_{i=1}^{4} \lambda_i |\phi_i\rangle\langle\phi_i|$, with $\sum_i \lambda_i = 1$. Here, we relabeled the Bell states in Eq. (2.26) according to $|\phi^{+,-}\rangle \to |\phi_{1,2}\rangle$ and $|\psi^{+,-}\rangle \to |\phi_{3,4}\rangle$. Recall that the measurement observables of Alice and Bob are σ_z and σ_x in the BB84 protocol. The QBER Q_z, Eq. (4.4), with Bell-diagonal states ρ_{AB} is calculated according to

$$Q_z = \mathrm{tr}\Big(\big(|01\rangle\langle 01| + |10\rangle\langle 10| \big) \rho_{\mathrm{AB}} \Big). \tag{4.8}$$

Perfect correlation in the σ_z basis is provided by $|\phi_{1,2}\rangle$, while $|\phi_{3,4}\rangle$ lead to perfect anticorrelations, hence $Q_z = \lambda_3 + \lambda_4$. A similar calculation leads to $Q_x = \lambda_2 + \lambda_4$. Once the quantum signal leaves the laboratory of Alice, we assume that Eve has full knowledge of the state, i.e., Eve holds the purification $|\psi\rangle_{\mathrm{ABE}} = \sum_i \sqrt{\lambda_i}\,|\phi_i\rangle\,|e_i\rangle$ of ρ_{AB}. We obtain the reduced state ρ_{AE} by partially tracing out Bob's degrees of freedom from the purification $|\psi\rangle_{\mathrm{ABE}}$. After the measurement of Alice, the system is projected into an eigenstate of $A_0 = \sigma_z$. This leads to:

$$\rho_{\mathrm{E}|a=\pm1} = \left(\sqrt{\lambda_1}\,|e_1\rangle \pm \sqrt{\lambda_2}\,|e_2\rangle\right) \text{h.c.} + \left(\sqrt{\lambda_3}\,|e_3\rangle \mp \sqrt{\lambda_4}\,|e_4\rangle\right) \text{h.c.}, \tag{4.9}$$

where h.c. is a shorthand notation for the hermitian conjugate of the expression in the preceding parenthesis. The nontrivial eigenvalues of both states in Eq. (4.9) are $\Lambda_1 \coloneqq \lambda_3 + \lambda_4$ and $\Lambda_2 \coloneqq 1 - \Lambda_1 = \lambda_1 + \lambda_2$, such that the Von Neumann entropy is

$$S\left(\rho_{\mathrm{E}|a}\right) = -\sum_{i=1}^{2} \Lambda_i \log_2 \Lambda_i = h(\Lambda_1) = h(Q_z) \quad \forall \ a \in \{\pm 1\}. \tag{4.10}$$

Since ρ_{AB} is Bell diagonal and Eve holds the purification, we have $S(\rho_{\mathrm{E}}) = S(\rho_{\mathrm{AB}}) = H(\boldsymbol{\lambda})$, where $\boldsymbol{\lambda} \coloneqq \{\lambda_i\}_{i=1}^{4}$. The Shannon entropy $H(\boldsymbol{\lambda})$ has to be chosen such that Eve's information is maximized. One finds [SBPC+09]:

$$\begin{aligned} H(\boldsymbol{\lambda}) &= h(Q_z) + (1 - Q_z)h(Q_x) + Q_z h(Q_x) \\ &= h(Q_z) + h(Q_x) \end{aligned} \tag{4.11}$$

and the asymptotic secret-key rate of the BB84 protocol becomes:

$$r \geqslant 1 - h(Q_z) - h(Q_x). \tag{4.12}$$

4.3. Extension to Conference Key Agreement

The building block in a quantum communication network is a bipartite point-to-point connection. To distribute a secure key in such a network, one can either perform multiple bipartite QKD protocols or exploit a genuinely multipartite entangled quantum resource to establish a conference key. The protocol proposed in [EKMB17] involves n parties, with three binary observables on each site. The n-QKD protocol can thus be seen as an entanglement-based multipartite generalization of the six-state protocol [Bru98]. In networks with a bottleneck architecture, such as the butterfly example [ACLY00], the n-QKD protocol can outperform multiple bipartite protocols. Here, we briefly discuss differences which arise in the multipartite extension that are important for our purposes. The quantum resource used in the n-QKD protocol is the n-GHZ state in Eq. (2.28). Recall that in the bipartite case, the pure 2-GHZ state $|\phi^+\rangle$ provides perfectly correlated measurement results, if Alice and Bob measure both in either the σ_z or in the σ_x basis. The situation is different in the multipartite case.

Theorem 4.2 (Perfect Correlation [EKMB17])**.** *For $n \geqslant 3$ qubits, the state $|\varphi_{corr}\rangle = a_0 |0\rangle^{\otimes n} + a_1 |1\rangle^{\otimes n}$ leads to perfect classical correlations between any number of parties, if and only if each of them measures in the σ_z basis.*

See [EKMB17] for the proof. The ideal quantum resource is the equally weighted n-GHZ state in Eq. (2.28) to guarantee the randomness of the final secure bit string. Another difference is the definition of the QBER Q_z, which is in the multipartite setting the probability that *at least* one Bob obtains a different measurement result w.r.t. Alice in the σ_z basis. The bipartite error rates are denoted by $Q_{\mathrm{AB}^{(j)}}$ and the noisiest channel between Alice and Bob$^{(j)}$ determines the error-correction information that Alice has to publish in the classical postprocessing step of the protocol, i.e., [EKMB17]

$$Q_z \coloneqq \max_{j\in\{2,\ldots,n\}} \left(Q_{\mathrm{AB}^{(j)}}\right). \tag{4.13}$$

4.4. Imperfections Break Security

So far, we tacitly and lightheadedly assumed that our devices behave *exactly* as we want them to. This, however, is a radical demand from our devices. Every realistic implementation is necessarily imperfect, which can be exploited by Eve to break the security of a cryptographic protocol. Subject of such adapted eavesdropping strategies, so-called *side-channel* attacks, can be any device involved in the QKD scheme. For example, the *photon-number splitting* attack [BLMS00] exploits that a realistic quantum source emits photons according to a Poissonian distribution. Another vulnerability is the dead time of single photon detectors [WKR$^+$11].

Here, we follow an example given in Ref. [PAB$^+$09], which illustrates that the security of the entanglement-based BB84 protocol critically requires that the QKD-resource state $|\psi\rangle$ is an element of a four dimensional Hilbert space $\mathcal{H}_{\mathrm{AB}}$. As already discussed, the measurements results of Alice and Bob are perfectly correlated if their input values coincide and they are uncorrelated if their inputs are in discord. In terms of expectation values this translates to

$$\langle A_x B_y \rangle_{|\psi\rangle} = \delta_{x,y} \quad \forall\ x, y \in \{0, 1\} \tag{4.14}$$

with $A_0 = B_0 = \sigma_z$ and $A_1 = B_1 = \sigma_x$. In four dimensions, the only state compatible with this statistics is the Bell state $|\phi^+\rangle$. Alice and Bob trust that the quantum source distributes the maximally entangled state $|\phi^+\rangle$ and they commence the key generation. In a larger-dimensional Hilbert space, however, even separable and thus insecure quantum states can reproduce the statistics in Eq. (4.14), as the following example shows [PAB$^+$09]. The state

$$\rho'_{\mathrm{AB}} = \frac{1}{4} \sum_{k,k'=0}^{1} \left|k, k'\right\rangle\!\left\langle k, k'\right| \otimes \left|k, k'\right\rangle\!\left\langle k, k'\right| \tag{4.15}$$

together with the extended observables $A'_0 = B'_0 = \sigma_z \otimes \mathbb{1}$ and $A'_1 = B'_1 = \mathbb{1} \otimes \sigma_z$, reproduce the statistics in Eq. (4.14).

As demonstrated, the security of the BB84 protocol is compromised if the behavior of the quantum devices behavior is different from the description of the theoretical model used in usual security proofs. This calls for a new level of security, which leads us to device-independent QKD.

Chapter 5

The Device-independent Approach to QKD

A device-independent formulation claims the highest level of security in quantum cryptography. In this approach, an exact internal characterization of any quantum device is avoided. Security is verified by data (acquired from test rounds in a protocol) that exhibits nonlocal output statistics, which witnesses the desired behavior of the quantum devices. This no-characterization approach deprives the eavesdropper of the possibility to take advantage of the malfunctions of the devices, which virtually removes the threat of side-channel attacks. Beyond that, it bridges reality and the necessarily idealized description of it. This motivates DIQKD from a practical point of view, even in the absence of an eavesdropper.

We open this chapter with Sec. 5.1 which briefly surveys different levels of security in the DIQKD and assumptions therein. Afterwards, we review a central result for this thesis in Sec. 5.2 which is a direct connection of the CHSH inequality violation to the asymptotic DI secret-key rate [PAB$^+$09]. In Sec. 5.3 an extension to DI conference key agreement (DICKA) is discussed [RMW18, RMW19]. Section 5.4 outlines how numerical bounds on the DI secret-key rate can be achieved in a general Bell setting [MPA11]. The current status of DIQKD in experiments is the subject of Sec. 5.5.

5.1. Overview and Foundations

As argued, DI security proofs require a DI witness to certify nonlocal correlations and it is thus natural, and in fact necessary, to incorporate a Bell test in a DI cryptographic protocol. The underlying physical principle that grants security is the monogamy of entanglement, which was already implicitly described in Ekert protocol [Eke91]. However, the idea to certify a certain behavior of a device via input-output correlations, so-called *self-checking*, was first put forward in [MY98]. First quantitative progress was achieved by bounding the information of a no-signaling eavesdropper about a single signal between Alice and Bob [BHK05]. This enabled subsequent publications, as for example [PAB$^+$09], in which security of a DIQKD protocol was proven under the assumption that the devices behave identically and independently (iid) in

each round. In the DI setting, however, the iid assumption is generally not justified and the first security proof in the *fully* DI setting, i.e., without the iid assumption, was established in [VV14] and improved in [AFRV19, AFDF$^+$18] by means of entropy accumulation [DFR16].

5.1.1. Different Nuances of Security

Behavior of the eavesdropper – Eve's different types of attacks are in ascending order of generality, *individual*, *collective*, and *coherent* attacks [SBPC$^+$09]. In the first two types, Eve is assumed to hold a purification $|\Psi\rangle_{\mathrm{ABE}} = |\psi\rangle_{\mathrm{ABE}}^{\otimes N}$, that is factorized in the states of each round of the protocol. She distributes the states $\rho_{\mathrm{AB}} = \mathrm{tr}_{\mathrm{E}}\left(|\psi\rangle\langle\psi|_{\mathrm{ABE}}\right)$ to Alice and Bob in every round. Furthermore, Eve performs the same attack on each signal. In individual attacks, she performs the attack before the honest parties start the classical communication. In collective attacks, Eve stores her ancillas in a quantum memory until she gathered additional information from the classical communication to optimize her attack. The most general attacks are the coherent ones, where Eve is only restricted by quantum mechanics. She can for instance entangle multiple signals and alter her strategy after intermediate steps. Eve holds the purification of the global quantum state of all N signals, i.e., $|\Psi\rangle_{\mathrm{ABE}}$ in a total Hilbert space $\mathcal{H}_{\mathrm{A}}^{\otimes N} \otimes \mathcal{H}_{\mathrm{B}}^{\otimes N} \otimes \mathcal{H}_{\mathrm{E}}$ of unknown local dimensions.
Behavior of the quantum devices – The iid assumption in particular imposes, that the devices have no internal memory which affects subsequent measurements, i.e., the measurement in round i of the protocol is only a function of the ith input. An important tool to deal with non-iid implementations is the entropy accumulation theorem (EAT). In plain terms, the EAT allows to relate Eve's uncertainty about the total output of Alice $\boldsymbol{a} = \{a_i\}_{i=1}^N$ to a sum of Eve's uncertainties about each individual output a_i, up to corrections that are of order $\sqrt{N}$ and provided the protocol is a sequential procedure [AFRV19, AFDF$^+$18].

However, we don't want to delve into the technicalities of entropy accumulation for the following reason: In Sec. 5.2, we will relate the violation of the CHSH inequality to the asymptotic DI secret-key rate under the iid assumption and given Eve performs collective attacks. As proven in Ref. [AFRV19], this key rate represents an upper bound on the key rates in the non-iid implementation and against the most general Eve. In the asymptotic limit, which we consider, the rates coincide and we can use the more accessible results of Ref. [PAB$^+$09] with a clear conscience.

5.1.2. Assumptions of DIQKD

As argued, we drop any assumptions regarding details of the inner workings of quantum devices. However, some prerequisites must be in place in order to make quantum cryptography meaningful. We assume [PAB$^+$09, RMW18]:

(i) Quantum mechanics is correct.
(ii) The laboratories of the honest parties are isolated, that is, there is no unwanted leakage of information into the environment.

(iii) Each party is in possession of a trusted, genuine random number generator. The parties trust all classical devices they use for classical data processing. They further communicate via authenticated classical channels.

(iv) Each measurement device has m inputs and generates in each round one out of k measurement results. There is no further specification of the measurement device and it could therefore be manufactured and prepared by Eve.

(v) Alice holds a quantum source which generates some unknown quantum state of arbitrary local dimension. The eavesdropper holds the purified quantum state. No further assumptions are imposed on the source and equivalently, it could be Eve who prepares and distributes the states.

(vi) There is no unwanted communication between the quantum source and the measurement device of Alice.

5.2. The Bipartite Case

The central result of Ref. [PAB+09] is a lower bound on the asymptotic bipartite DI secret-key rate. As it is essential for our work in Refs. [HKB18, HMKB19, HKB19], cf. App. A, C, and E, respectively, we want to properly introduce it. To this end, we first describe the setting under which the results are derived and review the DIQKD protocol. An upper bound on the Holevo quantity between Alice and Eve as a function of the CHSH inequality violation is presented afterwards.

5.2.1. Setting and Modified DI Ekert Protocol

Alice has an uncharacterized measurement device with two inputs $x \in \{0, 1\}$ that implements some measurement on her share of the quantum state, which outputs a binary value $a \in \{\pm 1\}$. Likewise, Bob has a black box with three inputs $y \in \{0, 1, 2\}$ with dichotomic outcomes $b \in \{\pm 1\}$. We assume that Eve performs collective attacks and the devices behave according to the iid assumption. Furthermore, the honest parties perform one-way classical postprocessing from Alice to Bob. See Fig. 5.1 for a schematic representation of the bipartite DIQKD setting.

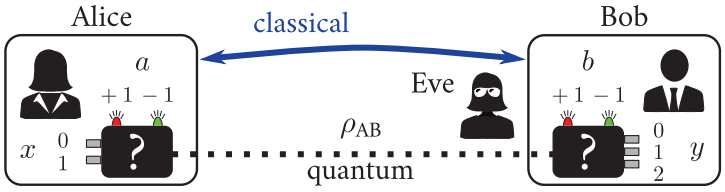

Figure 5.1: Alice and Bob are connected with a classical and a quantum channel. Eve holds the purification $|\Psi\rangle_{ABE} = |\psi\rangle_{ABE}^{\otimes N}$ and distributes in each round an uncharacterized bipartite state ρ_{AB} to Alice and Bob. The honest parties choose $x \in \{0, 1\}$ and $y \in \{0, 1, 2\}$, which implements a measurement with a binary output $a, b \in \{\pm 1\}$.

Before the protocol starts, Alice fixes the value of two parameters $\beta \in (2, 2\sqrt{2}]$ and $\delta \in (0, 2\sqrt{2} - 2)$, see also [PAB+19]. The protocol involves the following steps:

(i) *Measurements.* In each round, the parties perform a measurement on their share of an unknown quantum state ρ_{AB}. There are two types of rounds, the key generation (type-0) and the parameter estimation (type-1) round, where the latter is performed much less frequently. A preshared random key determines the type of each round. For type 0, Alice and Bob choose the input $(x, y) = (0, 2)$. In type-1 measurement rounds, the parties choose their inputs $x, y \in \{0, 1\}$ uniformly at random.

(ii) *Parameter estimation.* For all type-1 rounds, Bob sends all inputs and outputs to Alice and she estimates the CHSH value

$$S = \sum_{x,y=0}^{1} (-1)^{x \cdot y} \langle A_x B_y \rangle . \tag{5.1}$$

If $S \leqslant \beta - \delta$, Alice announces that the protocol aborts. Given that the protocol continues, the parties publicly communicate the list of inputs for type-0 rounds to generate the raw key. Bob sends the outputs for a small amount of type-0 rounds as well, with which Alice estimates the QBER

$$Q = P\left(a \neq b | x = 0, y = 2\right) . \tag{5.2}$$

The data which is used to calculate the parameters S and Q is discarded. This classical communication is not attributed to the postprocessing.

(iii) *Classical postprocessing.* Similar to a usual QKD protocol, error-correction and privacy amplification are performed.

The type-1 rounds are called *spot-checking* rounds. For this reason, the above protocol is also known as spot-checking CHSH protocol. A value $\beta - \delta$ closer to the Tsirelson bound $2\sqrt{2}$ increases the secret-key rate, as we will see. However, it comes at the expense of an increased probability that the protocol aborts.

We call an *honest implementation* of the protocol, an implementation where the devices behave in a specified way, as for example according to the iid assumption. A protocol is called ϵ^c*-complete*, if the probability that the protocol aborts in an honest implementation is at most ϵ^c. Likewise, we say a protocol is *incomplete*, if there exists no honest implementation that leads to not aborting the protocol.

5.2.2. Asymptotic DI Secret-Key Rate

In the setting described above, the asymptotic secret-key rate in the limit of $N \to \infty$ signals is lower bounded by the Devetak-Winter rate

$$r \geqslant H(A_0 : B_2) - \chi\left(A_0 : E\right) . \tag{5.3}$$

We can assume w.l.o.g. that the marginal probabilities are uniform, i.e., $\langle A_x \rangle = \langle B_y \rangle = 0$, as it can be achieved by classical postprocessing and it does not affect

the values of Q and S. Therefore, as in Sec. 4.2, the mutual information is given by $H(A_0 : B_2) = 1 - h(Q)$. The goal is now to upper bound the Holevo quantity

$$\chi(A_0 : E) = S(\rho_E) - \frac{1}{2} \sum_{a_0=\pm 1} S(\rho_{E|a_0}) \tag{5.4}$$

in terms of CHSH inequality violation, where the factor $\frac{1}{2}$ is due to the symmetrization of the marginal probability distribution $\langle A_0 \rangle = 0$.

Theorem 5.1 (Upper Bound on Holevo Quantity [PAB+09])**.** *Let $|\psi\rangle_{ABE}$ be a quantum state and $\{A_0, A_1, B_0, B_1\}$ a set of measurements, yielding a violation S of the CHSH inequality. Then, after Alice and Bob have symmetrized their marginals,*

$$\chi(A_0 : E) \leqslant h\left(\frac{1 + \sqrt{S^2/4 - 1}}{2}\right). \tag{5.5}$$

An immediate consequence is a lower bound on the DI secret-key rate in Eq. (5.3),

$$r \geqslant 1 - h(Q) - h\left(\frac{1 + \sqrt{S^2/4 - 1}}{2}\right). \tag{5.6}$$

Given the importance of Theorem 5.1, we want to outline the proof.

(i) *Reduction to qubits.* As we are not allowed to assume specifics of the Hilbert space dimension, we have to ensure that Eve's accessible information is not compromised by the reduction to qubit states. Thus, the first step is to prove that we are allowed to assume w.l.o.g., that Eve sends mixed two-qubit states $\rho_{AB} = \sum_\lambda p_\lambda \rho_\lambda$. This can be achieved by employing the structure of the CHSH test with two binary observables on each site.[1]

(ii) *Reduction to Bell-diagonal states.* It is further not restrictive to assume, that $\rho_\lambda = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ is Bell diagonal and that the measurements of Alice and Bob are carried out in the σ_z-σ_x plane.

(iii) *Upper bound.* In this step, one first calculates $\chi_\lambda(A_0 : E)$ for any Bell-diagonal state ρ_λ. We already presented a similar calculation for the BB84 protocol in Sec. 4.2. One obtains an expression that depends on the eigenvalues $\boldsymbol{\lambda}$ and the polar angle θ of Alice's general qubit observable

$$A_0 = \cos(\theta)\sigma_z + \sin(\theta)\sigma_x. \tag{5.7}$$

Next, Eve's accessible information is maximized w.r.t. θ and one finds $\theta = 0$, hence $A_0 = \sigma_z$. Therefore, the upper bound $\chi_\lambda(A_0 : E) \leqslant H(\boldsymbol{\lambda}) - h(\lambda_1 + \lambda_2)$ can be established, similar to the BB84 case, cf. Eq (4.10). This upper bound, in turn, is upper bounded by a concave function $F(S_\lambda)$ of CHSH inequality violation S_λ with a Bell-diagonal state ρ_λ. The function F is a binary entropy function in the form of the right-hand side of inequality (5.5).

[1] Note that this step can be generalized to n parties with a corresponding multipartite Bell inequality with two dichotomic observables on each side.

(iv) *Last step.* With the concavity of F, one finds

$$\chi(A_0 : E) = \sum_\lambda p_\lambda \chi_\lambda (A_0 : E) \leqslant \sum_\lambda p_\lambda F(S_\lambda) \leqslant F\Big(\sum_\lambda p_\lambda S_\lambda\Big). \tag{5.8}$$

Finally, it holds that $S \leqslant \sum_\lambda p_\lambda S_\lambda$ and for $S \geqslant 2$, F is monotonically decreasing function of S. Therefore, the right-hand side in inequality (5.8) is upper bounded by $F(S)$, which finishes the proof.

Importantly, the parameters Q and S are two independent quantities accessible from the classical data, which can be used to certify the correctness and secrecy of the exchanged key. No assumptions have to be made about the specifics of the implementation. A secret key can be extracted from the data, if it exhibits nonlocal correlations that give rise to a Bell inequality violation and if the QBER is below a certain threshold. Reference [PAB+09] provides a specific example for an honest implementation that saturates the bound in Theorem 5.1, which is thus tight.

We stress that there is *no* analytical expression for a DI secret-key rate known, which does not rely on the bound in inequality (5.6) or on the violation of the CHSH inequality.

5.3. Extension to DI Conference Key Agreement

To motivate the extension to DI conference key agreement (DICKA), we want to clarify an important subtlety, which we kept quiet about so far. Two ingredients are crucial in *any* viable DIQKD protocol. Measurements and quantum states are required that provide on one hand highly correlated measurement results to reduce the amount of error-correction information and on the other hand a maximum Bell inequality violation to certify security of the correlation between the honest parties. However, the measurement settings in different types of measurement rounds cannot be chosen arbitrarily.

Remark 5.2 (Requirements on Bell Test)**.** *At least one party, say, Alice, has to use one input for key generation* ***and*** *for spot-checking. By doing so, Alice is able to monitor the honesty of her device.* [2] *This necessitates a Bell test in which maximum violation and perfect correlation among all parties are possible at the same time.*

This requirement was first explicitly described and exploited in Refs. [HMKB19] and [HKB19], cf. App. C and E. The statement above suggests that not all Bell inequalities are suitable for DIQKD and this is in fact true as we will see in this section.

[2] Otherwise the eavesdropper, who potentially manufactured the devices, could have preprogrammed them in the following way to break the security of the protocol: Eve equips the measurement devices with quantum states that maximally violate the Bell inequality and which are measured if Alice uses the input for spot-checking rounds. On the other hand, if Alice uses her key generation input, the device always outputs a fixed binary value. In this way, Alice and Bob conclude that they share nonlocal correlations and Eve obtains full information without revealing her presence.

To this end, recall the MABK and Parity-CHSH inequality in Sec. 3.3. We will review two proposals [RMW18] and [RMW19] to achieve DICKA based on these inequalities, and we will pinpoint the reason that prevents the first proposal from being a viable option.

5.3.1. First Approach - MABK Inequality

Recall that the MABK inequality (3.10), is a full-correlation $(n, 2, 2)$-Bell inequality and it is recursively defined according to Eq. (3.9), which imprints the CHSH structure into the multipartite generalization. Thus, given an MABK value $\mathcal{M}_n > 2^{\frac{n-2}{2}}$, that is, certified genuine multipartite entanglement, one can reformulate the MABK inequality violation as violation of an effective CHSH inequality between one party and the remaining $n-1$ other parties. This is the statement of the *MABK-CHSH correspondence* [RMW18]:

$$\mathcal{M}_n > 2^{\frac{n-2}{2}} \qquad \Rightarrow \qquad \mathcal{M}_2 = \frac{\mathcal{M}_n}{2^{\frac{n-2}{2}}} > 1. \tag{5.9}$$

The security proof of the DICKA protocol in [RMW18] proceeds as follows: First the EAT is used to relate Eve's uncertainty about the total output of Alice to a sum of Von Neumann entropies evaluated on each signal, as described in [AFRV19]. The next step is to find a so-called *min-tradeoff function*, that is a differentiable function of a Bell value that bounds the single-round Von Neumann entropy. This is the challenging part. However, by identifying the violation of the MABK inequality with the violation of an effective CHSH inequality, a bound on Eve's accessible information via the tight results of [PAB$^+$09] is enabled. Exchanging the CHSH value in Eq. (5.5) with a rescaled n-MABK value then quantifies Eve's information about Alice's output.

To put achievable DI conference key rates into perspective, an honest implementation is proposed in [RMW18], which reveals the flaw of this approach. In the ideal scenario, the quantum resource distributed to all parties is the archetypical n-GHZ state. The protocol stipulates two observables for Alice, $A_0 = \sigma_z$ and $A_1 = \sigma_x$. All Bobs measure σ_z in key generation rounds and in spot-checking rounds, they measure observables that maximally violate the MABK inequality. With a combination of statements we already formalized, the fundamental problems of the honest implementation become clear. Recall:

(i) Theorem 4.2: Perfect correlation requires all parties to measure σ_z.
(ii) Remark 5.2: The structure of the Bell setting has to be such that perfect correlation and maximum violation can be achieved at the same time.
(iii) Remark 3.11: Measurements of σ_z are suboptimal to maximally violate full-correlation Bell inequalities .

The proposed honest implementation claims to allow perfectly correlated measurement results and at the same time violate the Svetlichny bound $2^{\frac{n-2}{2}}$ of the MABK inequality. Due to the arguments listed above, this is not the case, see [HMKB19],

App. C. If the parties verify genuine multipartite entanglement, the MABK-CHSH correspondence applies which guarantees security. However, in this case the parties cannot be perfectly correlated and the amount of error-correction information is too large, which thus prevents the generation of a common raw conference key. Alternatively, the parties are perfectly correlated, but then the Svetlichny bound cannot be violated and the security is breached.

Beyond the honest implementation, we proved in [HMKB19] for $n = 3$ parties via the NPA hierarchy that perfect correlation and violation of the Svetlichny bound are mutually exclusive in the MABK test. Consequently, there cannot exist *any* honest implementation that does not abort the protocol. This renders the DICKA protocol based on the MABK test incomplete.

5.3.2. Second Approach - Parity-CHSH Inequality

In Ref. [RMW19] a corrected version of the DICKA protocol is presented, which includes an adjustment of both the protocol and the Bell test. The Parity-CHSH test is compatible with constraints imposed by Theorem 4.2 and Remark 5.2. As already discussed in Sec. 3.3.2, the Parity-CHSH inequality is closely related to the CHSH inequality. It represents two CHSH inequalities (that are equivalent up to relabelling) depending on the measurement results of $n - 2$ parties. This constitutes the counterpart to the MABK-CHSH correspondence and allows again to employ the good lower bounds of the bipartite setting. The security proof then proceeds in a similar way as the former version with the MABK inequality.

In the proposed honest implementation, all parties measure σ_z in key generation rounds. For spot-checking rounds, Alice and Bob$^{(2)}$ measure

$$A_0 = \sigma_z, \quad A_1 = \sigma_x, \quad B_0^{(2)} = \frac{\sigma_z + \sigma_x}{\sqrt{2}}, \quad B_1^{(2)} = \frac{\sigma_z - \sigma_x}{\sqrt{2}}, \tag{5.10}$$

and all other Bobs measure $B^{(j\geqslant 3)} = \sigma_x$. The quantum resource is the n-GHZ state. Conditioned on the parity $\bar{b} = 0$ or $\bar{b} = 1$, cf. Eq. (3.15), the pure n-GHZ state is turned into the pure Bell state $|\phi^+\rangle$ or $|\phi^-\rangle$, respectively, between Alice and Bob$^{(2)}$. With this, they can maximally violate the respective CHSH inequalities, thereby guaranteeing security.

5.4. Quantifying DI Secret-Key Rates via NPA

In this section, we describe how the NPA hierarchy, cf. Sec. 3.6, can be used to lower bound the DI secret-key rates in terms of an observed Bell inequality violation. We follow the methods described in [MPA11]. First, we provide a different expression for the bipartite asymptotic DI secret-key rate. Multiple techniques [Ren08, TSSR11, AFDF$^+$18] reduce its calculation to

$$r \geqslant S(A|E) - H(A|B), \tag{5.11}$$

the difference between Eve's uncertainty about Alice's output, described by the conditional Von Neumann entropy $S(A|E)$, and the amount of required error-correction information quantified by the conditional Shannon entropy $H(A|B)$. In the multipartite setting [EKMB17], $H(A|B)$ is replaced by $\max_j H(A|B^{(j)})$, as explained in Sec. 4.3.

Consider a bipartite DIQKD setup, in which the honest parties exchange N signals. Eve is allowed to perform coherent attacks and she holds the purification ρ_{ABE} of the global state with $\mathrm{tr}_{\mathrm{E}}(\rho_{\mathrm{ABE}}) = \rho_{\mathrm{AB}}$. We further assume an iid implementation.[3] Let $\boldsymbol{x}_{\mathrm{r}}$ denote the string of Alice's input values to generate her outputs $\boldsymbol{a}$, the raw key. After Alice performed her measurements, her parts of the global state can be written in a classical register $|\boldsymbol{a}\rangle\langle\boldsymbol{a}|$ and the joint state between her and Eve is a *classical-quantum* (cq) state

$$\rho_{\mathrm{AE}} = \sum_{\boldsymbol{a}} P(\boldsymbol{a}|\boldsymbol{x}_{\mathrm{r}})\, |\boldsymbol{a}\rangle\langle\boldsymbol{a}| \otimes \rho_{\mathrm{E}|\boldsymbol{a}}, \tag{5.12}$$

where $\rho_{\mathrm{E}|\boldsymbol{a}}$ denotes the reduced state of Eve conditioned on the output $\boldsymbol{a}$. For cq states, the *conditional min-entropy* $S_{\min}(\boldsymbol{a}|E)$ quantifies the amount of Eve's uncertainty about the output $\boldsymbol{a}$. We gain virtually nothing by rigorously defining the min-entropy and refer to [Ren08] for details. Importantly $S(\boldsymbol{a}|E) \geq S_{\min}(\boldsymbol{a}|E)$ always holds, which is the first step towards a lower bound on $S(\boldsymbol{a}|E)$. For cq states, the min-entropy is related to Eve's *guessing probability* $P_{\mathrm{g}}(\boldsymbol{a}|E)$ according to [KRS09]

$$S_{\min}(\boldsymbol{a}|E) = -\log_2(P_{\mathrm{g}}(\boldsymbol{a}|E)), \tag{5.13}$$

where $P_{\mathrm{g}}(\boldsymbol{a}|E)$ is the maximum probability with which Eve can guess the output $\boldsymbol{a}$ conditioned on her information E. For a single binary-valued signal a_i, maximum uncertainty of Eve translates to $P_{\mathrm{g}}(a_i|E) = \frac{1}{2}$. Likewise, in case of minimal uncertainty, Eve correctly predicts every output of Alice and thus $P_{\mathrm{g}}(a_i|E) = 1$.

Our objective is to find an upper bound on $P_g(\boldsymbol{a}|E)$ to cover the worst-case scenario. Because $-\log_2(x)$ is a monotonically decreasing function of x, Eq. (5.13) then provides a lower bound on $S_{\min}(\boldsymbol{a}|E)$. Consider a single signal ($N = 1$) ρ'_{AB} which is uncorrelated to Eve and measured by Alice with outcome a. Then, Eves optimal strategy to correctly guess a is to output the most probable outcome, i.e., $P_{\mathrm{g}}(a) = \max_a P(a|x_{\mathrm{r}})$. Let G denote the Bell operator associated to the DIQKD setting[4] and let g_{obs} be the (expected) observed Bell inequality violation. We can write $P_{\mathrm{g}}(a) \leqslant f(g_{\mathrm{obs}})$, where f is a concave and monotonically decreasing function of g_{obs}. The bound $f(g_{\mathrm{obs}})$ can always be established with the NPA hierarchy and the

[3] In the DIQKD model of Ref. [MPA11], the iid assumption is necessarily fulfilled if the N signals are measured in parallel on N pairs of devices. Thus, fully DIQKD is in principle possible. However, for a realistic implementation where the raw key is generated by consecutive measurements on the same devices the iid assumption is required.

[4] For example $G_{\mathrm{CHSH}} = A_0B_0 + A_1B_0 + A_0B_1 - A_1B_1$ is the Bell operator of the CHSH inequality, which can then be written as $|\mathrm{tr}\,(G_{\mathrm{CHSH}}\rho)| \leqslant 2$.

solution of the following SDP provides the maximum possible value for $P_{\mathrm{g}}(a)$ for a fixed parameter g_{obs}:

$$\begin{aligned} &\max_{\rho'_{\mathrm{AB}}, A_x, B_y} \ \mathrm{tr}\left(A_0\, \rho'_{\mathrm{AB}}\right) \\ &\text{subject to: } \mathrm{tr}\left(G\rho'_{\mathrm{AB}}\right) = g_{\mathrm{obs}}. \end{aligned} \tag{5.14}$$

Note that the maximization is performed over all states ρ'_{AB} and observables A_x, B_y that are compatible with the observed data $\mathrm{tr}\left(G\rho'_{AB}\right) = g_{\mathrm{obs}}$.

Now consider the general case of N signals and where Eve can use her information to increase her guessing probability. Let us denote with N_{est}, the number of signals used by Alice and Bob to perform spot-checking measurements, by which they calculate the estimated Bell inequality violation g_{est}. Then, the total guessing probability is upper bounded as [MRC+14]

$$P_{\mathrm{g}}(\boldsymbol{a}|E) \leqslant \left(f(g_{\mathrm{est}}) + N_{\mathrm{est}}^{-\frac{1}{4}}\right)^N, \tag{5.15}$$

which is independent of Eve. This implies that in the asymptotic limit $N \to \infty$, a lower bound on the DI secret-key rate (5.11) is given by

$$r \geqslant -\log_2\left(f(g_{\mathrm{est}})\right) - H(A|B), \tag{5.16}$$

where $f\left(g_{\mathrm{est}}\right)$ is obtained from the solution of the SDP (5.14).

Note that we did not specify anything about the observables and states, merely an observed Bell inequality violation is required. Bounds by SDPs of the form (5.14) are thus device-independent and they are valid against the most general adversary. They are, however, often overly pessimistic. It is an open problem how to obtain tighter bounds in a general setting, numerically, as well as analytically. Recent development [TSG+19] hints at improvement with the SDP approach, by employing the full output statistics as constraints in the SDP. From the analytical side, Refs. [RMW18, RMW19] showed how relations of Bell inequalities to the CHSH inequality can enable good analytical bounds via the results presented in Sec. 5.2. Finally, recall that the upper bound on the Holevo quantity in the bipartite case, cf. Theorem 5.5, is derived by using various techniques specific to the CHSH setting. Therefore, a tailored Bell inequality for the purposes of DIQKD is a potentially fruitful approach. In Ref. [HKB19], App. E, we take a first step into this direction by introducing a genuine multipartite Bell inequality which is specifically designed for DICKA.

5.5. State-of-the-art DIQKD Experiments

While QKD is already successfully realized in the experiment and increasingly becomes commercially available (see for example Ref. [ZXC+18] for an overview), its DI counterpart faces fundamental challenges [GPS10]. In particular, because all optical Bell tests are susceptible to the detection loophole. Due to photon losses during

the transmission, not all entangled photons can be detected, which effectively compromises the detection efficiency. These non-detection events lead to post-selected measurement statistics. Post-selected data can exhibit nonlocal properties even if the origin of the correlations is in fact not nonlocal. One way to deal with this problem is to randomly assign measurement results to non-detection events [TT08], as this leads to a decrease of nonlocality. Closing the detection loophole is a crucial requirement for the implementation of a DIQKD protocol. Here, the recently demonstrated loophole-free Bell inequality violation [GVW$^+$15, HBD$^+$15] represents an advance in this direction.

In a more restricted setting where the quantum source is assumed to be well characterized and only the measurement devices are treated as black boxes (so-called *measurement DI* QKD), meaningful progress is reported in Ref. [TYC$^+$14]. Here, 10^2 secure bits per second can be established over a distance of 50 km in an MDI setting, which was improved in a follow-up work [YCY$^+$16].

A first step towards DICKA is to reliably certify multipartite entanglement in a DI manner. For up to six parties, the detection of genuine multipartite entanglement is achieved in the MDI setting in Ref. [BBS$^+$13] with the detection loophole closed.

Last but not least, in Ref. [HKB18], App. A, we consider multiple honest implementations for the spot-checking CHSH protocol to benchmark the threshold requirements for experimental parameters, such as the detector efficiency or the fidelity of the quantum resource w.r.t. to the Bell state $|\phi^+\rangle$. To access profitable DI rates, our findings highlight the necessity for experimental improvement of virtually all quantum devices involved in the DIQKD scheme.

Chapter 6

Quantum Repeaters

To exploit quantum key distribution to its full potential, a reliable method to distribute entangled states over large distances in a quantum network is required. The canonical choice for the carrier of quantum information is the photon, as it can be transmitted through optical fibers, free space, or, more generally, through a quantum channel. Such channels are necessarily lossy and in this context, photon losses are the main source of errors. These losses scale exponentially with the length L of the point-to-point connection. This is characterized by the *transmissivity*

$$\eta(L) = 10^{-\alpha \frac{L}{10}}, \tag{6.1}$$

which represents the probability that a photon is *not* lost in the channel. The *attenuation coefficient* α describes the weakening of the electromagnetic field caused by the material of the channel. For optical fibers at fixed wavelengths around 1550 nm, a minimal attenuation coefficient $\alpha \approx 0.17$ dB/km can be achieved.

Clearly, photon losses fundamentally limits any point-to-point quantum communication. Besides losses, there are other sources of errors that probabilistically alter the quantum state of the photons. Therefore, a repetition of the quantum signal at an intermediate point in the classical sense is prevented by the no-cloning theorem. This calls for a more sophisticated approach to overcome photon losses, which brings us to the *quantum repeater*.

Based on [PLOB17], we render the limitations of repeaterless quantum communication more precise in Sec. 6.1. Afterwards, in Sec. 6.2, we introduce the first quantum repeater protocol [BDCZ98] and embed it into the framework QKD. An alternative quantum repeater proposal [MLK+16] is discussed in Sec. 6.3. We conclude with Sec. 6.4 which outlines the current status of quantum repeater implementations.

6.1. Fundamental Repeaterless Bound

To identify a quantum repeater as a device that offers an advantage for quantum communication in comparison to a direct link, we first need to quantify what ultimately can be achieved with a point-to-point connection. Here, we require the notion of

the quantum capacity $C(\mathcal{E})$ of a quantum channel $\mathcal{E}$ [BDS97]. To this end, consider a bipartite setup with two remote parties Alice and Bob. Suppose Alice sequentially wants to distribute a specific *target state* ϕ via a quantum channel $\mathcal{E}$ to Bob. Due to the action of the quantum channel, however, the actually transmitted state ρ_{AB} differs from the desired target state. The parties are allowed to perform arbitrary local operations (LOs) and unlimited classical communication (CCs). These *adaptive LOCCs* assist the parties in implementing any quantum-state distribution protocol. After N uses of the channel $\mathcal{E}$, Alice and Bob share a global quantum state ρ_{AB}^{N}, which depends on the channel $\mathcal{E}$ and on the sequence of performed adaptive LOCCs. One way to characterize the performance of such a protocol, is the rate at which the protocol allows Alice to distribute a state ρ_{AB}^{N}, that is ϵ-close to the target state ϕ^{N}, i.e.,

$$\left\| \rho_{\mathrm{AB}}^{N} - \phi^{N} \right\|_{1} \leqslant \epsilon, \tag{6.2}$$

where the *trace norm* $\|\cdot\|_{1}$ of a linear operator is defined as the sum of its singular values. The maximum rate optimized over all adaptive LOCCs that the quantum channel $\mathcal{E}$ asymptotically permits, is defined as the *two-way quantum capacity* $C(\mathcal{E})$ of the channel. We refer to Ref. [PLOB17] for the formal definition of the quantum capacity, as we restrict our discussion to a specific class of channels and therefore, the general framework is not required.

As the capacity $C(\mathcal{E})$ is optimized over all LOCCs, it provides a fundamental upper bound on the amount of quantum information that Alice can asymptotically transmit to Bob. Via these benchmarks, one can unambiguously identify any type of device that supports the quantum communication between Alice and Bob as a quantum repeater. The device only has its justification as a quantum repeater, if it provides a larger quantum capacity than the direct link. In this case, we call the device *genuine* or *effective quantum repeater* [MHKB19, PAB+19].

6.1.1. Pure-Loss Channel

We focus on optical communication via free-space or fiber point-to-point connections. Suppose the quantum channel between Alice and Bob carries a single photonic mode. Let $b^{\dagger}$ denote the photonic *creation operator* which creates a photon in the mode of the channel. That is, if $|\mathrm{vac}\rangle$ denotes the vacuum state, the action of the creation operator is $b^{\dagger}|\mathrm{vac}\rangle = |1\rangle$.[1] The capacity of the *pure-loss channel* $\mathcal{E}_{\mathrm{loss}}^{(\eta)}$ is completely characterized by the transmissivity η, as we will see in Eq. (6.4). We can model its action by a beam splitter that, with probability $1-\eta$, injects the photon of the single mode of the channel into a vacuum mode of the environment. To this mode, we associate a creation operator $b_{\mathrm{E}}^{\dagger}$, i.e., the action of the pure-loss channel reads

$$\mathcal{E}_{\mathrm{loss}}^{(\eta)} : b^{\dagger} \;\mapsto\; \sqrt{\eta}\, b^{\dagger} + \sqrt{1-\eta}\, b_{\mathrm{E}}^{\dagger}. \tag{6.3}$$

[1] A thorough discussion of basic concepts of quantum optics goes beyond the scope of this thesis. We refer to Ref. [SZ99] for an in-depth and excellent introduction to quantum optics.

Now consider a quantum channel which admits the decomposition $\mathcal{E} = \mathcal{E}_{\mathrm{B}} \circ \mathcal{E}_{\mathrm{loss}}^{(\eta)} \circ \mathcal{E}_{\mathrm{A}}$ into a lossy component $\mathcal{E}_{\mathrm{loss}}^{(\eta)}$ and some arbitrary, but fixed quantum channels $\mathcal{E}_{\mathrm{A,B}}$ that describe the quantum operation on Alice's and Bob's site, respectively. The *PLOB-repeaterless bound* [PLOB17] states that the capacity of such quantum channels is upper bounded by capacity of the pure-loss channel $\mathcal{E}_{\mathrm{loss}}^{(\eta)}$, which is directly related to the transmissivity η according to:

$$C(\mathcal{E}) \leqslant C(\mathcal{E}_{\mathrm{loss}}^{(\eta)}) = -\log_2(1-\eta)\,. \tag{6.4}$$

Figure 6.1 visualizes the described notions.

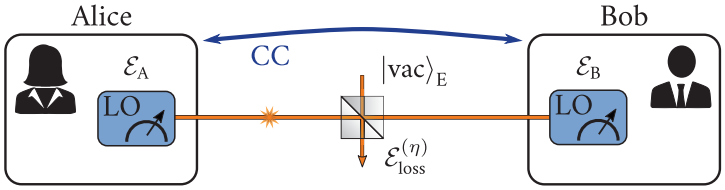

Figure 6.1: Alice wants to distribute quantum states to Bob via a pure-loss channel $\mathcal{E}_{\mathrm{loss}}^{(n)}$, which is modeled by a beam splitter that couples the photon into a vacuum mode of the environment with probability $1-\eta$. The parties perform some local operation (LO), described by the CPTP map $\mathcal{E}_{\mathrm{A,B}}$, respectively, and they can communicate via a classical channel.

In the case where the target state ϕ^N allows to establish a secret key between Alice and Bob, we call $C(\mathcal{E})$ the secret-key capacity $K(\mathcal{E})$. This puts a fundamental limit on the secret-key rate, achievable with any point-to-point link. For the pure-loss channel, $K(\mathcal{E}_{\mathrm{loss}}^{(n)}) = -\log_2(1-\eta)$ holds. In the regime of high losses $\eta \ll 1$, the secret-key capacity can be approximated as

$$K(\mathcal{E}_{\mathrm{loss}}^{(n)}) = -\log_2(1-\eta) \approx 1.44\eta, \tag{6.5}$$

that is, $K(\mathcal{E}_{\mathrm{loss}}^{(n)})$ scales linearly with the transmissivity η, which in turn is exponentially suppressed by the length of the link, cf. Eq. (6.1). This, in particular, means that the repeaterless maximum secret-key rate per optical mode is upper bounded by 1.44η bits per channel use at high loss [PAB+19]. This highlights the fundamental limitations of point-to-point (fiber-based) QKD, which is limited to some hundreds of kilometers [BBR+18]. Similar results where obtained by Ref. [TGW14].

To circumvent the detrimental impact of the channel attenuation on the photons, the total length can be split into multiple segments. This approach is at the heart of every quantum repeater concept, which leads to a series of pure-loss channels. The overall capacity of the quantum repeater (per mode) then needs to outperform the capacity of the direct link, cf. Eq. (6.4). Different quantum repeater proposals are categorized into *generations* based on their technical demands and implemented

methods to overcome loss and operational errors [MLK+16]. The first generation employs quantum memories [BDCZ98, vLLS+06, DLCZ01], from which we introduce one example in the following section. Other proposals use implemented error-correction [JTN+09, FWH+10, MKL+14], which we survey in Sec. (6.3).

6.2. The Original Quantum Repeater

In the so-called *nested* repeater scheme of Ref. [BDCZ98], the total length consists of 2^N segments of a fixed *fundamental length* $L_0 = L2^{-N}$ (see also Fig. 6.2). Entangled states are distributed among adjacent repeater stations, which are equipped with quantum memories to store the incoming entangled states, as well as with quantum processors in order to perform local operations on the quantum states. Importantly, they are able to perform so-called *entanglement swapping* (ES), which is an application of quantum teleportation [BBC+93]. In this way, the distance over which entanglement is distributed is doubled with each successful ES, at the cost of consuming quantum states as a resource. Figure 6.2 visualizes the architecture of the original quantum repeater and illustrates the notion of ES.

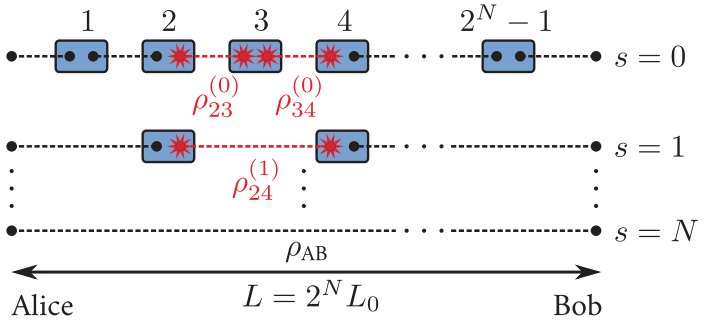

Figure 6.2: The original quantum repeater scheme [BDCZ98] with N nesting levels and $2^N - 1$ intermediate repeater stations. Entangled states which successfully connect two adjacent repeater stations at *nesting level* $s = 0$ are called *elementary links*, which are created by individual quantum sources. Once two neighboring elementary links are established, ES swapping is performed which creates an entangled link in nesting level $s = 1$. Here, this is illustrated at the third repeater station, where a Bell measurement is performed on the two subsystems stored in the quantum memories. Depending on the measurement result, a local operation is applied to the subsystem stored at the fourth repeater station. This creates an entangled link in nesting level $s = 1$ in the form of the state $\rho_{24}^{(1)}$. A consecutive execution of successful ES in N nesting levels, ultimately distributes an entangled state ρ_{AB} among two remote parties separated by the full distance L.

6.2.1. Repeater Rate

The task of the quantum repeater is to distribute entangled quantum states among Alice and Bob. A suitable figure of merit that quantifies the performance of a quantum repeater is the *repeater rate* R_{rep}, i.e., the rate at which the quantum repeater distributes entangled states to the remote parties. This quantity depends on the architecture of the quantum repeater and the quantum systems used for its implementation. The quantum repeater consists of the entire segmented line between Alice and Bob. Every building block consists of many quantum devices, including memories, sources, processors, detectors, and channels. Consequently, the repeater rate is a complicated function of the operational performance of all these quantum devices. Here, we outline some parts of the quantum repeater and address how the corresponding errors are modeled in the original quantum repeater, cf. Ref. [ABB$^+$13]. For simplicity, we assume perfect quantum memories and perfect single-qubit gates.

(i) *Quantum channel.* The segments of length L_0 are pure-loss channels, characterized by the transmissivity $\eta(L_0)$ in Eq. (6.1). Every fundamental link in nesting level $s = 0$ has a capacity that is upper bounded by $-\log_2(1-\eta(L_0))$.

(ii) *Quantum source.* An ideal quantum source generates a pure maximally entangled Bell state, as for example $|\phi^+\rangle$, Eq. (2.26), and distributes it to adjacent repeater stations i and $i+1$. The quality of the source can be described by the *quantum fidelity* $F\left(|\phi^+\rangle, \rho^{(0)}_{i,i+1}\right) \coloneqq \langle\phi^+|\,\rho^{(0)}_{i,i+1}\,|\phi^+\rangle$ [NC10], which quantifies the overlap between the distributed state $\rho^{(0)}_{i,i+1}$ and the ideal one $|\phi^+\rangle$. [2]

(iii) *Detectors.* We assume photon number resolving detectors of efficiency η_d, with measurements that can be described by POVM elements [KL10],

$$\Pi^{(n)} \coloneqq \eta_d^n \sum_{m=0}^{\infty} \binom{n+m}{n} (1-\eta_d)^m \,|n+m\rangle\langle n+m|\,, \tag{6.6}$$

associated to the detection of n photons. Here, $|n+m\rangle$ denotes the *Fock state* of corresponding photon number.

(iv) *Quantum gates.* Entanglement swapping requires controlled two-qubit operations, performed by gates of a certain quality p_G. Naturally, these gates are imperfect and introduce errors. For the original quantum repeater [BDCZ98], the depolarizing noise model,

$$\mathcal{E}(\rho) = p_G \mathcal{E}^{\text{ideal}}(\rho) + (1-p_G)\frac{\mathbb{1}}{4}, \tag{6.7}$$

is proposed, where the gate operates ideally with probability p_G. If an error occurs, however, the gate converts the state into a complete mixed state.

[2] The quality of the state can be improved by performing so-called *entanglement distillation* (ED). These additional quantum operations introduce further operational errors. For an increased overall success probability, the advantages gained via ED need to outweigh the disadvantages due to the additional operational errors. Here, we neglect the possibility of ED for the sake of simplicity and refer to Ref. [BDCZ98, BPvL11, ABB$^+$13] for further readings.

The errors introduced by the components of the quantum repeater give rise to a success probability $P_{\text{ES}}^{(i)}$ for ES swapping at nesting level i, which affects the repeater rate R_{rep}. For low success probability $P_0 \ll 1$ of establishing an elementary link, a concise expression for the repeater rate is given by [SSdRG11]

$$R_{\text{rep}} = \frac{c}{2L_0}\left(\frac{2}{3}\right)^N P_0 \prod_{i=1}^{N} P_{\text{ES}}^{(i)}, \tag{6.8}$$

where $c = 2 \times 10^8 \text{m/s}$ denotes the speed of light in the fiber.

In practice, the optimal strategy is to immediately perform ES as soon as two neighboring elementary links are established and then proceed by already distributing new states among the empty quantum memories. This approach can significantly increase the repeater rate, as numerical computations suggest. However, this is difficult to characterize analytically, in part because the success probabilities in higher nesting levels depend on the successful ES in all preceding nesting levels. In Ref. [HKB18], App. A, we derived a modified and generalized expression of the repeater rate in Eq. (6.8). In doing so, we obtain slightly higher key rates that are closer to the optimal strategy we investigated via Monte Carlo simulations.

6.2.2. Quantum Key Distribution with Quantum Repeaters

Finally, let us put the quantum repeater into the context of QKD. The repeater rate R_{rep}, Eq. (6.8), as a function of loss and operational errors, allows us to investigate the secret-key rate that Alice and Bob can achieve within the described error models. In this setting, we adopt the figure of merit of Ref. [ABB$^+$13] for the QKD protocol and call

$$R \coloneqq R_{\text{raw}} r_\infty = R_{\text{rep}} P_{\text{click}} R_{\text{sift}} r_\infty \tag{6.9}$$

the secret-key rate, which consists of the raw key rate R_{raw} and the *secret fraction* r_∞.[3] The raw key rate R_{raw} is given by the product of the repeater rate R_{rep}, the sifting rate R_{sift}, and the probability P_{click}, which we comment on in the following:

(i) The sifting rate R_{sift} describes the fraction of key generation rounds in the QKD protocol. We can achieve approximately $R_{\text{sift}} \approx 1$ in an asymmetric protocol where the type-1 measurement rounds are chosen much less frequently [LCA05].

(ii) The parameter P_{click} describes the probability that Alice and Bob detect an event that they can use for QKD. For single-photon detectors of efficiency η_d and in the usual device-dependent (DD) QKD setup, P_{click} is given by η_d^2. The situation is different in the DI setting. As already discussed for the detection loophole, cf. Sec. 5.5, we cannot ignore no-detection events. They have to be

[3] Note that in the asymptotic limit, the secret fraction corresponds to the secret-key rates we discussed in chapters 4 and 5.

incorporated into the statistics of the protocol. Usually, this is done by randomly assigning a measurement result to no-detection events [TT08]. In this sense every event is a valid QKD event, that is, $P_{\text{click}} = 1$. However, this random output guessing decreases the nonlocality of the quantum correlations between Alice and Bob. We can describe its affect by an additional error model that mixes the quantum state, e.g.,

$$\rho_{\text{AB}} \quad \longmapsto \quad \eta_d^2 \rho_{\text{AB}} + (1 - \eta_d^2) \frac{\mathbb{1}}{4}, \tag{6.10}$$

for two-qubit states ρ_{AB}.

The task is now to maximize the overall secret-key rate in Eq. (6.9). The repeater rate R_{rep} clearly depends on the actual implementation of the quantum repeater. The secret fraction r_∞, however, only depends on the type of QKD protocol that is employed by Alice and Bob. If they choose to run the BB84 protocol, we use Eq. (4.12) for r_∞. If the parties choose to run the spot-checking CHSH protocol, we use Eq. (5.6) instead. Note that in latter case, the parties assume that the entire quantum repeater is under Eve's control.

In Ref. [HKB18], App. A, we consider a scenario that allows a direct and reasonable comparison of achievable secret-key rates in the DD and DI case. By investigating multiple honest implementations, we quantify how experimental malfunctions manifest themselves in achievable DI secret-key rates.

6.3. The Third-generation Quantum Repeater

Here, we briefly address the *third-generation* or error-corrected quantum repeater, where *quantum error correction* (QEC) is used to tackle loss and operational errors. In particular, no quantum memories are required at intermediate repeater stations.

Quantum Error Correction in a Nutshell

Here, we briefly discuss the central idea of QEC and refer to [LB13] for an in-depth introduction. Consider a bipartite setup in which Alice wants to transmit a general pure qubit state $|\psi\rangle$ to Bob. Due to errors during the transmission, however, Bob receives a different state $|\psi'\rangle$, which we assume to be pure for simplicity. One approach that allows Bob to recover the original state is to send redundant quantum information. An example where this built-in redundancy is most transparent, is the *three-qubit repetition code*,

$$|0\rangle \quad \longmapsto \quad |0,0,0\rangle =: |\bar{0}\rangle \qquad \text{and} \qquad |1\rangle \quad \longmapsto \quad |1,1,1\rangle =: |\bar{1}\rangle\,, \tag{6.11}$$

where one *logical* qubit $|\bar{0}\rangle\,, |\bar{1}\rangle$ is encoded in three *physical* qubits. Under the simple assumption that only a single bit-flip error can occur, Bob is able to unambiguously identify and correct this error.

More generally, a quantum error-correcting code (QECC) encodes k logical qudits of dimension d into $n > k$ physical qudits. The logical states are the *codewords* of the QECC and span the *code space* $\mathcal{C}$ of dimension d^k, which is a subspace of the total Hilbert space $\mathcal{H} = \mathbb{C}^{d^n}$. The *code distance* δ of a QECC quantifies the maximum number t of independent errors that can be corrected according to $t \coloneqq \lfloor \frac{\delta-1}{2} \rfloor$. We call a QECC with n physical qudits, k logical qudits and distance δ an $[\![n, k, \delta]\!]_d$-QECC.

An example for a QECC is the $[\![9, 1, 3]\!]_2$-Shor code, which can correct an arbitrary single-qubit error. More sophisticated QECCs exist in the form of *quantum polynomial codes* [CGL99], where for every prime number $d \geqslant 2\delta + 1$, there exist a $[\![2\delta - 1, 1, \delta]\!]_d$-QECC. Such codes are well-suited for third-generation quantum repeaters [MZL+17, MHKB18].

Qudit Noise Model

In Sec. 2.6 we already introduced the depolarizing channel for qubits. A generalization for a qudit state ρ of dimension d is given by

$$\mathcal{E}_P : \ \rho \quad \longmapsto \quad \sum_{r,s=0}^{d-1} p_{r,s} \left(X^r Z^s\right) \rho \left(X^r Z^s\right)^\dagger , \tag{6.12}$$

also called *generalized Pauli-error channel* with Kraus operators $\left\{\sqrt{p_{r,s}} X^r Z^s\right\}_{r,s=0}^{d-1}$, that are proportional to the generalized Pauli operators defined in Eq. (2.12). In this error model, the Pauli operator $X^r Z^s$ is applied to the qudit state with probability $p_{r,s}$. This quantum channel includes the qudit depolarizing channel, in which the trivial error $X^0 Z^0 = \mathbb{1}$ occurs with probability $p_{0,0} = 1 - p(d^2 - 1)/d^2$ and all other errors are equiprobable, i.e., $p_{r,s} = p/d^2$ for all $(r, s) \neq (0, 0)$. Note that for $d = 2$, the qubit depolarizing Kraus operators in Eq. (2.31) are reproduced.

Error-corrected Qudit Quantum Repeater

We conclude this discussion with a protocol that allows the distribution of entangled states to two remote parties. Alice and Bob are connected with an error-corrected qudit repeater, that is a segmented line with $N - 1$ intermediate repeater stations, located at the intersection points of N segments of fundamental length $L_0 = L/N$. These segments are quantum channels, which we model according to the generalized Pauli-error channel introduced above. We assume that Alice, Bob, and each repeater station are equipped with a quantum source which can generate the equally weighted qudit superposition:

$$|+\rangle_d \coloneqq \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \, . \tag{6.13}$$

Furthermore, the two-qudit controlled-Z gate,

$$\mathrm{CZ} \coloneqq \sum_{k=0}^{d-1} |k\rangle\langle k| \otimes Z^k \tag{6.14}$$

is required. It applies the generalized Pauli-Z operator Z^k on the target qudit, given the control qudit is in state $|k\rangle$. The CZ gate is an example of so-called *Clifford gates* [Got99], a class of unitary operators U that transforms a generalized Pauli operator $X^r Z^s$ into $X^{r'} Z^{s'}$, with $r \neq r'$ and $s \neq s'$. An application of the CZ gate onto $|+\rangle_d^{\otimes 2}$ generates the maximally entangled two-qudit state,

$$|\Psi\rangle \coloneqq \mathrm{CZ}\,|+\rangle_d \otimes |+\rangle_d = \frac{1}{d} \sum_{j,k=0}^{d-1} \omega^{jk}\,|j\rangle \otimes |k\rangle\,, \tag{6.15}$$

recalling the definition $\omega \coloneqq e^{\frac{2\pi i}{d}}$. With these notions, we can explain the ideal qudit quantum repeater protocol supported by an illustration, see Fig. (6.3).

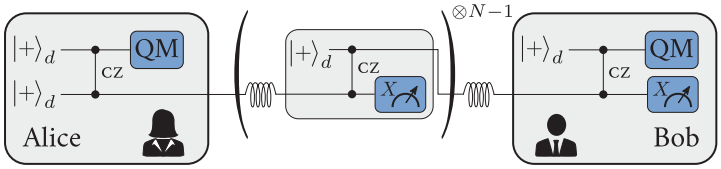

Figure 6.3: A sketch of the error-corrected qudit repeater line with $N-1$ intermediate repeater stations, adapted from Ref. [MHKB19], App. D. Alice generates the entangled two-qudit state $|\Psi\rangle = \mathrm{CZ}\,|+\rangle_d \otimes |+\rangle_d$ in Eq. (6.15), stores one qudit in her quantum memory (QM), and sends the other qudit to the first intermediate repeater station. There, an additional state $|+\rangle_d$ is prepared which is entangled with the incoming qudit via the application of a CZ gate. This step corresponds to the entanglement swapping. The qudit that already traveled $1/N$ of the total distance L, is measured in the X basis, which yields a classical outcome $c_1 \in \{0, \ldots, d-1\}$ that is communicated to Bob. Meanwhile, the fresh qudit is sent to the next repeater station, where the same procedure is repeated. Ultimately, Bob receives a list of measurement results $\{c_i\}_{i=1}^{N-1}$ from each repeater station and a qudit from repeater station $N-1$ which he entangles with a fresh $|+\rangle_d$-qudit. Again, the former qudit is measured in the X-basis which outputs a result c_N. Conditioned on all measurement results c_i, Bob applies a specific generalized Pauli operator on his remaining qudit. Upon a successful application, Alice and Bob share the entangled state $|\Psi\rangle$.

To effectively perform QEC in such a quantum repeater line, a precise understanding of how Pauli errors propagate across Clifford gates is instrumental [Got98, Got99]. An error analysis for a third-generation qubit repeater is carried out based on these propagation rules in [EKB16]. In Ref. [MHKB18], App. B, we present a generalization for error-corrected qudit quantum repeaters. In this analysis, the full error statistics of the qudit states ρ distributed to Alice and Bob is computed. This paves the way for further investigations, as for example the application of third-generation quantum repeaters for QKD in arbitrary dimensions and for a systematic analysis to identify parameter regimes, in which error-corrected qudit repeaters are able to surpass the PLOB-repeaterless bound which we present in [MHKB19], App. D.

6.4. On the Experimental Status of Quantum Repeaters

A promising new proposal for QKD beyond the PLOB bound is so-called *twin-field* (TF) QKD [LYDS18]. Here, two parties generate optical fields, with an electromagnetic phase that are sufficiently close, hence the term *twin*. The states are sent to a single middle node where they are combined and detected. This scheme already proved its usefulness for establishing a secret key and it allows to beat the PLOB bound, as recently demonstrated in a proof-of-principle experiment [MPR+19]. This demonstration represents the first prototype of a genuine quantum repeater.

The architecture of TFQKD is derived from the *Lütkenhaus protocol* [LJKL16], a simple quantum repeater line with a single middle node, equipped by two quantum memories. This proposal is a promising candidate for a near-term realization of a full-fledged quantum repeater with state-of-the-art technology. Different platforms can be used for its implementation, such as the TFQKD example or with quantum memories in the form of *nitrogen-vacancy* centers in diamonds [RYG+19]. Further analysis has been performed with the TFQKD approach, indicating that the repeaterless bound can be surpassed with so-called *decoy-state methods* [CAL19, GC19]. Last but not least, we present in Ref. [MHKB19], App. D, a systematic analysis in order to benchmark experimental requirements, such that a third-generation qudit quantum repeater can overcome the repeaterless bound.

Chapter 7

Overview of Results

This chapter summarizes the main results achieved in the course of my research. For details, I refer to the respective publications and to Appendices A to E, where my scientific contributions are described.

Appendix A
Device-independent secret-key-rate analysis for quantum repeaters

In publication [HKB18], App. A, we study achievable device-independent (DI) secret-key rates in a bipartite setting with two different quantum repeater proposals. We systematically analyse various honest implementations in the DI setting and compare it to the device-dependent (DD) counterpart. Secret-key rates depend on the employed quantum key distribution (QKD) protocol. Thus, it is crucial to identify and consider an implementation in which the DD and the DI QKD protocol are effectively equivalent. As we describe, the asymmetric versions of the BB84, cf. Sec. 4.2, and the spot-checking CHSH protocol, cf. Sec. 5.2, are equivalent in the asymptotic limit. This guarantees a fair DD-to-DI comparison, effectively independent of a possible imbalance due to the protocol. In doing so, we shed light on the fundamental differences between both scenarios.

Furthermore, our systematic analysis serves as a guideline for implementing a quantum repeater for the purposes of DIQKD, as we benchmark the threshold requirements for experimental parameters, such as the detector efficiency or the quality of the quantum states. To obtain profitable DI rates, our findings highlight the necessity for experimental improvement of virtually all quantum devices involved in the DIQKD scheme. In addition, we show that the proneness of DIQKD to imperfections implies different optimization strategies for the secret-key rate. This, in particular, limits the number of tolerable entanglement swapping (ES) procedures and thus implies a different optimal architecture of the quantum repeater in comparison to the DD case.

As a side product, we develop a slightly generalized repeater rate for quantum repeaters with probabilistic ES. This repeater rate is closer to the achievable rates

with an optimal repeating strategy, cf. Sec. 6.2.1, which we verify by means of Monte Carlo simulations.

Appendix B
Propagation of generalized Pauli errors in qudit Clifford circuits

In Ref. [MHKB18], App. B, we introduce a so-called *error probability tensor*. A useful tool to track how generalized Pauli errors in arbitrary dimensions, cf. Sec. (6.3), propagate through quantum circuits that consist of Clifford gates only. Via this error probability tensor, the full error statistics of qudit states sent through the circuit, can be computed. We apply this tool to a third-generation qudit repeater line with arbitrarily many intermediate repeater stations. This, in particular, allows us to quantify the distributed entanglement in terms of logarithmic negativity. Our analysis shows that higher dimensional qudit systems can provide an advantage in this regard.

More generally, the full knowledge about the distributed qudit states paves the way for further investigations. As for example the application for QKD under realistic noise models or the systematic analysis we perform in [MHKB19], App. D.

Appendix C
Comment on "Fully device-independent conference key agreement"

Publication [HMKB19], App. C, is a comment to the article [RMW18], which proposes a protocol to achieve device-independent conference key agreement (DICKA). The DICKA protocol is based on the MABK Bell test, recall Secs. 3.3 and 5.3, which suffers from fundamental flaws, as we explain in the article. In plain terms, the protocol allows the distribution of secret keys, which are either highly correlated but insecure or secure but uncorrelated. For DIQKD, both requirements have to be fulfilled. For odd-numbered parties, we analytically establish this incompatibility in the form of:

Theorem [HMKB19].— Let $n \geqslant 3$ be odd and let the n parties perform the honest implementation of the DICKA protocol. Then, the n-MABK value cannot exceed the bound that certifies genuine multipartite entanglement among all n parties.

Furthermore, we provide numerical evidence that the same argument holds for the even-partite case. Beyond the proposed honest implementation, we discover that this incompatibility is deeply rooted in the structure of the MABK test. Concretely, we prove via semidefinite programming (SDP), that for three parties there cannot exist measurements and quantum states that provide perfectly correlated measurement results and a sufficiently large violation of the MABK inequality at the same time. Due to the symmetry of the MABK test, we further conjecture that this fundamental incompatibility applies for all n, which renders the protocol incomplete.

Appendix D
Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters

As discussed in Sec. 6.1, point-to-point quantum communication faces fundamental limitations. The implementation of a full-fledged quantum repeater is a demanding and expensive challenge. A thorough study to identify suitable candidates and parameter regimes which allow to overcome the repeaterless bound is thus essential. In Ref. [MHKB19], App. D, we provide such a study for third-generation qudit quantum repeaters with the generalized Pauli error channel, cf. Sec. 6.3, as a noise model. We analytically devise a figure of merit, which allows the certification of a larger capacity with the repeater than the direct link in certain parameter regimes. We performed the analysis with the tools of Ref. [MHKB18], App. B, and for two different types of encoding, namely Fock and multimode encoded qudits.

Appendix E
A Genuine Multipartite Bell Inequality for Device-independent Conference Key Agreement

Bell inequalities are the cornerstone of DI security proofs. In Ref. [HKB19], App. E, we establish a novel family of genuine multipartite Bell inequalities. For $n \in \mathbb{N}$ parties, it is given by

$$\left\langle A_1 \bigotimes_{j=2}^{n} B_+^{(j)} \right\rangle - \delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \left\langle A_0 \bigotimes_{j=2}^{n} B_-^{(j)} \right\rangle - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\left\langle A_0 \otimes \sum_{\boldsymbol{\alpha}_{2k-1}^{(n)} \in \mathcal{S}_{2k-1}^{(n)}} \bigotimes_{j=1}^{2k-1} B_-^{\left(\alpha_{2k-1,j}^{(n)}\right)} \right\rangle \right] - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\left\langle \sum_{\boldsymbol{\alpha}_{2k}^{(n)} \in \mathcal{S}_{2k}^{(n)}} \bigotimes_{j=1}^{2k} B_-^{\left(\alpha_{2k,j}^{(n)}\right)} \right\rangle \right] \begin{cases} \leqslant 1 \\ \geqslant -\left(2^{n-1}-1\right) \end{cases}, \tag{7.1}$$

which recovers the well known Clauser-Horne-Shimony-Holt (CHSH) inequality for $n = 2$ and contains the Parity-CHSH inequality as a subclass. Based on our results in Ref. [HMKB19], App. C, we identified crucial properties that a Bell inequality needs to fulfill in order to be a viable option for multipartite DIQKD. As a result, we were able to tailor our Bell inequalities specifically to the task of multipartite DIQKD. With this new approach, we take first steps towards multipartite secret-key rates, depending on a Bell inequality violation, different from the CHSH inequality which, so far, is missing.

Our manuscript furthermore provides several characterizations of the Bell inequality. Among them:

(i) We analytically prove the classical upper and lower bounds for any $n \in \mathbb{N}$.

(ii) Via the Navascués-Pironio-Acín hierarchy, cf. Sec. 3.6.2, we established the Tsirelson bound of our Bell inequality (7.1) for $n \in \{3, 4\}$, which are tight within numerical precision. These bounds can be saturated with the GHZ

state. Further numerical evidence and the symmetry of our Bell inequality indicate, that the GHZ state can saturate the Tsirelson bound for all $n \in \mathbb{N}$.

(iii) Measurement observables are proposed for any number of parties which allow maximum Bell value with the n-GHZ state. Our results suggest, that the Tsirelson bound of our Bell inequality can be analytically calculated and it amounts to an optimization over a single parameter.

(iv) In addition, we discuss the existence of intermediate bounds. A violation of such bounds device-independently certifies, that at least a certain amount of parties are entangled with Alice. In particular, for $n = 3$ we establish that $\sqrt{2}$ is a Svetlichny bound, i.e., a Bell value larger than $\sqrt{2}$ certifies genuine tripartite entanglement.

Finally, we prove the usefulness of our Bell inequality for multipartite DIQKD. We consider an honest implementation and calculate via the NPA hierarchy achievable conference key rates, which we compare to multiple bipartite DIQKD protocols. In the low noise regime and in bottleneck networks, higher DI secret-key rates can be achieved with the multipartite protocol.

Chapter 8

Conclusion and Outlook

Two main topics constitute the core of this dissertation. On one hand, multipartite device-independent (DI) quantum key distribution (QKD) and the importance of Bell inequalities therein. On the other hand, quantum repeaters which, hitherto, are the most promising candidates for a quantum device that implements long-distance QKD, as well as for overcoming fundamental limitations on point-to-point quantum communication.

For multipartite DIQKD, we studied in our article [HMKB19] a published protocol, which we proved to be incomplete. That is, there cannot exist an honest implementation that does not lead to the protocol aborting. We precisely described that the fundamental problem of the protocol lies within the structure of the Mermin-Ardehali-Belinskiĭ-Klyshko (MABK) inequality, which prevents to achieve perfectly correlated measurement results and sufficiently large MABK inequality violation at the same time. These results lay the foundation for the subsequent work [HKB19], in which we identified the structural properties a Bell test requires, in order to be a viable option for DI conference key agreement (CKA). This, in turn, allowed us to tailor a Bell inequality specifically to this task. As a result, we discovered a family of genuine multipartite Bell inequalities which was motivated by the structure of the Greenberger-Horne-Zeilinger (GHZ) qubit state. This class of inequalities exhibits intriguing properties which we analytically characterized. Moreover, we demonstrated the usefulness of these Bell inequalities for DICKA by quantifying DI conference key rates. To this end, semidefinite programming techniques are employed, combined with multipartite constraints.

Although several aspects of our Bell inequality were described in [HKB19], a more in-depth analysis of its properties is desirable. A starting point is to clarify the role of partially entangled states and the existence of associated intermediate bounds. As we conjectured in the article, our Bell inequality serves as a DI witness for entanglement among a certain number of parties (one of them being Alice). Such DI entanglement witnesses are useful to avoid a false-positive entanglement detection, as described in Ref. [BBS$^+$13]. Beyond that, an important goal is to analytically relate the violation of our Bell inequality to a bound on Eve's accessible information. So far, every established analytical bound [PAB$^+$09, RMW19] relies on the Clauser-Horne-

Shimony-Holt (CHSH) Bell setting. Here, several techniques, specific to the structure of the CHSH inequality, are instrumental for the derivation. Thus, we believe that Bell inequalities tailored to DICKA are a fruitful approach to achieve secret-key rates based on a violation different from the CHSH inequality.

Besides conceptualizing theoretical tools for DIQKD, we also investigated the possibilities of implementing large-scale (bipartite) DIQKD via quantum repeaters in our publication [HKB18]. We provided a systematic analysis on how experimental quantities affect achievable DI secret-key rates and identified parameters with particularly detrimental impact. Our findings highlight the proneness of the desired DI security to imperfections of virtually all quantum devices. This, in particular, calls for a different optimal architecture of the quantum repeater for the purposes of DIQKD and further limits the distance one can overcome in comparison to the device-dependent (DD) version.

Our systematic analysis is not exhaustive. It remains for future research to include further quantum repeater models and error sources in the analysis to identify the quantum repeater implementation most-suitable for DIQKD. An advance in this regard is the measurement DI middle-note in twin-field QKD proposed in [LYDS18].

In the DD setting, we devised a general method to describe the error propagation of generalized Pauli errors in a error-corrected qudit quantum repeater [MHKB18]. In doing so, we can compute the full error statistics of the distributed qudit states. This paved the way for a follow-up work [MHKB19], in which we investigated the potential of error-corrected quantum repeaters to surpass the fundamental repeaterless bound dictated by [PLOB17]. Our results show that higher dimensional quantum states can provide an advantage for this task.

In Refs. [MHKB18, MHKB19], we focused on a specific class of quantum error-correcting codes (QECCs). Future research could, inter alia, investigate potential improvement by employing different QECCs.

Our research is part of a global trend towards the so-called second quantum revolution [MDM03], which promises concrete quantum technology applications. We hope that our scientific contributions provide additional insight and stimulate further research in the field of (device-independent) quantum communication in a large-scale quantum network.

Bibliography

[ABB+13] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß. Quantum repeaters and quantum key distribution: Analysis of secret-key rates. *Phys. Rev. A*, 87:052315, 2013.

[ABG+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98(23):230501, 2007.

[ACLY00] R. Ahlswede, N. Cai, S.-R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. Inf. Theor.*, 46(4):1204–1216, 2000.

[AFDF+18] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.*, 9(1):459, 2018.

[AFRV19] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *SIAM J. Comp.*, 48(1):181–225, 2019.

[AGR82] A. Aspect, P. Grangier, and G. Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, 1982.

[AMPS16] N. Aharon, S. Massar, S. Pironio, and J. Silman. Device-independent bit commitment based on the chsh inequality. *New J. Phys.*, 18(2):025014, 2016.

[Ard92] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Phys. Rev. A*, 46(9):5375, 1992.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, New York, 1984.

[BBB+12] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang. A framework for the study of symmetric full-correlation bell-like inequalities. *J. Phys. A: Math. Theor.*, 45(12):125301, 2012.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[BBM92] C. H. Bennett, G. Brassard, and D. N. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[BBR+18] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, 2018.

[BBS+13] J. T. Barreiro, J.-D. Bancal, P. Schindler, D. Nigg, M. Hennrich, T. Monz, N. Gisin, and R. Blatt. Demonstration of genuine multipartite entanglement with device-independent witnesses. *Nat. Phys.*, 9(9):559, 2013.

[BC90] S. L. Braunstein and C. M. Caves. Wringing out better bell inequalities. *Ann. Phys.*, 202:22–56, 1990.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, 2014.

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, 1998.

[BDS97] Charles H. Bennett, David P. DiVincenzo, and John A. Smolin. Capacities of quantum erasure channels. *Phys. Rev. Lett.*, 78:3217–3220, 1997.

[Bel64a] J. S. Bell. *Physics (Long Island City N.Y.)*, 1:195, 1964.

[Bel64b] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[Ben92] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, 1992.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95(1):010503, 2005.

[BK93] A. V. Belinskiĭ and D. N. Klyshko. Interference of light and bell's theorem. *Phys. Usp.*, 36(8):653–693, 1993.

[BKP06] J. Barrett, A. Kent, and S. Pironio. Maximally nonlocal and monogamous quantum correlations. *Phys. Rev. Lett.*, 97:170409, 2006.

[BLMS00] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, 2000.

[BPvL11] N. K. Bernardes, L. Praxmeyer, and P. van Loock. Rate analysis for a hybrid quantum repeater. *Phys. Rev. A*, 83:012323, 2011.

[Bru98] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021, 1998.

[CAL19] M. Curty, K. Azuma, and H.-K. Lo. Simple security proof of twin-field type quantum key distribution protocol. *Npj Quantum Inf.*, 5(1):64, 2019.

[CGL99] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648–651, 1999.

[CGL+02] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, 2002.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880, 1969.

[CKW00] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, 2000.

[CMA+13] B. Christensen, K. McCusker, J. Altepeter, B. Calkins, T. Gerrits, A. Lita, A. Miller, L. Shalm, Y. Zhang, S. Nam, et al. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111:130406, 2013.

[CTDL77] C. Cohen-Tannoudji, B. Diu, and F. Laloë. Quantum mechanics. volume 1 and. *Willey-VHC, Berlin*, 1977.

[DFR16] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *arXiv:1607.01796*, 2016.

[Dir39] P. A. M. Dirac. A new notation for quantum mechanics. In *Math. Proc. Camb. Philos. Soc.*, volume 35, pages 416–418. Cambridge University Press, 1939.

[DJR05] T. Decker, D. Janzing, and M. Rötteler. Implementation of group-covariant positive operator valued measures by orthogonal measurements. *J. Math. Phys.*, 46(1):012104, 2005.

[DLCZ01] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413, 2001.

[DW05] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. In *Proc. R. Soc. A*, volume 461, pages 207–235. The Royal Society, 2005.

[EKB13] M. Epping, H. Kampermann, and D. Bruß. Designing bell inequalities from a tsirelson bound. *Phys. Rev. Lett.*, 111:240404, 2013.

[EKB16] M. Epping, H. Kampermann, and D. Bruß. On the error analysis of quantum repeaters with encoding. *Appl. Phys. B*, 122(3):54, 2016.

[Eke91] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[EKMB17] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß. Multi-partite entanglement can speed up quantum key distribution in networks. *New J. Phys.*, 19(9):093012, 2017.

[EMSF+14] C. Erven, E. Meyer-Scott, K. Fisher, J. Lavoie, B. L. Higgins, Z. Yan, C. J. Pugh, J.-P. Bourgoin, R. Prevedel, L. K. Shalm, et al. Experimental three-photon quantum nonlocality under strict locality conditions. *Nat. Photonics*, 8(4):292, 2014.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777, 1935.

[FC72] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, 1972.

[Fis75] G. Fischer. *Lineare Algebra*. Vieweg, 1975.

[FSA+13] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Local orthogonality as a multipartite principle for quantum correlations. *Nature commun.*, 4:2263, 2013.

[FWH+10] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg. Surface code quantum communication. *Phys. Rev. Lett.*, 104:180503, 2010.

[GC19] F. Grasselli and M. Curty. Practical decoy-state method for twin-field quantum key distribution. *New J. Phys.*, 21(7):073001, 2019.

[GG99] N. Gisin and B. Gisin. A local hidden variable model of quantum correlation exploiting the detection loophole. *Phys. Lett. A*, 260(5):323 – 327, 1999.

[GHZ89] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond bell's theorem. In *Bell's theorem, quantum theory and conceptions of the universe*, pages 69–72. Springer, 1989.

[Got98] D. Gottesman. The heisenberg representation of quantum computers. *arxiv:9807006*, 1998.

[Got99] D. Gottesmann. Fault-tolerant quantum computation with higher-dimensional systems. *Chaos Soliton Fract*, 10:1749 – 1758, 999.

[GPS10] N. Gisin, S. Pironio, and N. Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, 2010.

[GVW+15] M. Giustina, M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, et al. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, 2015.

[HBD+15] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682, 2015.

[HHH96] R. Horodecki, M. Horodecki, and P. Horodecki. Teleportation, bell's inequalities and inseparability. *Phys. Lett. A*, 222(1):21 – 25, 1996.

[HKB18] T. Holz, H. Kampermann, and D. Bruß. Device-independent secret-key-rate analysis for quantum repeaters. *Phys. Rev. A*, 97:012337, 2018.

[HKB19] T. Holz, H. Kampermann, and D. Bruß. A genuine multipartite bell inequality for device-independent conference key agreement. *arXiv:1910.11360*, 2019.

[HMKB19] T. Holz, D. Miller, H. Kampermann, and D. Bruß. Comment on "fully device-independent conference key agreement". *Phys. Rev. A*, 100:026301, 2019.

[Hol73] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Inf.*, 9(3):3–11, 1973.

[Iva87] I.D. Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123(6):257 – 259, 1987.

[JTN+09] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin. Quantum repeater with encoding. *Phys. Rev. A*, 79:032325, 2009.

[KAF+10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, et al. Factorization of a 768-bit rsa modulus. In *Annual Cryptology Conference*, pages 333–350. Springer, 2010.

[KGR05] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501, 2005.

[KL10] P. Kok and B. W. Lovett. *Introduction to optical quantum information processing*. Cambridge University Press, 2010.

[KLM07] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[KRS09] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information theory*, 55(9):4337–4347, 2009.

[LB13] D. A. Lidar and T. A. Brun. *Quantum error correction*. Cambridge University Press, 2013.

[LCA05] H.-K. Lo, H.F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.*, 18(2):133–165, 2005.

[Leg08] A. J. Leggett. Realism and the physical world. *Rep. Prog. Phys.*, 71(2):022001, 2008.

[LJKL16] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus. Overcoming lossy channel bounds using a single quantum repeater node. *Appl. Phys. B*, 122(4):96, 2016.

[LYDS18] 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(7705):400, 2018.

[MDM03] A. G. J. MacFarlane, J. P. Dowling, and G. J. Milburn. Quantum technology: the second quantum revolution. *Philos. Trans. Royal Soc. A*, 361(1809):1655–1674, 2003.

[Mer90] D. N. Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65(15):1838, 1990.

[MHKB18] D. Miller, T. Holz, H. Kampermann, and D. Bruß. Propagation of generalized pauli errors in qudit clifford circuits. *Phys. Rev. A*, 98:052316, 2018.

[MHKB19] D. Miller, T. Holz, H. Kampermann, and D. Bruß. Parameter regimes for surpassing the plob bound with error-corrected qudit repeaters. *arXiv:1906.05172*, 2019.

[Mil82] F. Miller. *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. CM Cornwell, 1882.

[MKL+14] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.*, 112:250501, 2014.

[MLK+16] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang. Optimal architectures for long distance quantum communication. *Sci. Rep.*, 6:20463, 2016.

[MPA11] L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.*, 2:238, 2011.

[MPR+19] 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(5):334, 2019.

[MRC+14] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett. Full security of quantum key distribution from no-signaling constraints. *IEEE Trans. Inf. Theor.*, 60(8):4973–4986, 2014.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 503–509. IEEE Computer Society, 1998.

[MZL+17] S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang. Overcoming erasure errors with multilevel systems. *New J. Phys.*, 19(1):013026, 2017.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[NPA07] M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, 2007.

[NPA08] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.*, 10(7):073013, 2008.

[PAB+09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.*, 11(4):045021, 2009.

[PAB+19] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al. Advances in quantum cryptography. *arXiv:1906.01645*, 2019.

[Pau27] W. Pauli. Zur quantenmechanik des magnetischen elektrons. *Z. Phys.*, 43:601–623, 1927.

[PBD+00] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger. Experimental test of quantum nonlocality in three-photon greenberger-horne-zeilinger entanglement. *Nature*, 403(6769):515, 2000.

[Pea70] P. M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, 1970.

[Per06] A. Peres. *Quantum theory: concepts and methods*, volume 57. Springer Science & Business Media, 2006.

[Pit89] I. Pitowsky. *Quantum Probability – Quantum Logic*. Lect. Notes Phys. Vol. 321. Springer-Verlag, Berlin Heidelberg, 1989.

[Pla00] M. K. E. L. Planck. Zur theorie des gesetzes der energieverteilung im normalspectrum. *Verhandl. Dtsc. Phys. Ges.*, 2:237, 1900.

[PLOB17] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.*, 8:15043, 2017.

[PPK+09] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nature*, 461(7267):1101, 2009.

[PR94] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24(3):379–385, 1994.

[Ren08] R. Renner. Security of quantum key distribution. *Int. J. Q. Inf.*, 6(01):1–127, 2008.

[RGK05] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, 2005.

[RK05] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, pages 407–425. Springer Berlin Heidelberg, 2005.

[RKM+01] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409(6822):791, 2001.

[RMW18] J. Ribeiro, G. Murta, and S. Wehner. Fully device-independent conference key agreement. *Phys. Rev. A*, 97:022307, 2018.

[RMW19] J. Ribeiro, G. Murta, and S. Wehner. Reply to "comment on 'fully device-independent conference key agreement' ". *Phys. Rev. A*, 100:026302, 2019.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.

[RYG+19] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss. Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission. *Phys. Rev. A*, 99:052330, 2019.

[SAT+17] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio. Bell inequalities tailored to maximally entangled states. *Phys. Rev. Lett.*, 119:040402, 2017.

[SBPC+09] 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.*, 81:1301–1350, 2009.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell Sys. Tech. J.*, 27(3):379–423, 1948.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28(4):656–715, 1949.

[SR08] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, 2008.

[SSdRG11] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33–80, 2011.

[Sve87] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a bell-type inequality. *Phys. Rev. D*, 35:3066–3069, 1987.

[SZ99] M. O. Scully and M. S. Zubairy. Quantum optics. *Am. J. Phys.*, 67(7):648–648, 1999.

[Ter04] B. M. Terhal. Is entanglement monogamous? *IBM J. Res. Dev.*, 48(1):71–78, 2004.

[TGW14] M. Takeoka, S. Guha, and M. M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature commun.*, 5:5235, 2014.

[TSG+19] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim. Computing secure key rates for quantum key distribution with untrusted devices. *arXiv:1908.11372*, 2019.

[Tsi80] B. S. Tsirelson. Quantum generalizations of bell's inequality. *Lett. Math. Phys.*, 4(2):93–100, 1980.

[TSSR11] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.

[TT08] T. Tsurumaru and K. Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78:032302, 2008.

[TYC+14] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, et al. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.*, 113:190501, 2014.

[VB96] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Rev.*, 38(1):49–95, 1996.

[Ver26] G. S. Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, 45(2):109–115, 1926.

[vLLS+06] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto. Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.*, 96:240501, 2006.

[VV14] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113(14):140501, 2014.

[Weh06] S. Wehner. Tsirelson bounds for generalized clauser-horne-shimony-holt inequalities. *Phys. Rev. A*, 73:022110, 2006.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[WKR+11] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New J. Phys.*, 13(7):073024, 2011.

[WW00] R. F. Werner and M. M. Wolf. Bell's inequalities for states with positive partial transpose. *Phys. Rev. A*, 61:062102, 2000.

[WW01] R. F. Werner and M. M. Wolf. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64(3):032112, 2001.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802, 1982.

[YCY+16] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, 2016.

[ZXC+18] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan. Large scale quantum key distribution: challenges and solutions. *Opt. Express*, 26(18):24260–24273, Sep 2018.

[ZYC+03] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, M. Żukowski, and J.-W. Pan. Experimental violation of local realism by four-photon greenberger-horne-zeilinger entanglement. *Phys. Rev. Lett.*, 91:180401, 2003.

Appendix A

Device-independent secret-key-rate analysis for quantum repeaters

Title:	Device-independent secret-key-rate analysis for quantum repeaters
Authors:	Timo Holz, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review A
Impact factor:	2.909 (2017)
Date of submission:	24 November 2017
Publication status:	Published
Contribution by TH:	First author (input approx. 80%)

This publication corresponds to Ref. [HKB18]. A summary of the results is presented in Chap. 7. The general framework and research objective were worked out in collaboration with my co-authors and were regularly discussed with them. Together with HK, I identified a way to compare the device-dependent BB84 protocol to the device-independent spot-checking CHSH protocol, which was a crucial step for the systematic analysis presented in the article. I performed all analytical calculations myself, except the one presented in App. A.1 of the article, for which HK gave valuable input. All numerical computations (except the Monte Carlo simulations) were carried out by me. I created all plots and figures in the article. I wrote the entire manuscript which was proofread and improved by my co-authors.

Device-independent secret-key-rate analysis for quantum repeaters

Timo Holz,* Hermann Kampermann, and Dagmar Bruß
Theoretical Physics III, Heinrich Heine University Duesseldorf, D-40225 Duesseldorf, Germany

(Received 24 November 2017; published 31 January 2018)

The device-independent approach to quantum key distribution (QKD) aims to establish a secret key between two or more parties with untrusted devices, potentially under full control of a quantum adversary. The performance of a QKD protocol can be quantified by the secret key rate, which can be lower bounded via the violation of an appropriate Bell inequality in a setup with untrusted devices. We study secret key rates in the device-independent scenario for different quantum repeater setups and compare them to their device-dependent analogon. The quantum repeater setups under consideration are the original protocol by Briegel *et al.* [Phys. Rev. Lett. **81**, 5932 (1998)] and the hybrid quantum repeater protocol by van Loock *et al.* [Phys. Rev. Lett. **96**, 240501 (2006)]. For a given repeater scheme and a given QKD protocol, the secret key rate depends on a variety of parameters, such as the gate quality or the detector efficiency. We systematically analyze the impact of these parameters and suggest optimized strategies.

DOI: 10.1103/PhysRevA.97.012337

I. INTRODUCTION

Quantum cryptography—the science of (secure) private communication based on fundamental properties of quantum particles—is a very active field of research and was founded in the early 1980s [1]. An unconditionally secure encryption technique, the one-time pad [2], relies on a preshared key between the parties who wish to communicate. Secure communication can thus be achieved by securely distributing this key, which is the ultimate task of quantum key distribution (QKD). The famous BB84 protocol [3] was the first proposal for achieving secure QKD. Since then, a variety of other QKD protocols have been published [4–6]. However, the security of these *device-dependent* (DD) protocols relies on a perfect characterization of the measurement devices and the source, which is impossible in practice. Any realistic implementation is imperfect, which makes these QKD protocols vulnerable to an adversary [7–10]. Ideally, one wants to drop any assumption about any device involved in the QKD scheme, which is referred to as *device-independent* (DI) QKD [11,12].

As photons possess a long coherence time, one can transmit these particles through fibers or free space, thus allowing long-distance QKD. Due to photon losses, though, which exponentially scale with the distance one wants to overcome, QKD is limited to distances of $L \lesssim 150$ km [13,14]. This problem can be circumvented with quantum repeaters [15].

In this work, we aim at comparing achievable secret key rates in the DD and DI scenario for different quantum repeaters without implemented error correction. In particular, we provide a systematic analysis on how experimental quantities and errors manifest themselves in the corresponding secret key rates. The DD case has been analyzed in [16]. Here, we shed light on the fundamental differences between both scenarios, especially the requirements needed for a reasonably high DI secret key rate.

The structure of this paper is as follows. In Sec. II we review a generic quantum repeater model [15], recapitulate the fundamentals of QKD, and explain the peculiarities in the device-independent case. Important ingredients, such as the secret key rate R and the errors we account for, are described. In Sec. III we apply the given framework to the original quantum repeater proposal by Briegel *et al.* [15]. Section IV focuses on the key analysis for the hybrid quantum repeater [17].

II. GENERAL FRAMEWORK

The main source of errors in quantum communication with photons are losses in the optical fiber, which scale exponentially with the length L_0, such that the transmittivity η_t is given by

$$\eta_t(L_0) = 10^{-\alpha \frac{L_0}{10}}, \tag{1}$$

where α denotes the attenuation coefficient. In this work we use $\alpha = 0.17$ dB/km, which is the attenuation coefficient at wavelengths around 1550 nm. To overcome the exponential photon loss, quantum repeaters for long-distance quantum information transmission have been suggested.

In this section we review a generic model for a quantum repeater, originally introduced by Briegel *et al.* [15]. Furthermore, we briefly discuss other sources of errors in QKD and how we model and incorporate them in the quantum repeater scheme. See [16] for a detailed discussion of imperfections. We also review the main ideas of DIQKD, in particular the DI protocol that we use [11].

A. Generic quantum repeater model

The purpose of a quantum repeater is to generate and distribute entangled states over a large distance L that separates two parties, typically called Alice and Bob. In order to increase

*holzt@uni-duesseldorf.de

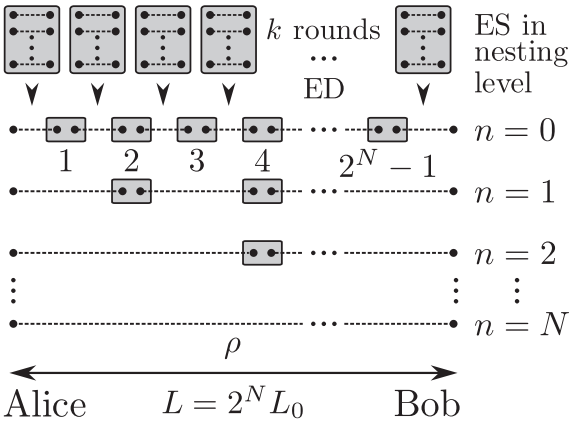

FIG. 1. A generic quantum repeater setup proposed by [15]. Let k denote the number of distillation rounds performed prior to the first ES and N the maximum nesting level. Alice and Bob are separated by the distance $L = 2^N L_0$ and share at the end of the nested protocol the entangled state ρ.

the distance over which the states are entangled, one performs entanglement swapping (ES) at intermediate repeater stations equally separated by a fundamental length L_0. In the nested quantum repeater proposal (see Fig. 1 for a schematic representation), ES is performed in N consecutive nesting levels, where 2^N segments of fundamental length L_0 amount to the total distance $L = 2^N L_0$, which corresponds to $2^N - 1$ intermediate repeater stations. For the sake of simplicity, we only allow state purification via entanglement distillation (ED) before the first ES is done. The repeater stations are equipped with quantum memories and processors to perform the mentioned quantum operations. For ED, we employ the Deutsch *et al.* [18] protocol, which generates after k rounds of distillation a final state of high purity out of 2^k copies of an initial state ρ_0. The ES protocol involves Bell measurements, which can be implemented in various ways in the experiment [19,20]. We review the ED and ES protocol in Appendix B.

As entanglement can be used as a resource for many quantum informational tasks [21,22], it is important to quantify the number of entangled states that can be distributed between Alice and Bob per second by a quantum repeater. This quantity is described by the repeater rate R_{rep}, which clearly depends on errors that occur in the quantum repeater. We briefly discuss which errors are taken into account and how we model them. Afterwards we discuss the time restrictions that we focus on and explicitly give the expression for the repeater rate.

1. Errors of the quantum repeater

The elements of a quantum repeater and their errors are as follows: (i) Quantum channel – Photon losses in the fiber are described via the transmittivity η_t, Eq. (1). (ii) Source – We assume that the source creates on demand a state ρ_0 and distributes it to adjacent repeater stations. The quality of these states is described via the fidelity F_0 with respect to a certain Bell state, defined in Eqs. (14a) and (14b). (iii) Detectors – We assume photon number resolving detectors (PNRDs) with efficiency η_d, where dark counts of the detectors are neglected. This is a reasonable approximation for realistic dark counts of the order of 10^{-5} or below, see [16]. (iv) Gates – ED and ES rely on controlled two-qubit operations, implemented by a gate with quality p_G. This imperfect gate introduces noise, thus mixing the ideal pure entangled state. We further assume that one-qubit gates work perfectly.

The errors in (i)–(iv) give rise to a success probability for ED in round k and for ES in nesting level n. We denote those probabilities with $P_{\text{ED}}^{(k)}$ and $P_{\text{ES}}^{(n)}$, respectively. Finally, let P_0 denote the probability that a source successfully links two adjacent repeater stations in the 0th nesting level with an initial entangled state ρ_0.

2. Repeater rate

For a given set of parameters and within a model that respects the errors we introduced in the previous section, one can achieve a certain repeater rate R_{rep}. In order to characterize this repeater rate, we need to clarify which time restrictions we account for. The only time-consuming operation that we consider is the time needed to distribute an entangled photon pair among adjacent repeater stations and acknowledge their successful transmission. This so-called fundamental time T_0 depends on the speed of light $c = 2 \times 10^8$ m/s in the fiber, the fundamental length L_0 separating two repeater stations, and the location of the photon source. We consider the case where the source is located at one repeater station, which yields the fundamental time $T_0 = 2L_0/c$ [16]. Furthermore, we investigate repeaters with deterministic and probabilistic ES, i.e., $P_{\text{ES}}^{(n)} = 1$ and $P_{\text{ES}}^{(n)} < 1$, respectively.

a. Deterministic ES. For perfect detectors $\eta_d = 1$, the ES can be performed in a deterministic manner. The corresponding repeater rate is given by [23]

$$R_{\text{rep}}^{\text{det}} = \frac{1}{T_0} \frac{1}{Z_n\left(P_{L_0}^{(k)}\right)}, \tag{2}$$

where the recursive probability $P_{L_0}^{(k)}$ in distillation round k is defined via

$$P_{L_0}^{(k)} := \frac{P_{\text{ED}}^{(k)}}{Z_1\left(P_{L_0}^{(k-1)}\right)} \quad \forall\, k \geqslant 1 \tag{3}$$

and $P_{L_0}^{(0)} := P_0$. Here, $Z_n(p)$ denotes the average number of attempts to successfully establish 2^n entangled pairs (each generated with probability p) and it is given by [23]

$$Z_n(p) := \sum_{j=1}^{2^n} \binom{2^n}{j} \frac{(-1)^{j+1}}{1-(1-p)^j}. \tag{4}$$

The 2^n generated pairs are then deterministically converted via ES in the repeater stations to an entangled pair between Alice and Bob.

b. Probabilistic ES. ES is a probabilistic procedure for imperfect detectors. Given $P_0 \ll 1$, the repeater rate of a quantum repeater with k rounds of ED and ES in n nesting levels can be approximated by

$$R_{\text{rep}}^{\text{prob}} = \frac{1}{T_0}\left(\frac{2}{3}\right)^{n+k} P_0 \prod_{j=1}^{k} \frac{P_{\text{ED}}^{(j)}}{a_{\text{ED}}^{(j-1)}} \prod_{i=1}^{n} \frac{P_{\text{ES}}^{(i)}}{a_{\text{ES}}^{(i-1)}}, \tag{5}$$

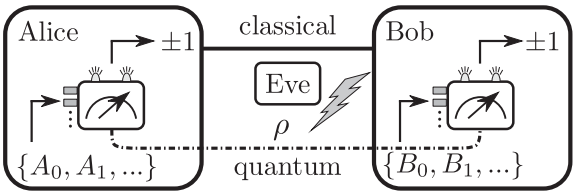

FIG. 2. A typical QKD setup. Alice and Bob share a classical and a quantum channel. A source provides possibly entangled states ρ that can be measured by the perfectly characterized measurement devices. A dichotomic classical output is generated in each measurement round.

which is a generalized and slightly modified version of the repeater rates given in [16,24].[1] Here, $a_{\mathrm{ED}}^{(j)}$ and $a_{\mathrm{ES}}^{(i)}$ denote constants that one has to choose depending on success probabilities to create an entangled state in the corresponding ED round and nesting level, respectively. They fulfill $0 < a_{\mathrm{ED}}^{(j)}, a_{\mathrm{ES}}^{(i)} \leqslant 1$ and are typically close to 1. The repeater rate in Eq. (5) underestimates the actual repeater rate, as already pointed out in [23]. Recently, a more sophisticated approach to quantify the repeater rate with probabilistic ES appeared in the literature [25].[2] To our knowledge, an analytical study of the optimal strategy has not been performed yet.[3]

B. Quantum key distribution

With the repeater rates in Eqs. (2) and (5), we now study the possibility to use the entangled states as a resource to generate a secret key.

1. Device-dependent QKD

Suppose that Alice and Bob share a classical, authenticated channel and a possibly entangled state ρ, transmitted through a quantum channel. A typical QKD setup is shown in Fig. 2. In each measurement round, Alice and Bob can choose from a set of measurement settings $\{A_0, A_1, \dots\}$ and $\{B_0, B_1, \dots\}$. The setting determines which measurement is performed on their subsystem. Throughout this work we consider dichotomic measurement outcomes $a_i, b_j \in \{\pm 1\}$.

The performance of a QKD protocol is quantified by the secret key rate [16]

$$R := R_{\mathrm{raw}} r_\infty = R_{\mathrm{rep}} R_{\mathrm{sift}} P_{\mathrm{click}} r_\infty, \tag{6}$$

which is our figure of merit. The quantities introduced in Eq. (6) are the raw key rate R_{raw}, the fraction R_{sift} of measurements performed in the same basis by Alice and Bob, the probability P_{click} for a valid measurement result, and the secret fraction r_∞ (see below).

After generating an arbitrarily long bit string, the classical postprocessing of the measurement data begins, including sifting, which corresponds to discarding measurements where the settings of Alice and Bob did not match. Note that we fix $R_{\mathrm{sift}} = 1$, which can be approximately achieved by choosing the measurement settings with biased probabilities [26]. The sifted or raw key leads to the raw key rate R_{raw}, which is the number of raw bits Alice and Bob generate per second. These bits are only partially secure, which is described by the secret fraction r_∞. The explicit form of r_∞ depends on the protocol one employs. A variety of QKD protocols exist in the literature, such as the BB84 and the six-state protocol [3,6]. In these QKD protocols one has full knowledge about the Hilbert space dimensions, which is crucial for the security of these protocols. For instance, the security of the BB84 protocol critically depends on the four dimensions of the Hilbert space associated to a qubit pair [27]. The secret fraction for the BB84 protocol is given by [13]

$$r_\infty^{\mathrm{BB84}} = \max\{0, 1 - h(Q_z) - h(Q_x)\}. \tag{7}$$

In Eq. (7) the binary entropy is denoted as $h(p) := -p \log_2(p) - (1-p)\log_2(1-p)$ and the quantum bit error rate (QBER) in measurement direction i is Q_i. The QBER is defined as the probability that Alice and Bob generate discordant outcomes, given a fixed set of measurement settings, i.e.,

$$Q_z = P(a \neq b \mid A = Z, B = Z), \tag{8a}$$

$$Q_x = P(a \neq b \mid A = X, B = X), \tag{8b}$$

for measuring Pauli Z and X operators.

2. Device-independent QKD

In practice, it is impossible to have full control over the devices involved in a QKD setup. The idea of DIQKD is to extract a secret key without making detailed assumptions about the involved devices [11]. The security of such DIQKD protocols is based on a loophole-free Bell-inequality violation [28], for which we have to assume that the two parties are causally separated. In the spirit of device independence, the measurement devices are treated as black boxes that perform some (unknown) measurement conditioned on a classical input chosen by Alice and/or Bob. The measurement should again yield a dichotomic classical output. However, in practice sometimes detectors fail and produce no outcome. Measurements where any of the black boxes do not produce an output have to

[1] In [24], the repeater rate for probabilistic ES is derived without initial ED and without the constants $a_{\mathrm{ES}}^{(i)}$. In [16] initial ED is included and a common constant a_{ED} is introduced for every ED round, which results in a larger repeater rate. In general, it is not justified to use a common constant a_{ED}, as they quickly approach unity for an increasing number of ED steps. As we show in Appendix A, one can tackle this problem in a more efficient way and one can similarly introduce constants for the ES procedure.

[2] Note, however, that for more than $n = 2$ nesting levels, the repeater rate of [25] rapidly becomes only numerically feasible and provides no further insight into our analysis. Also, since we want to keep n in principle arbitrary, we settle for the approximated repeater rate in Eq. (5).

[3] In practice, the optimal strategy for maximizing the repeater rate is to immediately perform ES as soon as entangled pairs are available in two neighboring repeater links and then proceed by already distributing new states among these available repeater stations. Monte Carlo simulations suggest that this approach can significantly exceed the analytical repeater rates in Eqs. (2) and (5), depending on n.

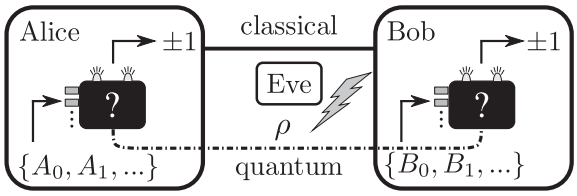

FIG. 3. The DIQKD setup. The measurement devices are treated as black boxes, i.e., the exact internal operations are unknown. Additionally, the dimension of the Hilbert space associated to the state ρ is not specified.

be incorporated into the measurement data. Alice and Bob can achieve this by randomly assigning a measurement result $\{\pm 1\}$ to such events [29]. In this sense, every event is a valid DIQKD measurement, yielding $P_{\text{click}} = 1$. Note that these events can be incorporated in our description by substituting the final state that Alice and Bob share in the following way:

$$\rho \quad \rightarrow \quad \eta_d^2 \rho + \frac{1-\eta_d^2}{4}\mathbb{1}, \tag{9}$$

where η_d refers to the probability that a no-detection event was replaced by a random outcome. Note that η_d enters the expression in (9) quadratically, because two detectors of the same efficiency are involved in each measurement. Figure 3 shows the DIQKD setup. The DI secret key rate can be calculated via

$$R^{\text{DI}} = R_{\text{raw}} r_\infty^{\text{DI}} = R_{\text{rep}} r_\infty^{\text{DI}}, \tag{10}$$

where we used $P_{\text{click}} = 1$ and $R_{\text{sift}} = 1$ (see above). In the DD case, the probability P_{click} is a function of the detector efficiency η_d, whereas in the DI scenario η_d enters the secret fraction r_∞^{DI} due to the modification of the quantum state in (9).

Comparing Eqs. (6) and (10) reveals that both key rates share the common repeater rate R_{rep}, which is consistent with the fact that the purpose of the quantum repeater is simply to provide entangled states to the two parties. Alice and Bob can then choose to trust their devices or not. Several DIQKD protocols have been proposed in the literature [11,30,31]. We employ the protocol in [11].

3. DIQKD protocol

In the DIQKD protocol of [11] Alice randomly (with biased probabilities) chooses between three measurement settings $\{A_0, A_1, A_2\}$. The exact internal measurement process is unknown, but the device generates a dichotomic classical output $a \in \{\pm 1\}$ (no-detection events get an assignment of ± 1, uniformly at random). Similarly, Bob chooses between two measurement settings $\{B_0, B_1\}$, producing a binary output $b \in \{\pm 1\}$ in each round. A random small subset of their (classical) measurement data generated with the setting $\{A_2, B_1\}$ is used to estimate $Q := P(a \neq b \mid A_2, B_1)$ and the outcomes of the settings $\{A_{0/1}, B_{0/1}\}$ are used to calculate

$$S := \text{Tr}\left[\rho \sum_{i,j\in\{0,1\}} (-1)^{i\cdot j} A_i \otimes B_j\right]. \tag{11}$$

The main result of [11] is a lower bound for the DI secret fraction of the remaining measurement data of the setting $\{A_2, B_1\}$, given by

$$r_\infty^{\text{DI}} = \max\left\{0, 1 - h(Q) - h\left(\frac{1+\sqrt{S^2/4-1}}{2}\right)\right\}, \tag{12}$$

under the condition that $S > 2$ and that the marginal probabilities of Alice and Bob are symmetric, i.e., $\text{Tr}[\rho A_i \otimes \mathbb{1}] = 0 = \text{Tr}[\rho \mathbb{1} \otimes B_j]$ for all i, j. This lower bound was proven for collective attacks and one-way classical postprocessing in [11]. See also [32] for more general quantum adversaries and general communication between the parties. In the following section we adopt the specific implementation given in [11], where Q and S are the QBER and the Clauser-Horne-Shimony-Holt (CHSH) parameter [33], respectively.

4. Comparing DDQKD and DIQKD protocols

To point out the distinct features separating both scenarios and how they impact the secret key rates, we have to make the DD and the DI protocol effectively comparable. The specific implementation given in [11] for the DI protocol uses

$$A_{0,1} = \frac{X \pm Z}{\sqrt{2}}, \quad A_2 = Z, \tag{13a}$$

$$B_0 = X, \qquad B_1 = Z, \tag{13b}$$

for the measurement operators. To compare this to the BB84 protocol, where Alice uses $\{A_x = X, A_z = Z\}$ and Bob $\{B_0, B_1\}$ as in Eq. (13b), we also consider the asymmetric implementation of the DI protocol, such that $\{A_2 = Z, B_1 = Z\}$ is measured with probability $\rightarrow 1$ and with a negligible but equal fraction with which the other measurement operators are used. In the DI and DD case they use these measurement settings to estimate the CHSH value, Eq. (11), and the QBER Q_x, respectively. Then, in the asymptotic limit, these protocols are equivalent in the sense that almost always the Z measurement is used. Alice and Bob only rely on different assumptions regarding the trust in their measurement devices.

5. Entangled state, QBER, and CHSH parameter

The explicit form of the state that is distributed to Alice and Bob by the quantum repeater is of fundamental importance for achievable secret key rates. Maximal correlation, and thus maximal security is provided if the state ρ is pure and in one of the four Bell states:

$$|\phi_{1,2}\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{14a}$$

$$|\phi_{3,4}\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{14b}$$

For the specific implementation in Eqs. (13), the ideal state is the pure state $|\phi_1\rangle$ for which the CHSH parameter reaches its maximum value $2\sqrt{2}$ [34] and the QBERs vanish. Then, the DD and DI secret fraction are both equal to 1, which maximizes the corresponding secret key rates. In practice, the source cannot provide perfectly pure states due to noise and other imperfections. Under the assumption that the initially distributed states ρ_0 are genuine two-qubit states, they can be

transformed into a generic Bell-diagonal state

$$\rho_0 = \sum_{i=1}^{4} c_{i,0}^{(0)} |\phi_i\rangle\langle\phi_i| \tag{15}$$

by using local operations [35].[4] The Bell coefficients $c_{i,0}^{(0)}$ are non-negative and fulfill normalization $\sum_i c_{i,0}^{(0)} = 1$. We assume throughout this work that the sources generate the generic Bell-diagonal state given in Eq. (15). The ED and ES protocols we use produce Bell-diagonal states, provided the input states have been of the form (15). The quantum repeater thus distributes the final state,

$$\rho = \sum_{i=1}^{4} c_{i,n}^{(k)} |\phi_i\rangle\langle\phi_i|, \tag{16}$$

to Alice and Bob, where $c_{i,n}^{(k)}$ denotes the Bell coefficients after ED in k rounds and ES in n nesting levels. The coefficients $c_{i,n}^{(k)}$ fulfill normalization, and they depend on $c_{i,0}^{(0)}$ and on the explicit form of the protocol. See [16,18] or Appendix B for details of the protocols. The transformation rules for the coefficients $c_{i,n}^{(k)}$ under ED and ES are summarized in Appendixes C and D for the two quantum repeater setups. For Bell-diagonal states, as in Eq. (16), the QBERs $Q_{x,n}^{(k)}$ and $Q_{z,n}^{(k)}$ are given by

$$Q_{x,n}^{(k)} = c_{2,n}^{(k)} + c_{4,n}^{(k)}, \tag{17a}$$

$$Q_{z,n}^{(k)} = c_{3,n}^{(k)} + c_{4,n}^{(k)}. \tag{17b}$$

To calculate the quantities needed for the DI secret fraction, one needs to substitute the state ρ, Eq. (16), with its noisy version (9). This results in

$$Q_{z,n}^{(k)} = \eta_d^2 \left(c_{3,n}^{(k)} + c_{4,n}^{(k)}\right) + \frac{1-\eta_d^2}{2}, \tag{18a}$$

$$S_n^{(k)} = 2\sqrt{2}\eta_d^2 \left(c_{1,n}^{(k)} - c_{4,n}^{(k)}\right), \tag{18b}$$

where $S_n^{(k)}$ denotes the violation of the CHSH inequality with the final state.

III. THE ORIGINAL QUANTUM REPEATER

Now we want to compare achievable secret key rates for the original quantum repeater (OQR) [15] in the DD and DI scenario. In Sec. III A we give the missing expressions needed to calculate the repeater rate R_{rep}. This is followed by a systematic secret-key-rate analysis, where we compare the DD and DI QKD performance numerically (Sec. III B) and analytically (Sec. III C). Since any two-qubit mixture can be transformed into depolarized Bell states with local operations [36], we assume that the sources initially distribute such states with Bell coefficients $c_{1,0}^{(0)} = F_0$ and $c_{i\geq 2,0}^{(0)} = (1-F_0)/3$, where F_0 denotes the fidelity with respect to the Bell state $|\phi_1\rangle$.

[4]Note that depolarizing reduces only nonlocal correlations.

A. Parameters and error model

In order to calculate the repeater rate R_{rep}, we need to specify the probabilities P_0, P_{click}, $P_{\text{ES}}^{(n)}$, and $P_{\text{ED}}^{(k)}$ and how the gate quality p_G enters the expression. The probability that the source successfully connects two adjacent repeater stations with an entangled photon pair is given by the transmittivity $P_0 = \eta_t(L_0)$, Eq. (1), and the probability for a valid QKD measurement is $P_{\text{click}} = \eta_d^2$. The ED and ES protocol employ controlled two-qubit gates, that may introduce noise due to imperfections. We adopt the depolarizing model of [15] for noisy gates,

$$\mathcal{O}(\chi) = p_G \mathcal{O}^{\text{ideal}}(\chi) + \frac{1-p_G}{4}\mathbb{1}, \tag{19}$$

where χ denotes an arbitrary two-qubit state on which the gate $\mathcal{O}$ acts. The ED and ES include twofold detections with PNRDs of efficiency η_d. For perfect detectors $\eta_d = 1$, the repeater rate is given by Eq. (2). In case of nonperfect detectors, however, the detection events lead to a factor $\eta_d^{2(k+n)}$ for the success probabilities $P_{\text{ED}}^{(k)}$ and $P_{\text{ES}}^{(n)}$. Starting from Eq. (5), we thus get

$$R_{\text{rep}}^{\text{prob}} = \frac{1}{T_0}\left(\frac{2}{3}\right)^{k+n} \eta_d^{2(k+n)} \eta_t(L_0) \prod_{i=1}^{n} \frac{1}{a_{\text{ES}}^{(i-1)}} \prod_{j=1}^{k} \frac{P_{\text{ED}}^{\prime(j)}}{a_{\text{ED}}^{(j-1)}} \tag{20}$$

for the repeater rate with probabilistic ES, where $P_{\text{ED}}^{\prime(j)}$ now denotes the success probability for ED in round j without the detector efficiency η_d, which can be calculated via the coefficients $c_{i,0}^{(j)}$ only [see Appendix C, Eq. (C2)].

B. Performance: DD vs DI secret key rate

With the framework provided in the previous sections, we now want to systematically analyze achievable secret key rates in the DD and DI scenario. We split the analysis into two parts, one with perfect detectors $\eta_d = 1$ and one with imperfect detectors $\eta_d < 1$, as this quantity determines which repeater rate has to be used for the calculation. Currently feasible PNRDs reach detector efficiencies of $\eta_d \approx 0.95$ at wavelengths around 1550 nm [37].

1. Perfect detectors

For this part we use the deterministic repeater rate in Eq. (2). Note that for $\eta_d = 1$, the differences in the secret key rates solely originate from the DD and DI secret fraction. We begin the performance analysis with perfect gate qualities $p_G = 1$ to understand how ED and ES influence the secret key rates. Suppose Alice and Bob are separated by the total distance $L = 600$ km. At the end of the repeater protocol, they receive a Bell-diagonal state with coefficients $c_{i,n}^{(k)}$. Figure 4 shows the secret key rates R and R^{DI} (upper subfigures), the corresponding secret fractions r_∞ and r_∞^{DI} (middle subfigures), and the fidelity $F(|\phi_1\rangle, \rho) := \langle\phi_1|\rho|\phi_1\rangle$ of the final state ρ and the pure Bell state $|\phi_1\rangle$ (lower subfigures) as a function of the initial fidelity F_0 for various numbers of initial ED rounds k and nesting levels n. The secret key rates are calculated via Eqs. (6) and (10). The secret fractions, Eqs. (7) and (12), are calculated via the QBERs and the CHSH parameter given in Eqs. (17) and (18).

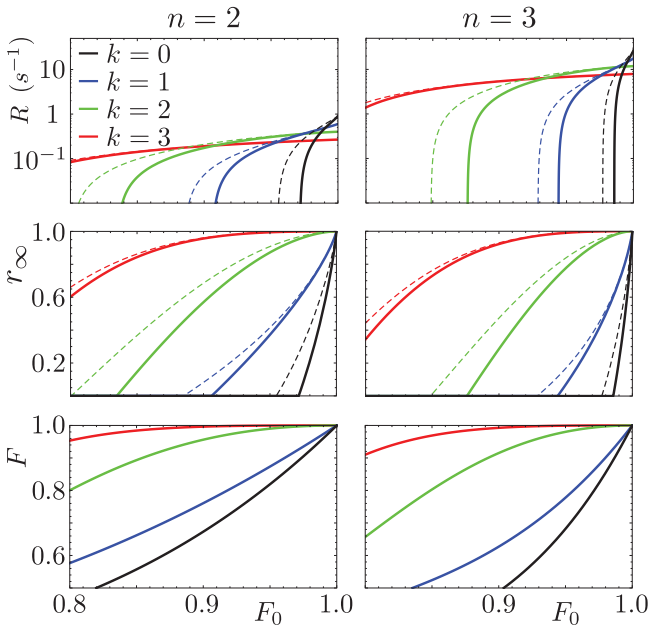

FIG. 4. Secret key rate R, secret fraction r_∞, and final fidelity $F = c_{1,n}^{(k)}$ with respect to $|\phi_1\rangle$ in the DD (dashed lines) and DI (solid lines) scenario versus the initial fidelity F_0 for the gate quality $p_G = 1$, perfect detector efficiency $\eta_d = 1$, and the total distance $L = 600$ km. Different numbers of initial ED rounds are shown, where $k = 0$ corresponds to the rightmost curve and $k = 3$ to the leftmost one. The left (right) column represents $n = 2$ ($n = 3$) nesting levels, which corresponds to a fundamental length $L_0 = 150$ km ($L_0 = 75$ km). Note that for $\eta_d = 1$, the curves for the final fidelity F for the DD and DI scenario coincide.

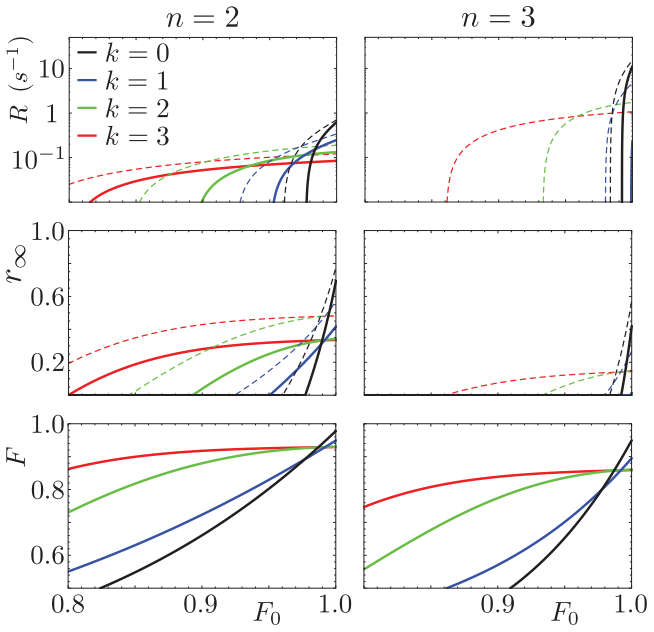

FIG. 5. Secret key rate R, secret fraction r_∞, and final fidelity $F = c_{1,n}^{(k)}$ with respect to $|\phi_1\rangle$ in the DD (dashed lines) and DI (solid lines) scenario versus the initial fidelity F_0 for $p_G = 0.99$, perfect detector efficiency $\eta_d = 1$, and the total distance $L = 600$ km. Different numbers of initial ED rounds are shown, where $k = 0$ corresponds to the rightmost curve and $k = 3$ to the leftmost one. The left (right) column represents $n = 2$ ($n = 3$) nesting levels. Note that for $\eta_d = 1$, the curves for the final fidelity F for the DD and DI scenario coincide.

The first feature that one notices is the fact that $R \geqslant R^{\mathrm{DI}}$ holds, which is what we expect since in the DD case, Alice and Bob can rely on more assumptions, which directly leads to a higher secret fraction. This should hold in any fair DD to DI comparison. The secret key rates are only identical in the ideal case where $\eta_d = 1$, $p_G = 1$, and $F_0 = 1$. Only under these perfect conditions do Alice and Bob share the pure and maximally entangled state $|\phi_1\rangle\langle\phi_1|$, which yields a secret fraction of 1. Comparing the case of $n = 2$ nesting levels with $n = 3$, one observes that both secret key rates significantly increase with n. For perfect gates, it is advantageous to reduce the fundamental length L_0 to decrease photon losses. This holds although more intermediate repeater stations involve more noisy states connected by ES, which reduces the secret fractions r_∞ and r_∞^{DI} as shown in Fig. 4. For a larger number of ED rounds k, both QKD protocols become more resistant to noise in the initial state ρ_0 but they suffer from an overall smaller secret key rate, as several copies of states are consumed. From the lower subfigures, we observe that ED and ES are two counteracting processes, when it comes to the final fidelity F with respect to $|\phi_1\rangle$. This is consistent with the shown secret fractions, since a lower fidelity F results in an increase of the QBERs and in a decrease of the CHSH parameter [see Eqs. (17) and (18)].

We now consider imperfect gates. Figure 5 shows the same quantities as in Fig. 4 but for $p_G = 0.99$. The lower gate quality has a strong impact on the DI secret fraction r_∞^{DI} and thus also on the DI secret key rate, especially for more nesting levels n. The mixing of the final state due to noisy gates has a significantly larger influence on the CHSH parameter as it has on the QBER Q_x. If the source distributes states with a high initial fidelity F_0, it is not beneficial for the final fidelity F to perform any ED. (See crossing points of solid lines in Fig. 5.)

2. *Imperfect detectors*

For an imperfect detector efficiency $\eta_d < 1$, the repeater rate is calculated via Eq. (5). The DD secret key rate additionally suffers from the global scaling factor $P_{\mathrm{click}} = \eta_d^2$ [see Eq. (6)]. In the DI scenario, however, the lack of perfect detectors is equivalent to performing QKD with states having increased noise, see substitution (9). These differences aside, the DD and DI secret key rates can be calculated as before. Figure 6 compares the secret key rates as a function of the fidelity F_0 for various numbers of ED rounds k, different numbers of nesting levels n, and different gate qualities p_G for $\eta_d = 0.975$ and $L = 600$ km. By comparing the upper two subfigures, we again observe that the gate quality has a much stronger impact on the DI secret key rate. Reducing $p_G = 1$ to $p_G = 0.99$ results in significantly smaller DI secret key rates, while the DD secret key rates are more or less of the same order. The difference between the DD and DI secret key rate becomes higher by increasing the number of initial ED rounds, which indicates that the number of imperfect quantum operations is a critical quantity for DIQKD. This is also confirmed by the lower subfigure, where we increased the number of nesting

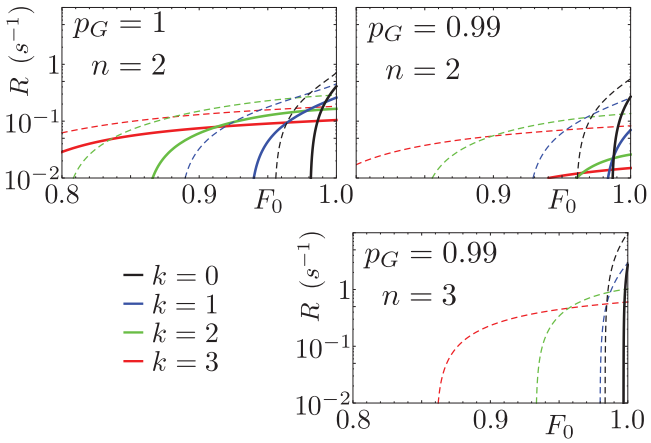

FIG. 6. DD (dashed lines) and DI (solid lines) secret key rate versus the fidelity F_0 with imperfect detectors of efficiency $\eta_d = 0.975$ and the total distance $L = 600$ km. We use different gate qualities p_G and different number of nesting levels n. The rightmost curve corresponds to $k = 0$ and the leftmost curve to $k = 3$ initial ED rounds.

levels from $n = 2$ to $n = 3$. One gets only a nonvanishing DI secret key rate for $k = 0$, whereas the DD secret key rates gain about 1 order of magnitude. Recall that performing ES in more nesting levels decreases the fundamental length L_0, thus reducing the probability of photon losses in the fiber. This explains the higher DD secret key rates for $n = 3$. However, in the DI case, the errors introduced by imperfections outweigh the benefits that one gains from a reduced fundamental length L_0. Hence, in the DI case one has to accept a larger amount of photon losses in the fiber of larger fundamental length L_0 in comparison to the DD case. In addition, one has to ensure that the source distributes entangled states of high initial fidelity F_0. This decreases the number of ED and ES steps and thus reduces

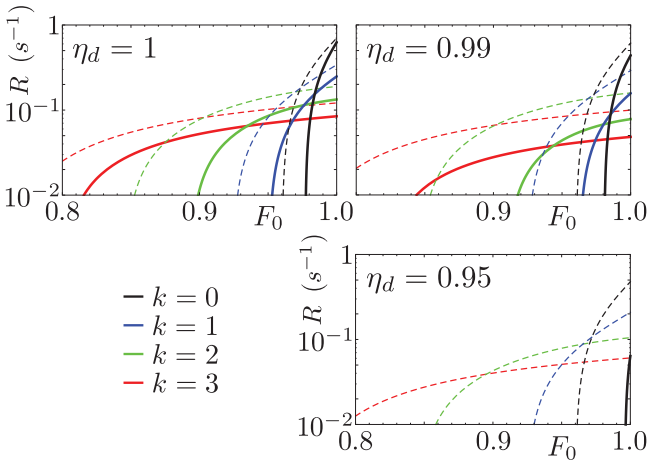

FIG. 7. DD (dashed lines) and DI (solid lines) secret key rate versus the fidelity F_0 for various different detector efficiencies η_d. The gate quality, the number of nesting levels, and the total length are set to $p_G = 0.99$, $n = 2$, and $L = 600$ km, respectively. The rightmost curve corresponds to $k = 0$ and the leftmost curve to $k = 3$ initial ED rounds.

the errors introduced by imperfect devices. We conclude that in general, the strategy for optimizing the DI secret key rate is different from the DD case. In Fig. 7 we vary the detector efficiency η_d and keep the gate quality p_G fixed. It compares DI (solid lines) and DD (dashed lines) secret key rates for various values of η_d and confirms the intuition that a reduction of the detector efficiency has a larger impact on the DI secret key rate. We observe a similar pattern as in Fig. 6. With a decreasing detector efficiency both secret key rates drop, but the DI secret key rate is far more affected by the imperfections of the detector than its DD analogon.

C. Analytical results – Performance

As the secret fractions are calculated via the coefficients $c_{i,n}^{(k)}$ of the final Bell-diagonal state, it is desirable to analytically characterize the behavior of the coefficients $c_{i,n}^{(k)}$ under ED and ES operations with imperfect devices. Formulating general analytical results is cumbersome due to the recursive nature of the transformation rules for the Bell coefficients under ED and ES, see Eqs. (C1) and (C3). In an idealized scenario, where the source distributes pure states, however, we can find closed transformation rules for the coefficients $c_{i,n}^{(k)}$, depending on the number of nesting levels n and the gate quality p_G. We thus consider the case $c_{1,0}^{(0)} = F_0 = 1$ and $c_{i\geqslant 2,0}^{(0)} = 0$, and since ED is obsolete for maximally entangled states we set $k = 0$. One can show via Eqs. (C3) that the coefficients transform according to

$$c_{1,n}^{(0)} = \frac{1 + 3p_G^{\bar{n}}}{4} \quad \text{and} \quad c_{i\geqslant 2,n}^{(0)} = \frac{1 - p_G^{\bar{n}}}{4} \quad \forall\, n \in \mathbb{N}, \tag{21}$$

where $\bar{n} := 2^n - 1$ denotes the number of intermediate repeater stations. With Eq. (21) one can express the QBERs and the CHSH parameter in terms of $\bar{n}$ and p_G. For the DD QBERs, Eqs. (17), one immediately finds

$$Q_{x,n}^{(0)} = Q_{z,n}^{(0)} = \frac{1 - p_G^{\bar{n}}}{2} \tag{22}$$

and for the DI quantities via Eqs. (18) similarly,

$$Q_{z,n}^{(0)} = \frac{1 - \eta_d^2 p_G^{\bar{n}}}{2}, \tag{23a}$$

$$S_n^{(0)} = 2\sqrt{2}\eta_d^2 p_G^{\bar{n}}. \tag{23b}$$

Recall that the DI secret fraction is only nonvanishing if the CHSH inequality is violated. Thus, we obtain the condition

$$S_n^{(0)} > 2 \Leftrightarrow \eta_d^2 p_G^{\bar{n}} > \frac{1}{\sqrt{2}}, \tag{24}$$

which the parameters p_G, η_d, and $\bar{n}$ have to fulfill. The DD and DI secret fractions then become

$$r_\infty^{\mathrm{DD}} = \eta_d^2 \left[1 - 2h\left(\frac{1 - p_G^{\bar{n}}}{2}\right)\right], \tag{25a}$$

$$r_\infty^{\mathrm{DI}} = 1 - h\left(\frac{1 - \eta_d^2 p_G^{\bar{n}}}{2}\right) - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{2\eta_d^4 p_G^{2\bar{n}} - 1}\right), \tag{25b}$$

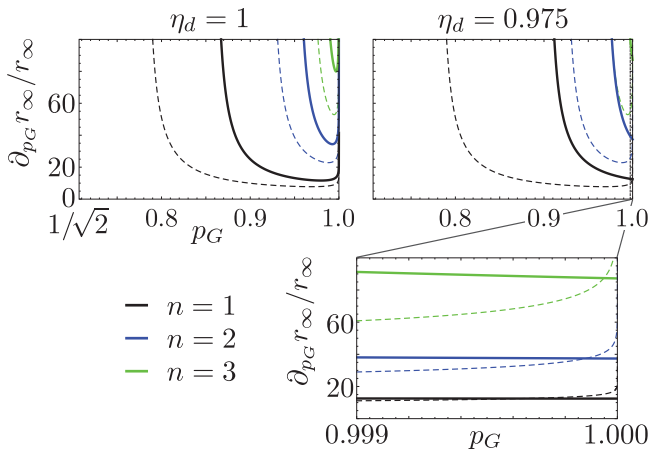

FIG. 8. Relative change $\partial_{p_G} r_\infty / r_\infty$ versus the gate quality p_G in the DD (dashed lines) and DI (solid lines) scenario for detector efficiencies $\eta_d = 1$ and $\eta_d = 0.975$ [see Eqs. (C4b) and (C6b)]. Different numbers of nesting level n are shown, where $n = 1$ corresponds to the leftmost curves and $n = 3$ to the rightmost ones.

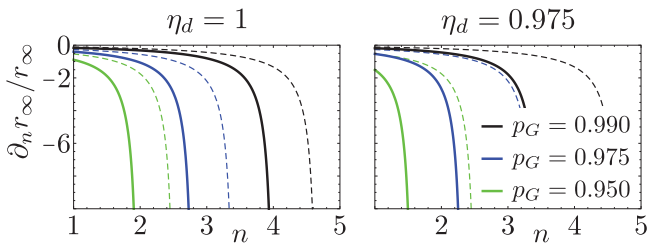

FIG. 9. Relative change $\partial_n r_\infty / r_\infty$ versus the number n in the DD (dashed lines) and DI (solid lines) scenario for detector efficiencies $\eta_d = 1$ and $\eta_d = 0.975$ [see Eqs. (C4c) and (C6c)]. The rightmost curves correspond to the gate quality $p_G = 0.99$ and the leftmost ones to $p_G = 0.95$.

where for r_∞^{DD}, we included the factor η_d^2 compared to Eq. (7). Now, we can investigate the impact of the experimental quantities η_d, p_G, and n onto the secret fractions in terms of partial derivatives, which are given in Eqs. (C4) and (C6) in Appendix C 2. We quantify the influence of the parameter onto the secret fractions via these partial derivatives and thus ask the question which of the two secret fractions, DD or DI, alters its value faster when the corresponding parameter is changed.

1. Impact of the detector efficiency η_d.

Using the fact that $\partial_{\eta_d} r_\infty^{\mathrm{DI}}$ is a monotonic function and respecting the condition given in Eq. (24), one can show that the inequality $\partial_{\eta_d} r_\infty^{\mathrm{DI}} > \partial_{\eta_d} r_\infty^{\mathrm{DD}}$ holds, see Eq. (C8) in Appendix C 2 for details. Hence, the DI secret fraction reacts more sensitively to changes in the detector efficiency than the effective DD secret fraction does.

2. Impact of the gate quality p_G

For the derivatives of the secret fractions with respect to the gate quality p_G and the nesting levels n, the ordering of the corresponding expressions in Eqs. (C4) and (C6) in Appendix C 2 is not as obvious as for the detector efficiency η_d. Thus, for the sake of simplicity, we settle for a numerical comparison. Figure 8 shows the relative change of the derivatives $\partial_{p_G} r_\infty$ in the DD [Eq. (C4b)] and DI [Eq. (C6b)] case with respect to the corresponding secret fraction r_∞ for $\eta_d = 1$ and $\eta_d = 0.975$ as a function of the gate quality. We observe that the relative change of the DI secret fraction is larger than its DD analogon. For $\eta_d < 1$ and almost perfect gates $1 - p_G \ll 1$, though, the opposite is true (see inset in Fig. 8). This follows from the fact that $\partial_{p_G} r_\infty^{\mathrm{DI}}$ no longer diverges for $p_G \to 1$ and $\eta_d < 1$, in contrary to $\partial_{p_G} r_\infty^{\mathrm{DD}}$; see Eqs. (C4b) and (C6b).

However, an important difference is that the relative change in the DI case also depends on the detector efficiency η_d, in contrast to the DD case. Figure 8 also verifies the intuition that the impact of the gate quality p_G rises with an increasing number of nesting levels, i.e., with an increasing number of imperfect quantum operations.

3. Impact of the nesting levels n

To quantify the influence of n, let us extrapolate the integer n to a continuous variable. In Fig. 9 we numerically compare the relative change of $\partial_n r_\infty$, Eqs. (C4c) and (C6c), with respect to corresponding secret fractions r_∞. It confirms that the relative change $\partial_n r_\infty / r_\infty$ in the DI case is larger than its DD analogon, as expected. Note that $\partial_n r_\infty / r_\infty$ is negative and that the DD ratio is again independent of the detector efficiency η_d. One can also observe, that the impact of n dramatically increases with a decreasing gate quality p_G, which is consistent with previous results.

To close this section we conjecture that our analytical results approximately hold for sufficiently pure initial states, since ϵ small contributions to other Bell states $|\phi_{i\neq 1}\rangle$ in the initially distributed states do not significantly alter the state at the end of the ES protocol.

IV. THE HYBRID QUANTUM REPEATER

Let us now consider the hybrid quantum repeater (HQR) introduced by van Loock *et al.* [17] and Ladd *et al.* [38]. It still employs the nested scheme for ES as shown in Fig. 1, but the repeater stations and the physical system representing the qubits are of fundamental difference compared to the OQR. As in [16], we also restrict our investigation to HQRs where unambiguous state discrimination (USD) measurements are involved for state generation [39,40]. In Part IV A of this section, we introduce the concepts of HQRs, and in Part III B the comparison of the DD-DI performance follows.

A. Setup, error model, and repeater rate

In Sec. IV A 1 we review the model for intermediate repeater stations and briefly capture the main ideas behind the entanglement creation in this setup. Afterwards, we present in Sec. IV A 2 the error model for noisy two-qubit gates and explain how to calculate the repeater rate. See [16] for more details.

1. Repeater station – Model

The HQR combines discrete and continuous degrees of freedom. Entanglement is for instance generated between two

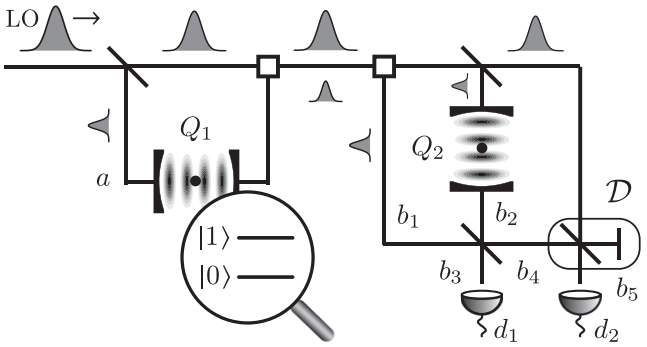

FIG. 10. Illustration of repeater stations in the HQR setup and the USD scheme following [40]. A coherent state $|\alpha\rangle$, the local oscillator (LO), is generated and sent through linear optical elements, such as beam splitters and optical switches. Different optical modes are denoted with a and b_i, for $i \in \{1,\ldots,5\}$. The LO passes a beam splitter and a part of it interacts with qubit Q_1, which is prepared in an equally weighted superposition of its two possible states $|0\rangle$ and $|1\rangle$. The resulting optical state is sent together with the LO to the next repeater station, where again a part of the LO interacts with qubit Q_2, also prepared in an equally weighted superposition of $|0\rangle$ and $|1\rangle$. A $50:50$ beam splitter is applied to modes b_1 and b_2 and a displacement operation $\mathcal{D}$ to the pulse in mode b_4. Depending on the measurement results of detectors d_1 and d_2, an entangled state between qubits Q_1 and Q_2 is generated.

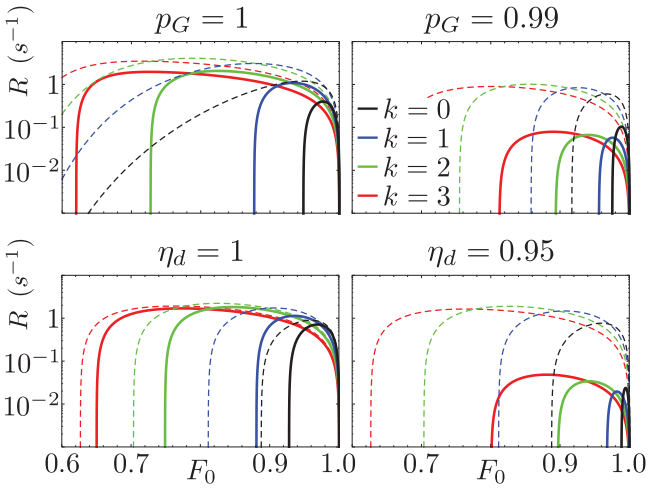

FIG. 11. DD (dashed lines) and DI (solid lines) secret key rate for the HQR versus the fidelity F_0. The total distance is $L = 300$ km, with $n = 2$ nesting levels. Different numbers of initial ED rounds k are shown, where the most narrow curves correspond to $k = 0$ and the most wide ones to $k = 3$. The upper two subfigures show the impact of the effective gate quality, as it is reduced from $p_G = 1$ to $p_G = 0.99$ with a fixed detector efficiency of $\eta_d = 0.975$. The lower subfigures similarly display the influence of the detector efficiency, where we reduce it from $\eta_d = 1$ to $\eta_d = 0.95$ with the fixed parameter $p_G = 0.995$.

trapped ions inside a cavity, which represent the qubits. The entangling interaction, however, is induced via coherent optical states. The interaction between the qubits and the light can thus be described within the Jaynes-Cummings framework [41]. A schematic model for intermediate repeater stations is shown in Fig. 10.

By performing a USD measurement on the optical modes, after they interacted with the qubits, the entangled state

$$\rho_0 = F_0|\phi_1\rangle\langle\phi_1| + (1-F_0)|\phi_2\rangle\langle\phi_2| \tag{26}$$

can be conditionally prepared. For the HQR, the probability P_0 to connect two adjacent repeater stations with an entangled state is given by [16]

$$P_0 = 1 - (2F_0 - 1)^{\frac{\eta_t\eta_d}{1+\eta_t(1-2\eta_d)}}. \tag{27}$$

Note that the probability P_0 vanishes for pure states $\rho_0 = |\phi_1\rangle\langle\phi_1|$ with $F_0 = 1$, in which case it is not possible to generate a secret key. For more details regarding the implementation and state preparation see [16,40].

2. Error model and repeater rate

ES and ED rely on controlled-Z operations. The model for a noisy two-qubit gate needs to be adjusted for the HQR implementation. According to [42], the noisy two-qubit gate $\mathcal{O}$ acting upon the two-qubit state $\chi \equiv \chi_{ab}$, which describes the main errors due to dissipation, is modeled by

$$\begin{aligned}\mathcal{O}(\chi) = \mathcal{O}^{\text{ideal}}\big[&p_c^2(p_G)\chi + (1-p_c(p_G))^2 Z_a Z_b \rho Z_a Z_b \\ &+ p_c(p_G)(1-p_c(p_G))(Z_a\chi Z_a + Z_b\chi Z_b)\big].\end{aligned} \tag{28}$$

Here,

$$p_c(p_G) := \frac{1+\exp\left(-\frac{\pi\left(1-p_G^2\right)}{2\sqrt{p_G}(1+p_G)}\right)}{2} \tag{29}$$

represents the probability for each qubit to not suffer a Z error. The quantity p_G in Eq. (29) is the local transmission parameter that describes the effect of photon losses onto the gate and can thus be seen as an effective gate quality. Following [16], we calculate the repeater rate according to Eq. (2) with deterministic ES, i.e., $P_{\text{ES}} = 1$. We use perfect qubit measurements for the ES and also ED operations, since the imperfections can in principle be eliminated from the protocol at the cost of additional photon losses in the quantum channel, which effectively reduces the gate quality [39]. Note, however, that we account for detector imperfections at the initial entanglement distribution [as η_d enters the probability P_0 in Eq. (27)] and detector imperfections at the final qubit measurements in the laboratories of Alice and Bob. The latter one implies again a factor $P_{\text{click}} = \eta_d^2$ for the DD secret key rate, while in the DI scenario the substitution (9) has to be performed. The DD and DI secret fractions are calculated according to Eqs. (7) and (12), and since the final state is again Bell diagonal, the QBERs and the CHSH parameter are given by Eqs. (17) and (18).

B. Performance: DD vs DI secret key rate

We now want to investigate the influence of the effective gate quality p_G, the detector efficiency η_d, and the number of ED and ES operations on the secret key rates. Figure 11 shows the DD and DI secret key rates versus the fidelity

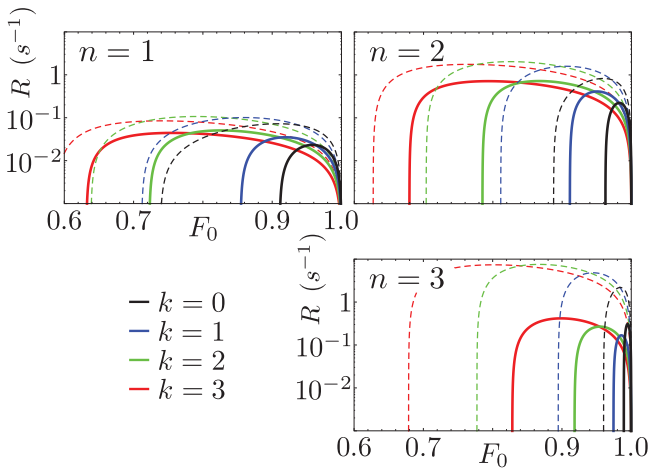

FIG. 12. DD (dashed lines) and DI (solid lines) secret key rate versus the fidelity F_0. The total distance, the gate quality, and the detector efficiency are $L = 300$ km, $p_G = 0.995$, and $\eta_d = 0.975$, respectively. As in Fig. 11, the most narrow curves correspond to $k = 0$ and the most wide ones to $k = 3$ ED rounds. The figure shows the impact of different nesting levels n, varied from $n = 1$ to $n = 3$.

F_0 for several numbers of initial ED rounds k. The total distance is $L = 300$ km with a fixed number of nesting levels $n = 2$. We can observe from the upper two subfigures that gate imperfections have a large impact on the DD secret key rate, as already pointed out in [16]. In the DI case, this becomes even more dramatic. The lower two subfigures show that detector errors do not significantly reduce the DD secret key rate. The DI secret key rate, however, is heavily compromised by these imperfections, as they lead to a mixed state due to the random assignment of measurement results.

We conclude the key rate analysis with Fig. 12, where the secret key rates are shown as a function of the initial fidelity F_0 for several numbers of nesting levels n at a fixed total distance of $L = 300$ km. We consider gate and detector errors by $p_G = 0.995$ and $\eta_d = 0.975$, respectively. As we can see, it is beneficial for the DD secret key rate to increase the number of nesting levels beyond $n = 2$ to reduce photon losses in the fiber. By doing so, the DD secret key rates gain approximately 1 order of magnitude. In the DI case, however, the errors introduced by the larger number of imperfect quantum operations outweigh again the benefits that one gains from a reduced fundamental length L_0. For a given fidelity F_0 the optimal number k of ED rounds is in general different from the DD scenario as well.

V. CONCLUSION AND OUTLOOK

In this work, we provided a detailed systematic analysis on achievable secret key rates of two quantum repeater setups in the device-independent (DI) scenario and compared it to the device-dependent (DD) case. We studied the original quantum repeater (OQR) [15] and the hybrid quantum repeater (HQR) [17]. The analysis includes a numerical investigation on how experimental quantities, such as the gate quality p_G, the detector efficiency η_d, the initial fidelity F_0, and the number of nesting levels n and initial entanglement distillation rounds k, influence the secret key rate. We observed for both setups that the DI security comes at the expense of being particularly sensitive towards malfunctions in the devices. Imperfections of the gates, the detectors, and the sources compromise the achievable DI secret key rate more than the DD one. Hence, for any realistic implementation, there is a gap between these secret key rates that increases with an increasing number of imperfect quantum operations. For the OQR with an idealized photon source, we additionally verified analytically that the parameters p_G, η_d, and n have a stronger impact on the DI secret key rate as they have in the DD scenario.

The proneness of DIQKD to imperfections naturally implies different optimization strategies for the DI and DD secret key rate. In the DD scenario the influence of the gate errors is not as severe as it is in the DI case, thus allowing a shorter fundamental distance L_0 and thus reducing photon losses in the fiber, i.e., in the DI case there are not as many intermediate repeater stations feasible as in the DD one. This immediately yields a stronger limitation for the total distance L that one can overcome in the DI setup. Similarly, the purity of the initially distributed states can be improved via more entanglement distillation rounds in the DD protocol, which makes it more robust to imperfections of the source.

It remains for future investigations to compare different DD and DI protocols, besides the BB84 and the modified Ekert protocol [3,11]. Other ideas are to extend this analysis to different quantum repeater models, such as the DLCZ quantum repeater [43]. One could also include more error sources of the quantum repeater, e.g., errors introduced by quantum memories, and investigate their impact on the secret key rates. For the latter one, we conjecture from the provided secret-key-rate analysis that further imperfections have a qualitatively similar impact on the DI secret key rate as the ones discussed in this work.

ACKNOWLEDGMENTS

The authors acknowledge support from the Federal Ministry of Education and Research (BMBF, Project Q.com-Q) and thank Peter van Loock for discussion.

APPENDIX A: REPEATER RATE – PROBABILISTIC ES

Here, we provide more details for the repeater rate with probabilistic ES in Eq. (5). In [24], the repeater rate

$$R_{\mathrm{rep}}^{\mathrm{prob}} = \frac{1}{T_0}\left(\frac{2}{3}\right)^n P_0' \prod_{i=1}^{n} P_{\mathrm{ES}}^{(i)} \tag{A1}$$

without initial ED is derived for $P_0' \ll 1$, where P_0' denotes the success probability to connect two adjacent repeater stations in nesting level $n = 0$ with an entangled pair (see also Fig. 1). We review the derivation of Eq. (A1) and explain how to improve this rate. Afterwards we include initial ED, inspired by [16].

1. Repeater rate without ED

Following [24], the number of attempts n_0 to successfully create an elementary link is governed by the probability distribution

$$p(n_0) = (1 - P_0')^{n_0 - 1} P_0', \tag{A2}$$

which yields the expectation value

$$\langle n_0\rangle = \sum_{n\in\mathbb{N}_0} n_0 p(n_0) = \frac{1}{P_0'}. \tag{A3}$$

In order to perform ES, one needs entangled states in two neighboring segments of the repeater line. The corresponding combined probability distribution is given by

$$\tilde{p}(n_0) = p(n_0)^2 + 2p(n_0)\sum_{k=1}^{n_0-1} p(k), \tag{A4}$$

which results in the average number of attempts

$$\langle \tilde{n}_0\rangle = \sum_{n_0\in\mathbb{N}_0} n_0 \tilde{p}(n_0) = \frac{3-2P_0'}{(2-P_0')P_0'}. \tag{A5}$$

The first ES step can now be performed, which succeeds with probability $P_{\mathrm{ES}}^{(1)}$, thus increasing the average number of attempts to create an entangled link in nesting level $n=1$ according to

$$\langle n_1\rangle = \langle \tilde{n}_0\rangle \sum_{k\in\mathbb{N}_0}(k+1)(1-P_{\mathrm{ES}}^{(1)})^k P_{\mathrm{ES}}^{(1)} = \frac{\langle \tilde{n}_0\rangle}{P_{\mathrm{ES}}^{(1)}}. \tag{A6}$$

From now on, our approach deviates from the one in [24], where $\langle \tilde{n}_0\rangle$ in Eq. (A5) is set to $3/2P_0'$, which is a good approximation for $P_0' \ll 1$. Here, we rewrite Eq. (A5) as

$$\langle \tilde{n}_0\rangle = \frac{3-2P_0'}{(2-P_0')P_0'} = \frac{1}{P_0'}\frac{3}{2}a_{\mathrm{ES}}^{(0)}, \tag{A7}$$

where we defined

$$a_{\mathrm{ES}}^{(0)} := \frac{1-2P_0'/3}{1-P_0'/2}. \tag{A8}$$

In complete analogy to Eq. (A3), the probability P_1 to create an entangled link in nesting level $n=1$ is given by the inverse of Eq. (A6), and we can define an according probability distribution $p(n_1)$ via P_1. This is in general not true, as the success probability of establishing a link in a higher nesting level $n=i$ in the n_ith attempt depends on success probabilities of the previous nesting levels [24] and the corresponding probability distribution $p(n_i)$ is not analog to the form given in Eq. (A2). However, this modification allows us to obtain the recursion

$$\langle n_i\rangle = \frac{1}{P_i} = \frac{\langle \tilde{n}_{i-1}\rangle}{P_{\mathrm{ES}}^{(i)}} \quad \forall\, i\in\mathbb{N}, \tag{A9}$$

$$\langle \tilde{n}_i\rangle = \frac{3-2P_i}{(2-P_i)P_i} = \frac{1}{P_i}\frac{3}{2}a_{\mathrm{ES}}^{(i)} \quad \forall\, i\in\mathbb{N}, \tag{A10}$$

if we iterate this argument to arbitrary nesting levels. The constants $a_{\mathrm{ES}}^{(i)}$ are defined as in Eq. (A8) with the corresponding probability P_i. The beginning of the recursion is given in Eqs. (A3) and (A7). Note that this approach also only yields a good approximation for $P_0' \ll 1$, but this strategy leads to repeater rates which are closer to achievable ones that are calculated with Monte Carlo simulations.

With the relations (A9) and (A10) we can express the average number of attempts to establish a single entangled link at the maximum nesting level $n=N$ as

$$\begin{aligned}\langle n_N\rangle &= \frac{\langle \tilde{n}_{N-1}\rangle}{P_{\mathrm{ES}}^{(N)}} = \frac{3}{2}\frac{a_{\mathrm{ES}}^{(N-1)}}{P_{\mathrm{ES}}^{(N)}}\frac{1}{P_{N-1}} = \cdots \\ &= \left(\frac{3}{2}\right)^N \frac{1}{P_0'}\prod_{i=1}^{N}\frac{a_{\mathrm{ES}}^{(i-1)}}{P_{\mathrm{ES}}^{(i)}}.\end{aligned} \tag{A11}$$

Each attempt lasts the fundamental time T_0, thus yielding the repeater rate

$$R_{\mathrm{rep}}^{\mathrm{prob}} = \frac{1}{T_0}\left(\frac{2}{3}\right)^N P_0' \prod_{i=1}^{N}\frac{P_{\mathrm{ES}}^{(i)}}{a_{\mathrm{ES}}^{(i-1)}}. \tag{A12}$$

2. Repeater rate with ED

In the spirit of [16], we now include initial ED, which is performed at each segment at nesting level $n=0$ and which thus only affects the success probability P_0'. Thus, P_0' is given by the recursively defined probabilities $P_0' = P_{L_0}^{(k)}$ for successful ED in k rounds in Eq. (3). By plugging the recursive probabilities into each other, one arrives at

$$P_{L_0}^{(k)} = \frac{2}{3}\frac{P_{\mathrm{ED}}^{(k)}}{a_{\mathrm{ED}}^{(k-1)}}P_{L_0}^{(k-1)} = \cdots = \left(\frac{2}{3}\right)^k P_0 \prod_{j=1}^{k}\frac{P_{\mathrm{ED}}^{(j)}}{a_{\mathrm{ED}}^{(j-1)}}, \tag{A13}$$

where we defined the constants $a_{\mathrm{ED}}^{(j)}$ for ED as in Eq. (A8). Replacing P_0' in Eq. (A12) with the right-hand side of Eq. (A13) yields the repeater rate in Eq. (5).

APPENDIX B: ED AND ES PROTOCOL

For completeness, we review the ED and ES protocols [16,18], which determine together with the noisy two-qubit gate models in Eqs. (19) and (28) the transformation of the coefficients $c_{i,n}^{(k)}$ (see Appendixes C and D). Let $C_{\mathrm{NOT}}^{s\to t}$ denote a controlled-X operation, where s and t indicate the source and the target qubit, respectively.

1. Entanglement distillation

Suppose Alice and Bob share the two states ρ_{a_i,b_i} for $i\in\{1,2\}$. The following steps are performed. (i) Alice/Bob rotates her/his particles by $+/-\frac{\pi}{2}$ around the X axis in the computational basis $\{|0\rangle,|1\rangle\}$. (ii) Alice/Bob applies $C_{\mathrm{NOT}}^{a_1\to a_2}/C_{\mathrm{NOT}}^{b_1\to b_2}$. (iii) The state ρ_{a_2,b_2} is measured in the computational basis. Then, if their measurement results coincide, the state ρ_{a_1,b_1} has been purified. Otherwise the state is discarded.

2. Entanglement swapping

Suppose the two entangled states $\rho_{a,b}$ and $\rho_{c,d}$ are distributed among two adjacent repeater stations. The following algorithm performs ES between these two states. (i) A $C_{\mathrm{NOT}}^{b\to c}$-gate is applied. (ii) Qubits b and c are measured in the basis $\{|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}\}$ and $\{|0\rangle,|1\rangle\}$, respectively. (iii) Depending on the measurement outcomes, a single-qubit rotation on qubit d is performed and one obtains the entangled state $\rho_{a,d}$.

APPENDIX C: ADDITIONAL MATERIAL – OQR

1. Transformation under ED and ES

With the discussed error models and the ED and ES protocols, we recall the transformation rules of the coefficients $c_{i,n}^{(k)}$. For the OQR, gate errors are modeled according to Eq. (19). See [16,18] for details.

a. Entanglement distillation. Two copies of the Bell-diagonal state $\rho^{(k-1)} = \sum_{i=1}^{4} c_i^{(k-1)} |\phi_i\rangle\langle\phi_i|$ represent the input states for the ED protocol. Provided the ED protocol is successful, one is left with one Bell-diagonal state with the coefficients

$$c_1^{(k)} = \frac{1}{8P_{\mathrm{ED}}^{\prime(k)}}\left[1 + p_G^2\left(8c_1^{(k-1)\,2} + 8c_4^{(k-1)\,2} - 1\right)\right], \quad \text{(C1a)}$$

$$c_2^{(k)} = \frac{1}{8P_{\mathrm{ED}}^{\prime(k)}}\left[1 - p_G^2\left(1 - 16c_1^{(k-1)}c_4^{(k-1)}\right)\right], \quad \text{(C1b)}$$

$$c_3^{(k)} = \frac{1}{8P_{\mathrm{ED}}^{\prime(k)}}\left[1 + p_G^2\left(8c_2^{(k-1)\,2} + 8c_3^{(k-1)\,2} - 1\right)\right], \quad \text{(C1c)}$$

$$c_4^{(k)} = \frac{1}{8P_{\mathrm{ED}}^{\prime(k)}}\left[1 - p_G^2\left(1 - 16c_2^{(k-1)}c_3^{(k-1)}\right)\right], \quad \text{(C1d)}$$

where the success probability of ED round k is

$$P_{\mathrm{ED}}^{\prime(k)} = \frac{1}{2}\left[1 + p_G^2\left(2c_1^{(k-1)} + 2c_4^{(k-1)} - 1\right)^2\right]. \quad \text{(C2)}$$

b. Entanglement swapping. Two qubit pairs, each in the Bell-diagonal state $\rho_{n-1} = \sum_{i=1}^{4} c_{i,n-1} |\phi_i\rangle\langle\phi_i|$, are the input states to the ES protocol, that includes a probabilistic Bell measurement on two qubits, one of each pair. The two qubits not involved in the Bell measurement are again in a Bell-diagonal state with coefficients $c_{i,n}$. The transformation rules are

$$c_{1,n} = \frac{1 - p_G}{4} + p_G \sum_{i=1}^{4} c_{i,n-1}^2, \quad \text{(C3a)}$$

$$c_{2,n} = \frac{1 - p_G}{4} + 2p_G(c_{1,n-1}c_{2,n-1} + c_{3,n-1}c_{4,n-1}), \quad \text{(C3b)}$$

$$c_{3,n} = \frac{1 - p_G}{4} + 2p_G(c_{1,n-1}c_{3,n-1} + c_{2,n-1}c_{4,n-1}), \quad \text{(C3c)}$$

$$c_{4,n} = \frac{1 - p_G}{4} + 2p_G(c_{1,n-1}c_{4,n-1} + c_{2,n-1}c_{3,n-1}), \quad \text{(C3d)}$$

and the success probability for ES is given by $P_{\mathrm{ES}}^{(n)} = \eta_d^2$, neglecting dark counts of the detector.

2. Analytical calculations

a. Partial derivatives of secret fractions. The partial derivatives of r_∞^{DD}, Eq. (25a), with respect to η_d, p_G, and n are given by

$$\partial_{\eta_d} r_\infty^{\mathrm{DD}} = 2\eta_d\left[1 - 2h\left(\frac{1 - p_G^{\bar{n}}}{2}\right)\right], \quad \text{(C4a)}$$

$$\partial_{p_G} r_\infty^{\mathrm{DD}} = 2\frac{\bar{n}\eta_d^2 p_G^{\bar{n}-1}}{\ln(2)}\operatorname{artanh}\left(p_G^{\bar{n}}\right), \quad \text{(C4b)}$$

$$\partial_n r_\infty^{\mathrm{DD}} = 2(\bar{n} + 1)\eta_d^2 p_G^{\bar{n}} \ln(p_G)\operatorname{artanh}\left(p_G^{\bar{n}}\right), \quad \text{(C4c)}$$

where we introduced the area hyperbolic tangent

$$\operatorname{artanh}(x) := \frac{1}{2}\ln\left(\frac{1 + x}{1 - x}\right) \quad \forall\, x \in (-1,1), \quad \text{(C5)}$$

which is the inverse tangent hyperbolic function. The partial derivatives of r_∞^{DI}, Eq. (25b), with respect to η_d, p_G, and n are

$$\partial_{\eta_d} r_\infty^{\mathrm{DI}} = \frac{2\eta_d p_G^{\bar{n}}}{\ln(2)} q(\eta_d, p_G, \bar{n}), \quad \text{(C6a)}$$

$$\partial_{p_G} r_\infty^{\mathrm{DI}} = \frac{\bar{n}\eta_d^2 p_G^{\bar{n}-1}}{\ln(2)} q(\eta_d, p_G, \bar{n}), \quad \text{(C6b)}$$

$$\partial_n r_\infty^{\mathrm{DI}} = (\bar{n} + 1)\eta_d^2 p_G^{\bar{n}} \ln(p_G) q(\eta_d, p_G, \bar{n}), \quad \text{(C6c)}$$

where the function $q(\eta_d, p_G, \bar{n})$ is defined as

$$q(\eta_d, p_G, \bar{n}) := \frac{2\eta_d^2 p_G^{\bar{n}}}{\sqrt{2\eta_d^4 p_G^{2\bar{n}} - 1}}\operatorname{artanh}\left(\sqrt{2\eta_d^4 p_G^{2\bar{n}} - 1}\right) + \operatorname{artanh}\left(\eta_d^2 p_G^{\bar{n}}\right). \quad \text{(C7)}$$

b. Comparison: Impact of detector efficiency. For the partial derivatives of r_∞^{DD} and r_∞^{DI} with respect to the detector efficiency, Eqs. (C4a) and (C6a), one can derive an ordering relation to show that η_d has a larger impact in the DI scenario. Note that $\partial_{\eta_d} r_\infty^{\mathrm{DI}}$ is positive for all parameters η_d, p_G, and $\bar{n}$ that fulfill the condition (24) and that $\eta_d \partial_{\eta_d} r_\infty^{\mathrm{DI}}$ is a strictly monotonically increasing function of $\eta_d^2 p_G^{\bar{n}}$. Hence, the following ordering holds:

$$\partial_{\eta_d} r_\infty^{\mathrm{DI}} \geqslant \eta_d \partial_{\eta_d} r_\infty^{\mathrm{DI}} \geqslant \lim_{\eta_d^2 p_G^{\bar{n}} \to \sqrt{2}^{-1}} \left(\eta_d \partial_{\eta_d} r_\infty^{\mathrm{DI}}\right) = \frac{\sqrt{2}}{\ln(2)}\left[\operatorname{artanh}(1/\sqrt{2}) + \sqrt{2}\right] > 2, \quad \text{(C8)}$$

where we used $\operatorname{artanh}(1/\sqrt{2}) > 0$ and $0 \leqslant \eta_d, \ln(2) \leqslant 1$. Finally, note that in the DD case, η_d enters the effective secret fraction $\eta_d^2 r_\infty^{\mathrm{BB84}}$ as a factor with r_∞^{BB84} given in Eq. (7). This partially derived with respect to η_d yields $2\eta_d r_\infty^{\mathrm{BB84}}$, which is upper bounded by 2. This proves the inequality $\partial_{\eta_d} r_\infty^{\mathrm{DI}} > \partial_{\eta_d} r_\infty^{\mathrm{DD}}$ as claimed in Sec. III C.

APPENDIX D: ADDITIONAL MATERIAL – HQR

1. Transformation under ED and ES

Here, we give the transformation relations for the Bell coefficients under ED and ES for the HQR, where gate errors enter the calculation via Eq. (28). See [16].

a. Entanglement distillation. We calculate the coefficients after ED round k with respect to the coefficients after ED round $k-1$, which we do not label here explicitly for a better overview. Also, we suppress the dependency on p_G of $p_c(p_G)$ and introduce the abbreviation $\bar{p} := 2p_c(p_c-1)$:

$$c_1^{(k)} = \frac{1}{P_{\mathrm{ED}}^{(k)}}\left\{\bar{p}^2(c_1-c_4)(c_1-c_4+c_2-c_3)+\bar{p}\left[c_1^2+c_4^2+(c_1-c_4)^2-c_1c_3-c_2c_4\right]+c_1^2+c_4^2\right\}, \tag{D1a}$$

$$c_2^{(k)} = \frac{1}{P_{\mathrm{ED}}^{(k)}}\{\bar{p}^2[c_1c_3+(c_2-c_3-c_4)c_4]-\bar{p}(c_3+c_4)c_4+2(\bar{p}+1)^2c_1c_4-\bar{p}(\bar{p}+1)c_1(c_1+c_2)\}, \tag{D1b}$$

$$c_3^{(k)} = \frac{1}{P_{\mathrm{ED}}^{(k)}}\left\{\bar{p}^2(c_1c_2+c_3c_4)+(\bar{p}+1)^2\left(c_2^2+c_3^2\right)-\bar{p}(\bar{p}+1)[c_2(c_3+c_4)+(c_1+c_2)c_3]\right\}, \tag{D1c}$$

$$c_4^{(k)} = \frac{1}{P_{\mathrm{ED}}^{(k)}}\{\bar{p}^2[c_2c_4+(c_1-c_3-c_4)c_3]-\bar{p}c_3(c_3+c_4)+2(\bar{p}+1)^2c_2c_3-\bar{p}(\bar{p}+1)(c_1+c_2)c_2\}. \tag{D1d}$$

The success probability for ED round k is given by

$$P_{\mathrm{ED}}^{\prime(k)} = (c_1+c_4)^2+(c_2+c_3)^2+\bar{p}(2c_1+2c_4-1)^2. \tag{D2}$$

b. Entanglement swapping. Similar to Eqs. (D1), we neglect the index for the previous nesting level $n-1$. The Bell coefficients transform under the ES protocol according to

$$c_{1,n} = 2(c_1c_4+c_2c_3)+2p_c[c_1(1-c_1-3c_4)-c_2(c_3-c_4)-(c_2-c_4)c_3]+p_c^2(2c_1+2c_4-1)^2, \tag{D3a}$$

$$c_{2,n} = 2(c_1c_3+c_2c_4)+p_c[(2c_1+2c_4-1)^2+2(c_1-c_4)(c_2-c_3)]-p_c^2(2c_1+2c_4-1)^2, \tag{D3b}$$

$$c_{3,n} = 2(c_1c_2+c_3c_4)+p_c[(2c_1+2c_4-1)^2-2(c_1-c_4)(c_2-c_3)]-p_c^2(2c_1+2c_4-1)^2, \tag{D3c}$$

$$c_{4,n} = \sum_{i=1}^{4}c_i^2-2p_c\left[\sum_{i=1}^{4}c_i^2-(c_1+c_4)(c_2+c_3)\right]+p_c^2(2c_1+2c_4-1)^2. \tag{D3d}$$

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] J. A. Buchmann, *Introduction to Cryptography* (Springer, New York, 2004).
[3] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, Bangalore, India, 1984), pp. 175–179.
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[7] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, in *Advances in Cryptology, EUROCRYPT'00* (Springer-Verlag, Berlin, 2000), pp. 289–299.
[8] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[9] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[10] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[12] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Palo Alto, California, 1998), pp. 503–509.
[13] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[14] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[15] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[16] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).
[17] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).
[18] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[19] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[20] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[21] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[22] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[23] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).
[24] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).
[25] E. Shchukin, F. Schmidt, and P. van Loock, arXiv:1710.06214 .
[26] H.-K. Lo, H. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
[27] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).
[28] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Phys. Rev. Lett. **107**, 170404 (2011).
[29] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).
[30] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[31] E. A. Aguilar, R. Ramanathan, J. Kofler, and M. Pawłowski, Phys. Rev. A **94**, 022305 (2016).
[32] R. Arnon-Friedman, R. Renner, and T. Vidick, arXiv:1607.01797.
[33] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[34] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[35] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[36] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[37] R. H. Hadfield, Nat. Photonics **3**, 696 (2009).
[38] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. **8**, 184 (2006).
[39] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).
[40] K. Azuma, N. Sota, R. Namiki, S. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303 (2009).
[41] E. T. Jaynes and F. W. Cummings, Proc. IEEE **51**, 89 (1963).
[42] S. G. R. Louis, W. J. Munro, T. P. Spiller, and K. Nemoto, Phys. Rev. A **78**, 022326 (2008).
[43] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).

Appendix B

Propagation of generalized Pauli errors in qudit Clifford circuits

Title:	Propagation of generalized Pauli errors in qudit Clifford circuits
Authors:	Daniel Miller, Timo Holz, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review A
Impact factor:	2.907 (2018)
Date of submission:	25 July 2018
Publication status:	Published
Contribution by TH:	Second author (input approx. 10%)

This publication corresponds to Ref. [MHKB18]. A summary of the results is presented in Chap. 7. The main research objective was jointly established by and regularly discussed among all authors. I helped conceptualizing general research ideas which led to the results presented in the article. Furthermore, I wrote parts of the manuscript, in particular the description of Fig. (7) of the article which constitutes one of the central results. Finally, I helped proofreading and improving the entire article.

Propagation of generalized Pauli errors in qudit Clifford circuits

Daniel Miller,* Timo Holz, Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

(Received 25 July 2018; published 14 November 2018)

It is important for performance studies in quantum technologies to analyze quantum circuits in the presence of noise. We introduce an error probability tensor, a tool to track generalized Pauli error statistics of qudits within quantum circuits composed of qudit Clifford gates. Our framework is compatible with qudit stabilizer quantum error-correcting codes. We show how the error probability tensor can be applied in the most general case, and we demonstrate an error analysis of bipartite qudit repeaters with quantum error correction. We provide an exact analytical solution of the error statistics of the state distributed by such a repeater. For a fixed number of degrees of freedom, we observe that higher dimensional qudits can outperform qubits in terms of distributed entanglement.

DOI: 10.1103/PhysRevA.98.052316

I. INTRODUCTION

Quantum computation and quantum communication are progressing fields with the prospect of faster computation [1,2] and secure communication [3–5] in comparison to their respective classical counterparts. Entangled quantum states are a key resource for quantum communication. The most promising approach to distribute entangled states among remote users are quantum repeaters [6–8]. Potentially fruitful candidates for units of quantum information are higher dimensional quantum systems, so-called qudits, as they inherently possess multiple degrees of freedom while being implementable with single photons [9–14].

Often, quantum protocols are designed under the assumption of perfect control of the utilized quantum systems. Real experiments, however, are always subject to noise. This necessitates studying such protocols in the presence of errors. In general, this problem is computationally hard since exponentially many classical resources are needed to simulate a quantum system. Explicit error analyses, however, have been carried out, e.g., for protocols based on qubits [15–17]. In accordance with the Gottesman-Knill theorem [18], this is possible due to the restriction to Clifford gates and Pauli error channels. In Ref. [17], Janardan *et al.* introduce a so-called error probability vector which can be used to estimate the success probability of quantum protocols composed of Clifford operations in the presence of Pauli errors.

In this paper, we extend the applicability of this tool to qudits of fixed but arbitrary dimension $D \geqslant 2$. For analytical investigations, it is helpful to rearrange its entries into a tensor, which we refer to as *error probability tensor*. To maintain compatibility with qudit stabilizer quantum error-correcting codes (QECCs), we use the same generalization of Pauli operators as in Refs. [19,20]. These generalized Pauli operators are unitary, traceless, and form an orthonormal basis for complex $D \times D$ matrices. Our error probability tensor provides a systematic procedure to track the statistics of generalized Pauli errors through quantum circuits composed of Clifford gates—gates which transform generalized Pauli operators into one another.

The paper is structured as follows. In Sec. II, we review the necessary background about qudits. In Sec. III, we define the error probability tensor and describe its use. In Sec. IV, we apply the error probability tensor for the error analysis of a qudit repeater line [21–23]. In Sec. V, we conclude and give an outlook on future work.

II. SETTING

In this section, the notation we will use throughout the paper is introduced. It covers basic quantum information processing with qudits.

A. Physical and logical qudits

A qudit is a quantum system with a Hilbert space of dimension $D \geqslant 2$. Following Ref. [24], we label computational basis states with elements in $\mathbb{Z}/D\mathbb{Z} = \{0, 1, \ldots, D-1\}$, the ring of integers modulo D. Qudit pure states are written as $z_0 |0\rangle + z_1 |1\rangle + \cdots + z_{D-1} |D-1\rangle$ with coefficients $z_j \in \mathbb{C}$, $\sum_{j\in\mathbb{Z}/D\mathbb{Z}} |z_j|^2 = 1$. Similarly, for pure n-qudit systems we have

$$|\psi\rangle = \sum_{\mathbf{j}\in(\mathbb{Z}/D\mathbb{Z})^n} z_{\mathbf{j}} \, |\mathbf{j}\rangle \,, \tag{1}$$

where the multiqudit computational basis states $|\mathbf{j}\rangle$ are labeled by vectors $\mathbf{j} = (j_1, \ldots, j_n)$ in the free module $(\mathbb{Z}/D\mathbb{Z})^n$. In the special case where D is a prime number, $\mathbb{Z}/D\mathbb{Z}$ is the same as $\mathbb{F}_D$, the finite field of order D. If all qudits are measured in the computational basis, the measurement result is the vector $\mathbf{j}$ with probability $|z_{\mathbf{j}}|^2$.

To correct errors, QECCs can be employed. An $[\![n, k, d]\!]_D$ QECC encodes n physical qudits into $k \leqslant n$ logical qudits. The distance d of the code is the minimal weight of an error

*daniel.miller@hhu.de

that maps a codeword to a different codeword. A QECC with distance d can correct up to $\lfloor (d-1)/2 \rfloor$ errors on arbitrary qudits [24]. Stabilizer QECCs for higher dimensional qudits, first introduced by Gottesman [19], have a logical code space stabilized by an Abelian subgroup of the generalized Pauli group. In our error analysis, we consider quantum polynomial codes [25–28] whose construction is outlined in Appendix A.

B. Quantum computation with qudits

Here we review the important classes of generalized Pauli gates and error channels, as well as qudit Clifford gates [19]. Up to a global phase, the generalized Pauli operators on a single qudit are products of the unitary operators

$$X := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} |k+1\rangle \langle k| \tag{2}$$

and

$$Z := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} \omega^k |k\rangle \langle k|, \tag{3}$$

where $\omega := \mathrm{e}^{2\pi i/D}$. For n qudits, there are (up to a global phase) D^{2n} different generalized Pauli operators, each of which can be written as

$$X^{\mathbf{r}} Z^{\mathbf{s}} := \bigotimes_{i=1}^{n} X^{r_i} Z^{s_i} = \sum_{\mathbf{k} \in (\mathbb{Z}/D\mathbb{Z})^n} \omega^{\mathbf{k}\cdot\mathbf{s}} |\mathbf{k}+\mathbf{r}\rangle \langle \mathbf{k}| \tag{4}$$

for unique vectors $\mathbf{r}, \mathbf{s} \in (\mathbb{Z}/D\mathbb{Z})^n$, where $\mathbf{k}\cdot\mathbf{s} = \sum_{i=1}^{n} k_i s_i$ is the standard bilinear form, and $\mathbf{k}+\mathbf{r} = (k_1 + r_1, \ldots, k_n + r_n)$ is the vector addition in $(\mathbb{Z}/D\mathbb{Z})^n$. Two generalized Pauli operators commute up to a phase,

$$(X^{\mathbf{r}} Z^{\mathbf{s}})(X^{\mathbf{r}'} Z^{\mathbf{s}'}) = \omega^{\mathbf{r}'\cdot\mathbf{s} - \mathbf{r}\cdot\mathbf{s}'} (X^{\mathbf{r}'} Z^{\mathbf{s}'})(X^{\mathbf{r}} Z^{\mathbf{s}}). \tag{5}$$

A generalized Pauli error channel $\mathcal{F} : \rho \mapsto \mathcal{F}(\rho)$ is a completely positive trace-preserving map with Kraus operators $\sqrt{f_{\mathbf{r},\mathbf{s}}} X^{\mathbf{r}} Z^{\mathbf{s}}$,

$$\mathcal{F}(\rho) = \sum_{\mathbf{r},\mathbf{s} \in (\mathbb{Z}/D\mathbb{Z})^n} f_{\mathbf{r},\mathbf{s}} (X^{\mathbf{r}} Z^{\mathbf{s}}) \rho (X^{\mathbf{r}} Z^{\mathbf{s}})^\dagger, \tag{6}$$

where $\sum_{\mathbf{r},\mathbf{s}} f_{\mathbf{r},\mathbf{s}} = 1$. This can be seen as the application of the Pauli operator $X^{\mathbf{r}} Z^{\mathbf{s}}$ to the state ρ with probability $f_{\mathbf{r},\mathbf{s}}$. The n-qudit depolarizing channel (see Appendix B),

$$\mathcal{F}_{\mathrm{dep}} : \rho \longmapsto f \frac{\mathbb{1}}{D^n} + (1-f)\rho, \tag{7}$$

is such a generalized Pauli error channel with probabilities

$$f_{\mathbf{r},\mathbf{s}} = \begin{cases} 1 - f + \frac{f}{D^{2n}} & \text{if } \mathbf{r} = \mathbf{s} = (0, \ldots, 0) \\ \frac{f}{D^{2n}} & \text{otherwise} \end{cases}. \tag{8}$$

The qudit Clifford group is the largest set of unitary operators which transform Pauli operators into one another; i.e., for every Clifford operator U and all vectors $\mathbf{r}, \mathbf{s}$, there are some vectors $\mathbf{r}', \mathbf{s}'$ such that $U(X^{\mathbf{r}} Z^{\mathbf{s}})U^\dagger \propto X^{\mathbf{r}'} Z^{\mathbf{s}'}$ holds ($\propto$ means up to a global phase). An important single-qudit Clifford gate is the Fourier gate,

$$F := \frac{1}{\sqrt{D}} \sum_{j,k \in \mathbb{Z}/D\mathbb{Z}} \omega^{jk} |j\rangle \langle k|, \tag{9}$$

which satisfies $FXF^\dagger = Z$ and $FZF^\dagger = X^{-1}$. For $D = 2$, the Fourier gate equals the Hadamard gate $H = (X+Z)/\sqrt{2}$. Another common single-qudit Clifford gate is the multiplication-with-l gate,

$$M(l) := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} |kl\rangle \langle k|, \tag{10}$$

where $l \in \mathbb{Z}/D\mathbb{Z}$ must be invertible such that $M(l)$ is unitary. The controlled-X and controlled-Z gates,

$$\mathrm{CX} := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} |k\rangle \langle k| \otimes X^k \tag{11}$$

and

$$\mathrm{CZ} := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} |k\rangle \langle k| \otimes Z^k, \tag{12}$$

are examples of important two-qudit Clifford gates.

III. TRACKING OF ERROR STATISTICS

Errors can originate from the malfunction of quantum gates. One can model a noisy quantum circuit by a sequence of ideal quantum gates U_i, each of which is followed by an error channel $\mathcal{F}_i$, as depicted in Fig. 1(a). All errors propagate to the end of the circuit giving rise to a single error channel $\mathcal{E}$; cf. Fig. 1(b), which describes the error statistics of the circuit as a whole. In general, it is difficult to derive $\mathcal{E}$ from the $\mathcal{F}_i$.

Here, we develop a mathematical framework to calculate the final error channel $\mathcal{E}$ in the case of qudit Clifford gates U_i and generalized Pauli channels $\mathcal{F}_i$. We start with the definition of the error probability tensor, and, in the subsequent subsections, we describe how to employ it for error analyses.

A. Definition of the error probability tensor

Throughout this paper, we can consider the case where the error statistics of the qudits' state are given by some generalized Pauli error channel $\mathcal{E}$; i.e., the qudits are in an erroneous state

$$\mathcal{E}(\rho) = \sum_{\mathbf{r},\mathbf{s} \in (\mathbb{Z}/D\mathbb{Z})^n} p_{\mathbf{r},\mathbf{s}} (X^{\mathbf{r}} Z^{\mathbf{s}}) \rho (X^{\mathbf{r}} Z^{\mathbf{s}})^\dagger, \tag{13}$$

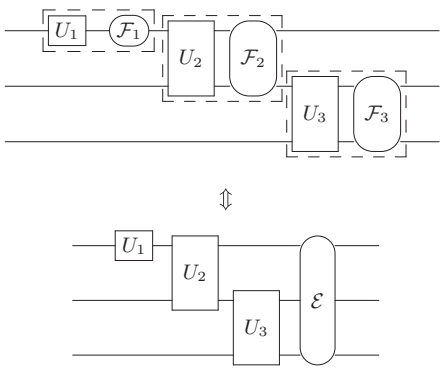

FIG. 1. A quantum circuit with noise modeled by error channels $\mathcal{F}_i$, after ideal unitary gates U_i (top), is mathematically equivalent to an ideal quantum circuit followed by some error channel $\mathcal{E}$ (bottom).

instead of the desired state ρ, where the coefficients $p_{\mathbf{r},\mathbf{s}} \geqslant 0$ sum to 1. Inspired by the notion of error probability vectors [17], we regard these D^{2n} coefficients as entries of a tensor

$$P := (p_{\mathbf{r},\mathbf{s}})_{\mathbf{r},\mathbf{s}\in(\mathbb{Z}/D\mathbb{Z})^n}, \tag{14}$$

which has $2n$ indices, $(\mathbf{r},\mathbf{s}) = ((r_1,\ldots,r_n),(s_1,\ldots,s_n))$. We call P the *error probability tensor*. The error statistics of the state ρ are uniquely determined by the entries of this tensor.

B. Updating the error probability tensor

In our approach, it suffices to know how $\mathcal{E}$, or equivalently P, changes after each instance in a quantum circuit. Starting with the identity channel $\mathcal{E} = \mathrm{id}$ at the beginning of the circuit, one can track how the error statistics transform step by step, until the end of the circuit. In this section, we present rules of how the error probability tensor is updated at every single step. Across qudit Clifford gates, its entries are permuted. At generalized Pauli error channels, the entries are updated via a tensor equation.

1. Qudit Clifford gates; permutations

The propagation of single generalized Pauli errors across qudit Clifford gates is well known [19,20]; cf. Fig. 2. For the propagation of full error statistics, we use the fact that a qudit Clifford gate U defines an automorphism of $(\mathbb{Z}/D\mathbb{Z})^n \times (\mathbb{Z}/D\mathbb{Z})^n$, $\pi_U : (\mathbf{r}',\mathbf{s}') \mapsto (\mathbf{r},\mathbf{s})$ via

$$U(X^{\mathbf{r}}Z^{\mathbf{s}})U^\dagger \propto X^{\mathbf{r}'}Z^{\mathbf{s}'}. \tag{15}$$

After the application of the (ideal) gate U, the error probability tensor $P = (p_{\mathbf{r},\mathbf{s}})_{\mathbf{r},\mathbf{s}}$ is updated to

$$P' := (p'_{\mathbf{r}',\mathbf{s}'})_{\mathbf{r}',\mathbf{s}'} = (p_{\pi_U(\mathbf{r}',\mathbf{s}')})_{\mathbf{r}',\mathbf{s}'}. \tag{16}$$

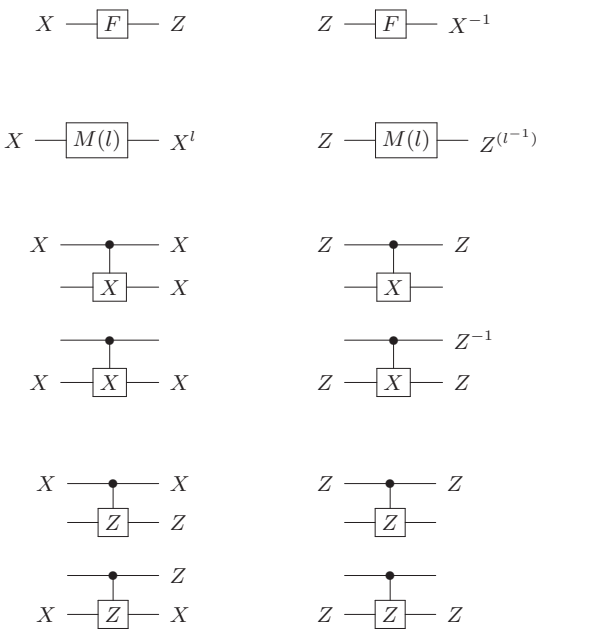

FIG. 2. Propagation rules of generalized Pauli errors for the F, $M(l)$, CX, and CZ gate. Across the F gate, X propagates into Z, and Z into X^{-1}. Across two-qudit gates, some single-qudit errors propagate into two-qudit errors; e.g., $X \otimes \mathbb{1}$ propagates into $X \otimes Z$ across the CZ gate.

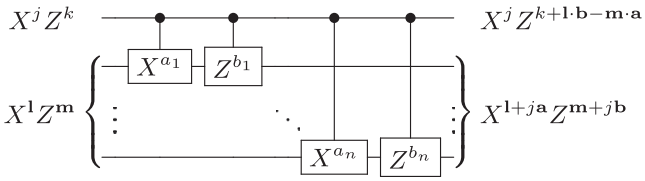

FIG. 3. Across a sequence of CX^{a_i} and CZ^{b_i} gates, the error $X^jZ^k \otimes X^{\mathbf{l}}Z^{\mathbf{m}}$ propagates into $X^jZ^{k+\mathbf{l}\cdot\mathbf{b}-\mathbf{m}\cdot\mathbf{a}} \otimes X^{\mathbf{l}+j\mathbf{a}}Z^{\mathbf{m}+j\mathbf{b}}$. This defines the automorphism $\pi_{C(\mathbf{a},\mathbf{b})}$ in Eq. (17):

In other words, the entries of the error probability tensor are permuted.

Now, we state explicit updating rules for the Clifford gates introduced in Sec. II: For every generalized Pauli gate $A = X^{\mathbf{r}}Z^{\mathbf{s}}$, the automorphism π_A is the identity since Pauli operators commute up to a phase; recall Eq. (5). For other Clifford gates, π_U might be nontrivial. For example, for the Fourier gate $\pi_F(r,s) = (s,-r)$, and for the multiplication-with-l gate $\pi_{M(l)}(r,s) = (l^{-1}r, ls)$. Denoting by $C(\mathbf{a},\mathbf{b})$ the sequence of CX^{a_i} and CZ^{b_i} gates (cf. Fig. 3), we find

$$\begin{aligned}&\pi_{C(\mathbf{a},\mathbf{b})}((j,\mathbf{l}),(k,\mathbf{m}))\\ &\quad= ((j,\ \mathbf{l}-j\mathbf{a}),(k-\mathbf{l}\cdot\mathbf{b}+\mathbf{m}\cdot\mathbf{a},\ \mathbf{m}-j\mathbf{b})),\end{aligned} \tag{17}$$

where $j\mathbf{a} = (ja_1,\ldots,ja_n)$ is scalar multiplication in the module $(\mathbb{Z}/D\mathbb{Z})^n$.

2. Generalized Pauli channels; tensor equations

An n-qudit Pauli error channel $\mathcal{F}$ with coefficients $f_{\mathbf{r},\mathbf{s}}$, as in Eq. (6), causes further errors. This is taken into account by updating the error probability tensor $P = (p_{\mathbf{r},\mathbf{s}})$ to $P' = (p'_{\mathbf{r},\mathbf{s}})$, where $p'_{\mathbf{r},\mathbf{s}}$ are the coefficients of the composed generalized Pauli error channel $\mathcal{E}' = \mathcal{F}\circ\mathcal{E}$,

$$\mathcal{E}'(\rho) = \sum_{\substack{\mathbf{i},\mathbf{j},\mathbf{k},\mathbf{l},\mathbf{r},\mathbf{s}\,\in\,(\mathbb{Z}/D\mathbb{Z})^n\\ \text{such that}\\ \mathbf{i}+\mathbf{k}=\mathbf{r}\text{ and }\mathbf{j}+\mathbf{l}=\mathbf{s}}} f_{\mathbf{i},\mathbf{j}}\, p_{\mathbf{k},\mathbf{l}} (X^{\mathbf{r}}Z^{\mathbf{s}})\rho(X^{\mathbf{r}}Z^{\mathbf{s}})^\dagger. \tag{18}$$

Rewriting the sum and comparing to Eq. (13), the entries of P' are given by

$$\begin{aligned}p'_{\mathbf{r},\mathbf{s}} &= \sum_{\mathbf{k},\mathbf{l}\in(\mathbb{Z}/D\mathbb{Z})^n} f_{\mathbf{r}-\mathbf{k},\mathbf{s}-\mathbf{l}}\, p_{\mathbf{k},\mathbf{l}}\\ &= \sum_{\mathbf{k},\mathbf{l}\in(\mathbb{Z}/D\mathbb{Z})^n} F_{\mathbf{r}\ \mathbf{s}}^{\ \mathbf{k}\ \mathbf{l}}\, p_{\mathbf{k},\mathbf{l}},\end{aligned} \tag{19}$$

where $(F_{\mathbf{r}\ \mathbf{s}}^{\ \mathbf{k}\ \mathbf{l}})$ is a tensor with $2n$ covariant and $2n$ contravariant indices. Its entries are given by $F_{\mathbf{r}\ \mathbf{s}}^{\ \mathbf{k}\ \mathbf{l}} := f_{\mathbf{r}-\mathbf{k},\mathbf{s}-\mathbf{l}}$. This notation becomes very handy when we deal with several error channels, since we can abbreviate the last expression in Eq. (19) in the spirit of Einstein's sum convention as $F_{\mathbf{r}\ \mathbf{s}}^{\ \mathbf{k}\ \mathbf{l}}\, p_{\mathbf{k},\mathbf{l}}$.

C. Contractions of the error probability tensor

In this section, we describe how contractions of the error probability tensor can be used to collect probabilities that correspond to similar events.

1. Measurements

If a qudit is measured in the computational basis, phase errors on that qudit become irrelevant. Therefore, it is meaningful to add up the probabilities of all errors which only differ by Z errors. For example, suppose qudit n is measured. Then the error probability tensor is truncated to a tensor with $2n-1$ indices with entries

$$p'_{\mathbf{r},\mathbf{s}'} = \sum_{t\in\mathbb{Z}/D\mathbb{Z}} p_{\mathbf{r},(\mathbf{s}',t)}, \tag{20}$$

where $\mathbf{s}' = (s_1, \ldots, s_{n-1})$. After the contraction, the index r_n is related to Ditflip errors on the measurement result; i.e., if c was the correct outcome, the actual outcome is $c + r_n$ with conditional probability $p_{\mathbf{r},\mathbf{s}'}$ (conditioned on the presence of an $X^{(r_1,\ldots,r_{n-1})}Z^{\mathbf{s}'}$ error on the unmeasured qudits). This approach can be easily extended to the measurement of multiple qudits. A measurement in the eigenbasis of a different Pauli operator can be substituted by an appropriate Clifford gate followed by a measurement in the computational basis.

2. Discarding qudits

If, at some point in the analysis, one wants to keep track of errors on only $n' < n$ qudits (e.g., after discarding ancillas), one can trace out the error statistics of the $n - n'$ unnecessary qudits. Assume without loss of generality that qudits $n'+1$ to n are discarded. The error statistics of the remaining qudits, stored in an error probability tensor $P' = (p'_{\mathbf{r}',\mathbf{s}'})$ with $2n'$ indices, are given by

$$p'_{\mathbf{r}',\mathbf{s}'} = \sum_{r_{n'+1},\ldots,r_n,s_{n'+1},\ldots,s_n\in\mathbb{Z}/D\mathbb{Z}} p_{\mathbf{r},\mathbf{s}}, \tag{21}$$

where $\mathbf{r} = (r_1, \ldots, r_n)$ is truncated to $\mathbf{r}' = (r_1, \ldots, r_{n'})$, and likewise for $\mathbf{s}$ and $\mathbf{s}'$.

3. Adding up probabilities of equivalent errors

So far, we have shown how the error probability tensor describes the performance of a studied quantum circuit, independent of its input state. If, however, one is interested in the error statistics of a particular stabilizer state, it is reasonable to consider equivalence classes of errors: The stabilizer group of an n-qudit state $|\psi\rangle$ is generated by n independent Pauli operators $S_i \propto X^{\mathbf{a}_i}Z^{\mathbf{b}_i}$ with $\mathbf{a}_i, \mathbf{b}_i \in (\mathbb{Z}/D\mathbb{Z})^n$. The exponents of all stabilizer operators form a submodule

$$W := \mathrm{span}_{\mathbb{Z}/D\mathbb{Z}}\{(\mathbf{a}_i, \mathbf{b}_i) |\ i \in \{1, \ldots, n\}\} \tag{22}$$

of $V := (\mathbb{Z}/D\mathbb{Z})^n \times (\mathbb{Z}/D\mathbb{Z})^n$. By definition, $X^{\mathbf{a}}Z^{\mathbf{b}}|\psi\rangle \propto |\psi\rangle$ holds for every $(\mathbf{a}, \mathbf{b}) \in W$. Likewise, for a given coset

$$\mathrm{co}(\mathbf{r}, \mathbf{s}) := \{(\mathbf{r} + \mathbf{a}, \mathbf{s} + \mathbf{b}) |\ (\mathbf{a}, \mathbf{b}) \in W\}; \tag{23}$$

i.e., for an element in the quotient module V/W, every pair of representatives $(\mathbf{j}, \mathbf{k})$, $(\mathbf{j}', \mathbf{k}') \in \mathrm{co}(\mathbf{r}, \mathbf{s})$ satisfies

$$X^{\mathbf{j}}Z^{\mathbf{k}}|\psi\rangle \propto X^{\mathbf{j}'}Z^{\mathbf{k}'}|\psi\rangle, \tag{24}$$

since $X^{\mathbf{j}}Z^{\mathbf{k}}$ and $X^{\mathbf{j}'}Z^{\mathbf{k}'}$ are the same up to a stabilizer of $|\psi\rangle$ (and a global phase). It is not meaningful to distinguish between such errors as they lead to the same erroneous state. Hence, the error probability tensor $P = (p_{\mathbf{r},\mathbf{s}})$, as given in Eq. (14), can be reduced to a tensor $\bar{P} = (p_{\mathrm{co}(\mathbf{r},\mathbf{s})})$ with D^n entries

$$p_{\mathrm{co}(\mathbf{r},\mathbf{s})} = \sum_{(\mathbf{j},\mathbf{k})\in\mathrm{co}(\mathbf{r},\mathbf{s})} p_{\mathbf{j},\mathbf{k}}. \tag{25}$$

We use cosets as indices because each of them corresponds to a whole class of errors with the same effect.

Consider, for example, the maximally entangled state

$$|\Psi\rangle := \frac{1}{D}\sum_{j,k\in\mathbb{Z}/D\mathbb{Z}} \omega^{jk}|j\rangle\otimes|k\rangle, \tag{26}$$

where again $\omega = \mathrm{e}^{2\pi i/D}$. The stabilizers of $|\Psi\rangle$ are $S_1 = X\otimes Z = X^{(1,0)}Z^{(0,1)}$ and $S_2 = Z\otimes X = X^{(0,1)}Z^{(1,0)}$. Hence, the submodule W in Eq. (22) is spanned by $(\mathbf{a}_1, \mathbf{b}_1) = ((1,0),(0,1))$ and $(\mathbf{a}_2, \mathbf{b}_2) = ((0,1),(1,0))$, i.e., $W = \{((\lambda,\mu),(\mu,\lambda)) \mid \lambda, \mu \in \mathbb{Z}/D\mathbb{Z}\}$. The elements in V/W can be expressed as $\mathrm{co}((0,r),(0,s)) = \{((\lambda,\mu+r),(\mu,\lambda+s)) \mid \lambda,\mu\in\mathbb{Z}/D\mathbb{Z}\}$, where $r, s \in \mathbb{Z}/D\mathbb{Z}$. The probability for an X^rZ^s error on the second qudit—or equivalently an $X^{-s}Z^{-r}$ error on the first qudit—is given by

$$p_{\mathrm{co}((0,r),(0,s))} = \sum_{\lambda,\mu\in\mathbb{Z}/D\mathbb{Z}} p_{(\lambda,\mu+r),(\mu,\lambda+s)}. \tag{27}$$

It is also possible to update the error probability tensor in its truncated form, where the stabilizers—and hence W and V/W—have to be updated after every Clifford gate. This approach is recommended for numerical treatments as it gives an advantage in execution time and memory. For analyses carried out by hand, however, we recommend to first compute P for the whole circuit and to truncate to $\bar{P}$ afterward, since calculating with quotient modules and cosets can be cumbersome.

IV. APPLICATION: QUDIT REPEATER LINE

The purpose of quantum repeater networks is the distribution of entangled states among remote users. The approaches to overcome the presence of noise in quantum repeaters are categorized into three so-called generations [7]. Third-generation quantum repeaters have, compared to generation 1 and 2, the advantage of fast one-way communication [29,30]. There, qudits are encoded with a QECC which is used to correct loss and operational errors at the repeater stations. An $[\![n, k, d]\!]_D$ QECC is optimal if it saturates the quantum singleton bound $2d - 2 + k \leqslant n$ [24]. Prominent examples of such codes are $[\![2d-1, 1, d]\!]_D$ quantum polynomial codes [25–28], where D is a prime and $d \leqslant (D-1)/2$ is arbitrary. These are specified in Appendix A.

Using the error probability tensor, we carry out an error analysis of third-generation quantum repeaters; cf. Appendixes C–E. This is a generalization of the error analysis of qubit repeaters, performed in Refs. [15,16], to the bipartite qudit case, which is a building block in qudit repeater networks [22]. In contrast to previous work [15,16,31–34], we do not compute secret key rates and certain cost functions. Instead, we focus on deriving the full error statistics of the distributed state ρ and thus ρ itself. Similar results are known for the qubit repetition code [35].

In Sec. IV A, the ideal qudit repeater protocol is explained. In Sec. IV B, we present an exact analytical solution of the error statistics of ρ in terms of the qudit dimension D, the number of repeater stations N, and various error rates, f_{T} (transmission), f_{G} (CZ gate), f_{M} (measurement), and f_{S} (storage). The distance L_0 between the repeater stations is only implicitly built in via the transmission error rate f_{T}. For example, optical fiber at telecommunication wavelengths has a channel loss of 0.2 dB/km [36]. In Sec. IV C, we discuss a quality-quantity trade-off of distributed states. Finally, in Sec. IV D, we compare the performance of $[\![2d-1,1,d]\!]_D$ QECCs for variable code distance d and physical qudit dimension D.

A. The ideal qudit repeater line protocol

Consider two parties, Alice and Bob, both holding a single qudit. They want to create the maximally entangled state $|\Psi\rangle$ defined in Eq. (26). To achieve this, Alice and Bob perform entanglement swapping via a one-way qudit repeater line. The protocol is as follows [21–23]: Alice prepares two qudits (labeled A and 1), each of them in the state $|+\rangle := \frac{1}{\sqrt{D}}\sum_{j\in\mathbb{Z}/D\mathbb{Z}}|j\rangle$. She then applies a CZ gate between these qudits, which yields the state $|\Psi\rangle$ of Eq. (26). Afterward, she stores her qudit A and sends qudit 1 to repeater station 1. There, another qudit (labeled 2) is prepared in the $|+\rangle$ state. When qudit 1 arrives, a CZ gate is applied between qudits 1 and 2. Qudit 1 is then destructively measured in the X basis. The measurement result is a classical digit $c_1 \in \mathbb{Z}/D\mathbb{Z}$. Meanwhile, qudit 2 is sent to the second repeater station, where the same steps as at station 1 are performed. Finally, after $N-1$ repeater stations, Bob receives qudit N, applies a CZ gate to qudit N and his own qudit (labeled B) and measures qudit N in the X basis. These steps are depicted in Fig. 4.

Alice and Bob now share a maximally entangled state whose exact form depends on all measurement outcomes $c_i \in \mathbb{Z}/D\mathbb{Z}$. Using the main-stabilizer approach of Ref. [22], one can show that it is the common $+1$ eigenstate of $\omega^{c_A}X_A \otimes Z_B$ and $\omega^{c_B}Z_A \otimes X_B$, where

$$c_{\mathrm{A}} := \sum_{i=1}^{N/2}(-1)^i c_{2i} \quad \text{and} \quad c_{\mathrm{B}} := \sum_{i=1}^{N/2}(-1)^i c_{N+1-2i}, \tag{28}$$

and we assume that N is even for simplicity. All classical digits c_i are sent to Bob. He postprocesses them into c_{A} and

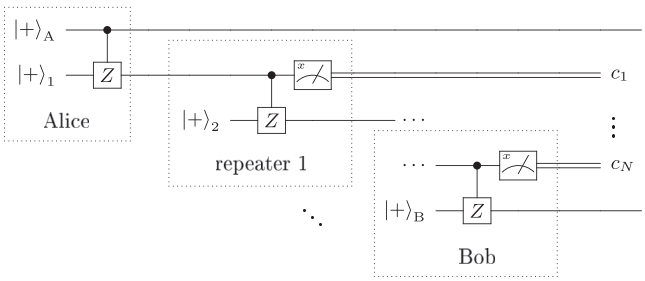

FIG. 4. A quantum circuit diagram representation of the qudit repeater line between Alice and Bob. Intermediate repeater stations are introduced to shorten the transmission distance of the qudits. All outcomes c_i of the X measurement at repeater i are transmitted to Bob (who counts as repeater N) for the Pauli-frame recovery of $|\Psi\rangle$.

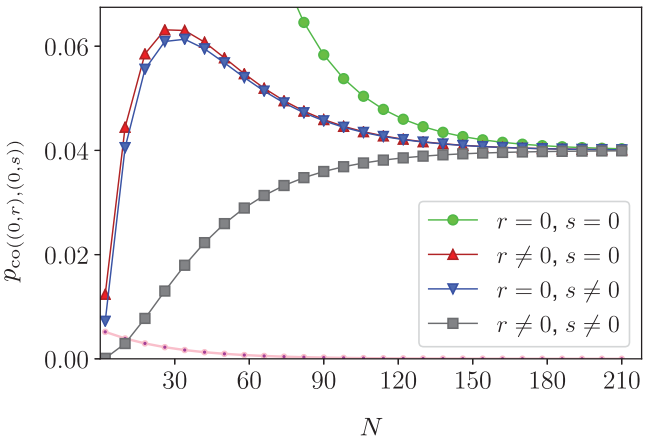

FIG. 5. Error statistics, Eq. (29), of a state distributed with a ququint repeater line encoded with the $[\![5,1,3]\!]_5$ quantum polynomial code. The entries of the (reduced) error probability tensor are plotted as functions of the number of repeater stations, N, where transmission, measurement, gate, and storage error rates are set to $f_{\mathrm{T}} = 0.05$, $f_{\mathrm{M}} = 0.01$, $f_{\mathrm{G}} = 0.001$, and $f_{\mathrm{S}} = 0.0001$, respectively. There are 1 green (circles; no errors), 4 red (triangles up; X_{B}^r error), 4 blue (triangles down; Z_{B}^s error), and 16 gray identical curves (squares; $X_{\mathrm{B}}^r Z_{\mathrm{B}}^s$ error). The pink curve (dots) shows the difference between red and blue curves.

c_{B} and applies the Pauli gate $X^{c_{\mathrm{A}}}Z^{-c_{\mathrm{B}}}$ to his qudit B. Taking Eq. (5) into account, this so-called Pauli-frame recovery produces the desired state $|\Psi\rangle$, as it is the unique two-qudit $+1$ eigenstate of $X_{\mathrm{A}} \otimes Z_{\mathrm{B}}$ and $Z_{\mathrm{A}} \otimes X_{\mathrm{B}}$.

B. Error statistics of noisy qudit repeater lines

We now present analytical results for the error statistics of the third-generation qudit repeater line described in the previous section. These results are valid for all polynomial codes and other $[\![n,1,d]\!]_D$ codes with similar properties. The probability of a logical X^rZ^s error on Bob's qudit B, or equivalently of a logical $X^{-s}Z^{-r}$ error on Alice's qudit A [recall Eq. (27)] is

$$p_{\mathrm{co}((0,r),(0,s))} = f_{0,0}^{\mathrm{local}} f_r^X f_s^Z + f_{\mathrm{err}}^{\mathrm{local}}\left(1 - f_r^X f_s^Z\right), \tag{29}$$

where f^{local} represent errors occurring locally on Alice's or Bob's qudit and f^X and f^Z represent errors propagating from repeater stations to the final state via Pauli-frame recovery. See Appendix C (without QECCs) and Appendix D (with QECCs) for detailed derivations.

The error statistics for a fixed-error-rate[1] ququint repeater line encoded with the $[\![5,1,3]\!]_5$ quantum polynomial code is

[1]A transmission error rate of $f_{\mathrm{T}} = 0.05$ corresponds to a repeater spacing of $L_0 \approx 1$km [36]. The best single-photon detector efficiencies are about 95% [37], so we choose $f_{\mathrm{M}} = 10^{-2}$ to keep the same order of magnitude. Gate error rates are not known for qudit CZ gates. We assume $f_{\mathrm{G}} = 10^{-3}$ because this is the error rate of state-of-the-art single-qudit gates [12], as well as a typical value for two-qubit gates in quantum communication [6,15,16,29,31]. There are no good quantum memories yet. We still include storage errors with an optimistic assumption of $f_{\mathrm{S}} = 10^{-4}$.

plotted as a function of the number of repeater stations in Fig. 5. Note that we choose $D = 5$ because it is the simplest case where a quantum polynomial code with code distance $d = 3$ exists. In total, there are D^2 curves in the figure, as curves of equal color overlap: one green, $D-1$ red, $D-1$ blue, and $(D-1)^2$ gray. The green curve,

$$p_{\mathrm{co}((0,0),(0,0))} = 1 - \sum_{(r,s)\neq(0,0)} p_{\mathrm{co}((0,r),(0,s))}, \tag{30}$$

is uniquely determined by the other curves and is directly related to the Uhlmann fidelity $\sqrt{\langle\Psi|\,\rho\,|\Psi\rangle} = \sqrt{p_{\mathrm{co}((0,0),(0,0))}}$ of the distributed state ρ [38,39]. This curve decreases as a function of N due to the fact that longer repeater lines contain more error sources, thus mixing the state ρ. For $N \approx 200$ repeater stations, $f_{0,0}^{\mathrm{local}}$ and $f_{\mathrm{err}}^{\mathrm{local}}$ converge to $1/D^2$, and f_r^X and f_s^Z converge to $1/D$, forcing all error probabilities to converge to an equilibrated value of $1/D^2 = 0.04$ as seen in Fig. 5. Hence, the distributed state approaches the maximally mixed state. The red and blue curves in the figure are the probabilities of single X^r and Z^s errors, respectively. These Ditflip and phase errors are introduced independently with probabilities f_r^X and f_s^Z, respectively, which are relatively small ($0 < f_{r\neq 0}^X, f_{s\neq 0}^Z \ll 1/D$) for short repeater lines ($N < 20$). As a result, it is more likely that Dit-flip and phase errors occur alone than together. This is why, for short repeater lines, the red and blue curves are much higher than the gray curves (simultaneous $X^r Z^s$ error). The red and blue curves surpass the equilibrium because accumulating X and Z errors have a low chance of canceling each other out. However, they can never surpass $1/D = 0.2$ because the corresponding errors originate in D-outcome measurements at the repeater stations. There is an asymmetry in the probabilities of X and Z errors, as they accumulate differently at the ends of the repeater line. The difference between red and blue, which is plotted in pink, decreases in the repeater line's length, demonstrating the role of the finite-size of the repeater line. Note that, for qubits, the red and blue curves would not show a local maximum in N since two X and Z errors, respectively, always cancel.

C. Tradeoff: Fidelity vs distribution probability

In practice, each qudit is encoded into the state of a photon, e.g., into its temporal or orbital-angular-momentum degrees of freedom [12]. During its transmission from one repeater station to the next, the photon is absorbed with probability

$$f_{\mathrm{abs}} = 1 - (1 - f_{\mathrm{C}})\mathrm{e}^{-\gamma}, \tag{31}$$

where f_{C} represents coupling losses, and the damping parameter $\gamma := L_0/L_{\mathrm{att}}$ is the ratio of the repeater spacing L_0 to the attenuation length $L_{\mathrm{att}} \approx 20\,\mathrm{km}$ of the fiber through which the photon is transmitted [15,16]. An error, which is caused by the absorption of the photon, is noticed by a nonclick event at its measurement. On the other hand, f_{T} represents unnoticed transmission errors. In the previous section, all errors were assumed to be undetected.

Similar to Refs. [15,16], we consider a variation of the protocol. A measurement outcome is marked as "?" if an absorption of the corresponding photon is noticed. Such a lost qudit can be thought of as being in the completely mixed state, which is equivalent to $X^r Z^s$ errors, each with probability $1/D^2$. Hence, Z^r errors are induced on the next qudit through the CZ gate (recall Fig. 2), so the measurement of the next qudit has an error with probability $(D-1)/D$. As this is a high probability, we preventively also mark that measurement outcome as "?". The adapted strategy is to abort and restart the protocol if more than a fixed number $k_{\max}$ of measurement outcomes at a given repeater station have been marked as "?". If, however, only $k \leqslant k_{\max}$ outcomes are marked as "?", they are discarded and the $n-k$ remaining outcomes form a classical error-correcting code with a Hamming distance of at least $d-k$. The logical measurement outcome is obtained by decoding the remaining physical outcomes according to this code.

As an example, we present this scheme for a $[\![13, 1, 7]\!]_{13}$ QECC. The top plot in Fig. 6 shows the behavior of the fidelity $F(k_{\max}) := \sqrt{\langle\Psi|\,\rho(k_{\max})\,|\Psi\rangle}$ of the distributed state $\rho(k_{\max})$ in terms of unnoticed and noticed transmission errors for various choices of $k_{\max}$. The bottom plot of Fig. 6 shows the corresponding probability $P_{k_{\max}}^{\mathrm{distr}}$ of the protocol not being aborted; cf. Eq. (E5) in Appendix E. Because of the brute force approach, we can only solve $P_{k_{\max}}^{\mathrm{distr}}$ for a repeater line with $N = 2$ repeater stations (including Bob); see Appendix E for more details.

In the following, we set $f := f_{\mathrm{T}} = f_{\mathrm{abs}}$. First, consider the top plot of Fig. 6. At $f = 0$, the fidelity of the distributed state is $F(k_{\max}) = 1 - 10^{-5}$, which is almost optimal. (For comparison, an unencoded repeater line yields a fidelity of 0.987.) Note that this is independent of $k_{\max}$ since no photons are lost. The fidelities decrease in f because of additional transmission errors. For $f > 0$, they are arranged as

$$F(0) > F(1) \approx F(2) > F(3) \approx F(4). \tag{32}$$

The difference between $F(0)$ and $F(1)$ is already significant for $f \approx 0.05$ because, in the case of an absorbed photon, a reduced $[12, 1, 6]_{13}$ code which can only correct up to two errors is used for $k_{\max} = 1$, while for $k_{\max} = 0$ the protocol is aborted if the original distance-7 code cannot be used. Note that $F(1)$ and $F(2)$ are approximately the same because the $[11, 1, 5]_{13}$ code, which is additionally employed for $k_{\max} = 2$, can correct as many errors as the $[12, 1, 6]_{13}$ code. A similar argument holds for $F(3) \approx F(4)$. In the limit $f \to 1$, all fidelities approach the worst-case value $F(k_{\max}) = 1/13 \approx 0.077$.

Now consider the bottom plot in Fig. 6. Note that the distribution probability does not depend on f_{T}. At $f = 0$, the probability of distributing a state is $P_{k_{\max}}^{\mathrm{distr}} = 1$ because no qudits are lost and the protocol never aborts. In total, $Nn = 26$ photons are transmitted. For $k_{\max} = 0$, the protocol is aborted if at least one photon is absorbed. This happens with probability $P_0^{\mathrm{distr}} = (1-f)^{26}$. This explains the rapid drop of the blue (solid) curve, P_0^{distr}. For higher $k_{\max}$, $P_{k_{\max}}^{\mathrm{distr}}$ decreases more slowly in f [cf. Eq. (E5)] as more photon losses are tolerated.[2] Thus, the distribution probabilities are

[2]For example, for $k_{\max} = 1$, the probability of distributing a state is $P_1^{\mathrm{distr}} = (1-f)^{26} + 26f(1-f)^{25} + 13f^2(1-f)^{24}$, where $26f(1-f)^{25}$ accounts for the 26 events where exactly one photon is lost. Similarly, the term $13f^2(1-f)^{24}$ accounts for 13 combinations of 2 lost photons which do not lead to an abortion.

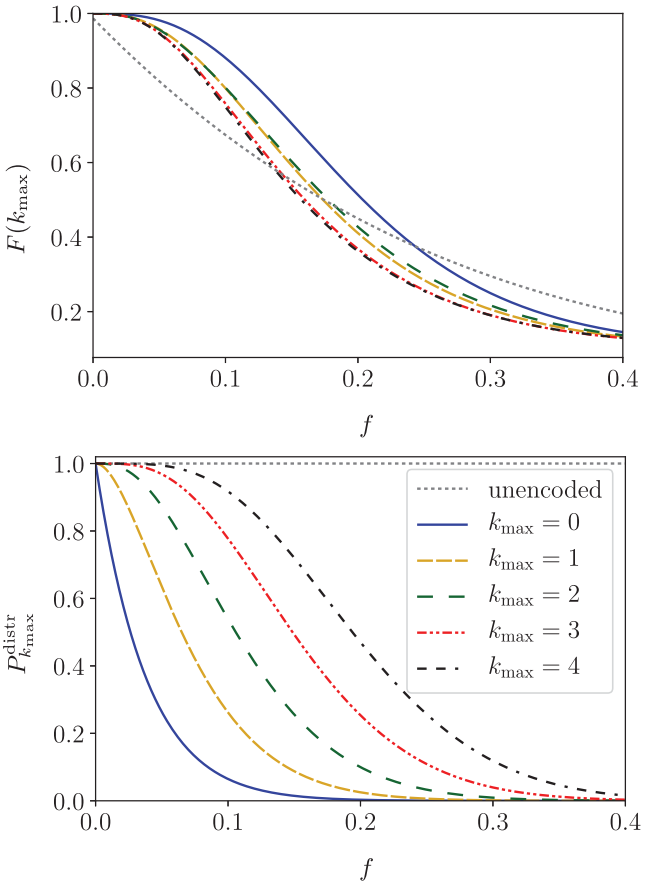

FIG. 6. The fidelity, $F(k_{\max})$, of the distributed state (top), and the probability of successfully distributing the state (bottom) as a function of unnoticed (f_{T}) and noticed (f_{abs}) transmission error rates $f := f_{\text{T}} = f_{\text{abs}}$ for different abortion strategies. The repeater line has $N = 2$ stations, and measurement, gate, and storage error rates are set to $f_{\text{M}} = 0.01$, $f_{\text{G}} = 0.001$, and $f_{\text{S}} = 0.0001$, respectively. The gray (dotted) curve shows the performance of an unencoded qudit with $D = 13$. The other curves show the performance of the $[\![13, 1, 7]\!]_{13}$ quantum polynomial code for different abortion conditions $k_{\max}$. If at any of the repeater stations the number of qudits marked as "?" is greater than $k_{\max}$, the protocol is aborted.

ordered as

$$P_0^{\text{distr}} < P_1^{\text{distr}} < P_2^{\text{distr}} < P_3^{\text{distr}} < P_4^{\text{distr}}. \tag{33}$$

Equations (33) and (32) show the tradeoff between the quantity and the quality of distributed states. Naturally, one should not choose $k_{\max}$ to be odd (if d is odd), since the fidelity is approximately that of $k_{\max} + 1$ but the corresponding distribution probability is significantly lower.

D. Optimizing the distributed entanglement

Consider the following scenario: Alice and Bob want to create an entangled state by using a qudit repeater line a single time. The qudit can be encoded into an arbitrary $[\![2d - 1, 1, d]\!]_D$ QECC with a fixed physical Hilbert space dimension $\dim(\mathcal{H}) = D^{2d-1}$. (For example, if $\dim(\mathcal{H}) = 27$, Alice and Bob can choose between $[\![1, 1, 1]\!]_{27}$ and $[\![3, 1, 2]\!]_3$

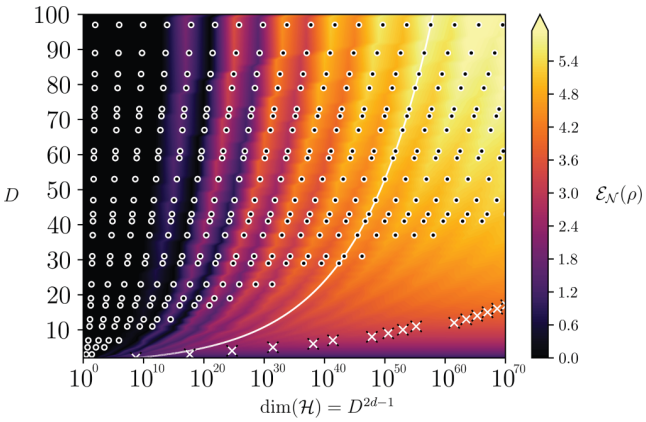

FIG. 7. The logarithmic negativity $\mathcal{E}_{\mathcal{N}}(\rho)$ of the state ρ distributed via a repeater line with $N = 50$ stations and encoded with a $[\![2d - 1, 1, d]\!]_D$ code for varying qudit dimension D and code distance d. The ambient Hilbert space of a logical qudit is $\mathcal{H}$; i.e., if for example $D = 100$ and $\dim \mathcal{H} = 10^{70}$, one logical qudit is encoded into 35 physical qudits. The transmission, measurement, gate, and storage error rates are set to $f_{\text{T}} = 0.05$, $f_{\text{M}} = 0.01$, $f_{\text{G}} = 0.001$, and $f_{\text{S}} = 0.0001$, respectively. The dots represent parameters for which quantum polynomial codes exist, namely $1 \leqslant d \leqslant (D + 1)/2$ for every fixed prime D. The crosses represent the codes listed in Table I. The white curve exemplary shows codes with constant code distance $d = 15$.

encoding.) They adjust the parameters D and d in order to maximize the logarithmic negativity

$$\mathcal{E}_{\mathcal{N}}(\rho) = \log_2(||\rho^{\text{T}_{\text{A}}}||_1), \tag{34}$$

where $\rho^{\text{T}_{\text{A}}}$ is the partial transpose of ρ with respect to Alice, and $||\cdot||_1$ is the trace norm [40]. The logarithmic negativity is an entanglement measure and thus a quantifier of distributed resources.

In Fig. 7, we show the logarithmic negativity $\mathcal{E}_{\mathcal{N}}(\rho)$ for all $[\![2d - 1, 1, d]\!]_D$ codes with $2 \leqslant D \leqslant 100$ and $D^{2d-1} \leqslant 10^{70}$, the latter of which is the physical Hilbert space dimension of the system into which one logical qudit is encoded; i.e., $\mathcal{H}$ is the ambient Hilbert space of a logical qudit. The state ρ is distributed by a qudit repeater line with $N = 50$ repeater stations (including Bob), where we assume that the error rates are independent of D.[3] We observe characteristic features in three different regions: (i) For small code distances d, the repeater line distributes no entanglement; i.e., $\mathcal{E}_{\mathcal{N}}(\rho) = 0$. (ii) For small dimension D and large code distances d, the logarithmic negativity is approximately optimal; i.e., $\mathcal{E}_{\mathcal{N}}(\rho) \approx \log_2(D)$. This is the region below the crosses in Fig. 7. (iii) In between, $0 \leqslant \mathcal{E}_{\mathcal{N}}(\rho) \leqslant \log_2(D)$ holds. For a fixed dimension D, the logarithmic negativity takes on values in an alternating fashion, governed by an overall trend to its maximum value,

[3]For storage, gate, and measurement errors, this assumption is probably not justified. However, experiments with time-bin qudits suggest that the transmission errors, which are the main error source, do not depend on D [13]. For orbital angular momentum qudits, on the other hand, transmission errors increase with D [41].

TABLE I. Parameter of the smallest $[\![2d_{\min}-1, 1, d_{\min}]\!]_D$ codes for which in Fig. 7 $\mathcal{E}_{\mathcal{N}}(\rho) > 0.99 \times \log_2(D)$ holds.

D	2	3	4	5	6,7	8, ..., 11	12, ..., 23
$d_{\min}$	15	19	21	23	25	27	29

with increasing code distance d. We will comment on these three regions in the following:

In region (i), for $d \in \{1, 2, 3, 4, 6\}$, too few errors can be corrected by the QECCs. Hence, the final state distributed to Alice and Bob lost any logarithmic negativity. Thus, it cannot even be used for entanglement distillation [40]. The first nonzero logarithmic negativity arises for $d = 5$, which shows that, for example, $[\![9, 1, 5]\!]_D$ codes perform sufficiently well in the considered parameter region to distribute states that are entangled to some degree. For $d = 6$, $[\![10, 1, 6]\!]_D$ codes are used, which correct as many errors as the $[\![9, 1, 5]\!]_D$ codes but rely on an additional physical qudit which also accumulates errors. Overall, these perform worse, explaining the respective vanishing of the logarithmic negativity.

In region (ii), note that for a fixed dimension D and sufficiently large distances $d \geqslant d_{\min}$, the distributed state ρ is almost pure. Under these conditions, the logarithmic negativity is approximately that of a pure maximally entangled state $|\Psi\rangle\langle\Psi|$, i.e., $\mathcal{E}_{\mathcal{N}}(\rho) \approx \log_2(D)$. In Table I, we show the values of $d_{\min}$ such that $\mathcal{E}_{\mathcal{N}}(\rho)$ is above $0.99 \times \log_2(D)$ for various dimensions D.

Finally, in region (iii), recall that codes with an odd code distance are beneficial for error correction. This argument explains the alternating values of $\mathcal{E}_{\mathcal{N}}(\rho)$ for fixed dimension D. The overall trend to higher values of the logarithmic negativity is simply explained by the fact that the corresponding QECCs can correct more errors with increasing code distance.

Overall, $\mathcal{E}_{\mathcal{N}}(\rho)$ increases in the qudit dimension D and the code distance d. Fixing either d or D and varying the other is not a fair comparison because the requirements to Alice and Bob also change, for example, the number of physical qudits $n = 2d - 1$ (for fixed D). A better comparison is obtained if $\dim(\mathcal{H}) = D^n$ (x axis in Fig. 7) is fixed instead. This would be relevant if, for example a single ququad ($D = 4, n = 1$) is as expensive as two entangled qubits ($D = 2, n = 2$). Figure 7 shows that the optimal strategy depends on the chosen value of $\dim(\mathcal{H})$. If it is small, e.g., 10^{10}, Alice and Bob should not increase D too much. If it is large, e.g., 10^{70}, the logarithmic negativity is optimized for large D. Even above the crosses, where distributed states are not maximally entangled (for the corresponding D), $\mathcal{E}_{\mathcal{N}}(\rho)$ still increases in D. For experimental implementations, this is good because more quantum polynomial codes exist for larger D, while no QECCs are known in the region where $\mathcal{E}_{\mathcal{N}}(\rho) \approx \log_2(D)$.

V. CONCLUSION AND OUTLOOK

The error probability tensor framework developed here is a useful tool for analyzing the propagation of generalized Pauli errors in quantum circuits composed of qudit Clifford gates. It enabled us to analytically derive the full error statistics of a state distributed via a qudit repeater line with arbitrary qudit dimension and arbitrarily many repeater stations. Our analysis demonstrates the advantage of quantum repeaters with quantum error correction, as well as the tradeoff between quality and preparation rate of distributed quantum states. For a fixed number of provided degrees of freedom our analysis suggests that higher dimensional qudits can increase the amount of distributed entanglement. In particular, we find that the amount of entanglement does increase in the qudit dimension only if sufficiently many errors can be corrected. Fortunately, in the superior parameter region, explicit quantum error-correcting codes are feasible in the form of quantum polynomial codes.

Experimentally, photonic qudits with physical qudit dimension up to the order of 10^5 can be realized [13]. Missing key ingredients for the realization of the here-discussed qudit repeaters are a procedure to encode logical states into a multiphoton system, as well as a way to physically implement the two-qudit controlled-phase gate between two physical photonic qudits. Gates between time-bin-encoded qudits are especially desirable, as time-bin qudits are less prone to errors than, for example, orbital angular momentum qudits.

In future work, we want to investigate the parameter regimes in which a bipartite qudit repeater can beat the PLOB repeaterless bound [42]. Furthermore, we aim to generalize our error analysis to multipartite qudit repeater networks. To conclude, we claim that the error probability tensor can be applied for analytical analyses of other quantum communication protocols, as they often only require Clifford gates.

ACKNOWLEDGMENTS

The authors thank Michael Epping and Liang Jiang for helpful discussions and Eric Sabo for feedback on the manuscript. The circuit diagrams were typeset using the package `Qcircuit.tex` [43]. The authors acknowledge support from the Federal Ministry of Education and Research (BMBF).

APPENDIX A: QUANTUM POLYNOMIAL CODES

An important class of higher dimensional stabilizer QECCs are polynomial codes [25–28]. They are examples of nonbinary CSS codes whose explicit construction is given in Ref. [27]. Quantum polynomial codes have already proven to be useful in the context of qudit quantum repeaters [33]. Among codes with other parameters (e.g., codes which encode more than one logical qudit), there is a $[\![2d-1, 1, d]\!]_D$ quantum polynomial code for every prime number D and every number $d \leqslant (D+1)/2$. Here, we outline a specific subfamily of these QECCs.

Let $D \geqslant 3$ be an odd prime and let $d := (D+1)/2$. Consider the $(d-1) \times D$ parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & 3 & \cdots & D-1 \\ 0 & 1 & 2^2 & 3^2 & \cdots & (D-1)^2 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 2^{d-2} & 3^{d-2} & \cdots & (D-1)^{d-2} \end{pmatrix} \tag{A1}$$

with entries $h_{j,k} := k^j \in \mathbb{F}_D$, where $0^0 := 1$. The vectors $\mathbf{h}_j := (k^j)_{0 \leqslant k \leqslant D-1} \in (\mathbb{F}_D)^D$ (rows of H) are mutually

orthogonal, each of them is orthogonal to $\mathbf{i} := (k^{d-1})_{0\leqslant k\leqslant D-1}$, and $\mathbf{i}\cdot\mathbf{i} = -1$ [44]. Therefore, the operators $S_j^X := X^{\mathbf{h}_j}$ and $S_j^Z := Z^{\mathbf{h}_j}$ mutually commute, each of the S_j^X and S_j^Z commutes with $X_\mathrm{L} := X^{\mathbf{i}}$ and $Z_\mathrm{L} := Z^{-\mathbf{i}}$, and $X_\mathrm{L}Z_\mathrm{L} = \omega^{-1}Z_\mathrm{L}X_\mathrm{L}$ is fulfilled. It follows that $\mathcal{S} := \langle S_j^X, S_j^Z \mid j \in \{0,\ldots,d-2\}\rangle$ is an Abelian subgroup of the qudit Pauli group on D qudits. Therefore, $\mathcal{S}$ defines a QECC [19,20] which encodes $D-2(d-1)=1$ logical qudit with logical operators X_L and Z_L. For each $a\in\mathbb{F}_D$, the logical code space has a basis state

$$|a_\mathrm{L}\rangle := \frac{1}{\sqrt{D^{d-1}}} \sum_{\substack{\lambda_0,\ldots,\lambda_{d-2}\in\mathbb{F}_D \\ \lambda_{d-1}=a}} |f_\lambda(0),\ldots,f_\lambda(D-1)\rangle\,, \tag{A2}$$

where for every vector $\boldsymbol{\lambda} := (\lambda_0,\ldots,\lambda_{d-1}) \in (\mathbb{F}_D)^d$ a corresponding polynomial is defined as $f_\lambda(T) := \lambda_0 + \lambda_1 T + \cdots + \lambda_{d-1}T^{d-1}$.

The reason this constitutes a good QECC is the redundancy inherent in this construction: Since the polynomial f_λ is defined via its coefficients λ_i, one can reveal f_λ if d evaluation values are known. Let $k_0,\ldots,k_{d-1}\in\mathbb{F}_D$ be mutually distinct and define the $d\times d$ Vandermonde matrix $V := (k_i^j)_{0\leqslant i,j\leqslant d-1}$ whose inverse is derived in Ref. [45]. This reveals $\boldsymbol{\lambda} = V^{-1}(f_\lambda(k_i))_{0\leqslant i\leqslant d-1}$. That is, the system of linear equations

$$\left.\begin{aligned} f_\lambda(0) &= \lambda_0 \\ f_\lambda(1) &= \lambda_0+\lambda_1+\cdots+\lambda_{d-1} \\ &\vdots \\ f_\lambda(D-1) &= \lambda_0+\cdots+(D-1)^{d-1}\lambda_{d-1} \end{aligned}\right\} \tag{A3}$$

can be solved from only d of its $D=2d-1$ equations. Based on the construction, one can see that quantum polynomial codes can correct up to 50% erasure errors, which is the bound set by the no-cloning theorem. Note that for these QECCs the CZ gate is transversal in the sense that applying CZ^{-1} to each pair of physical qudits within two logical qudits constitutes a logical CZ gate [26].

APPENDIX B: DISCRETIZATION OF THE DEPOLARIZING CHANNEL

Here, we show that for each normalized n-qudit state ρ the relation

$$\frac{\mathbb{1}}{D^n} = \frac{1}{D^{2n}} \sum_{\mathbf{r},\mathbf{s}\in(\mathbb{Z}/D\mathbb{Z})^n} (X^\mathbf{r}Z^\mathbf{s})\,\rho\,(X^\mathbf{r}Z^\mathbf{s})^\dagger \tag{B1}$$

holds. This states that the depolarizing channel corresponds to some probability for discrete X and Z errors on the qudits—an observation mentioned in Ref. [22].

To prove this, we expand the state ρ in the computational basis,

$$\rho = \sum_{\mathbf{j},\mathbf{k}\in(\mathbb{Z}/D\mathbb{Z})^n} z_{\mathbf{j},\mathbf{k}}\,|\mathbf{j}\rangle\langle\mathbf{k}|\,, \tag{B2}$$

and insert this expression and the expansion for Pauli operators, Eq. (4), into the right-hand side of Eq. (B1). By orthonormality, we find

$$\begin{aligned} &\sum_{\mathbf{r},\mathbf{s}\in(\mathbb{Z}/D\mathbb{Z})^n} (X^\mathbf{r}Z^\mathbf{s})\,\rho\,(X^\mathbf{r}Z^\mathbf{s})^\dagger \\ &\quad= \sum_{\mathbf{r},\mathbf{s},\mathbf{j},\mathbf{k}\in(\mathbb{Z}/D\mathbb{Z})^n} z_{\mathbf{j},\mathbf{k}}\,\omega^{(\mathbf{j}-\mathbf{k})\cdot\mathbf{s}}\,|\mathbf{j}+\mathbf{r}\rangle\langle\mathbf{k}+\mathbf{r}|\,. \end{aligned} \tag{B3}$$

Using the fact that complex roots sum up to zero, $\sum_{s\in(\mathbb{Z}/D\mathbb{Z})^n}\omega^{(\mathbf{l}-\mathbf{m})\mathbf{s}} = D^n\delta_{\mathbf{l},\mathbf{m}}$ and $\mathrm{Tr}(\rho)=1$, the entries of the operator in Eq. (B3) are given by

$$\begin{aligned} &\langle\mathbf{l}|\left(\sum_{\mathbf{r},\mathbf{s},\mathbf{j},\mathbf{k}\in(\mathbb{Z}/D\mathbb{Z})^n} z_{\mathbf{j},\mathbf{k}}\,\omega^{(\mathbf{j}-\mathbf{k})\cdot\mathbf{s}}\,|\mathbf{j}+\mathbf{r}\rangle\langle\mathbf{k}+\mathbf{r}|\right)|\mathbf{m}\rangle \\ &\quad= \sum_{\mathbf{r},\mathbf{s}\in(\mathbb{Z}/D\mathbb{Z})^n} z_{\mathbf{l}-\mathbf{r},\mathbf{m}-\mathbf{r}}\,\omega^{(\mathbf{l}-\mathbf{m})\cdot\mathbf{s}} \\ &\quad= D^n\delta_{\mathbf{l},\mathbf{m}} \sum_{\mathbf{r}\in(\mathbb{Z}/D\mathbb{Z})^n} z_{\mathbf{l}-\mathbf{r},\mathbf{l}-\mathbf{r}} = D^n\delta_{\mathbf{l},\mathbf{m}}. \end{aligned} \tag{B4}$$

Division by D^{2n} yields Eq. (B1) and finishes the proof.

APPENDIX C: ERROR ANALYSIS OF THE QUDIT REPEATER LINE WITHOUT QEC

Here, we derive Eq. (29) from the main text for unencoded repeater lines. We begin with the error model in Sec. C 1. In Sec. C 2, we compute the error statistics of the measurement at intermediate repeater stations, from which we derive the error statistics of the distributed state in Sec. C 3.

1. Error model

Since we do not assume a specific physical implementation of the qudits, all error sources are modeled by depolarizing channels. This is reasonable because for every error channel there is a worst-case approximation by a depolarizing channel. Nevertheless, our analysis can be adjusted to more specific error sources, if they can be modeled by Pauli error channels with independent X- and Z-type errors. Each faulty CZ gate is modeled by a perfect gate followed by single-qudit error channels $\mathcal{F}_\mathrm{G}$ on each qudit. Every time a qudit is transmitted from one station to the next, it is acted upon by an error channel $\mathcal{F}_\mathrm{T}$. Each faulty measurement is modeled by an error channel $\mathcal{F}_\mathrm{M}$ followed by a perfect measurement. Moreover, Alice's qudit undergoes storage errors, modeled by N channels $\mathcal{F}_\mathrm{S}$. For simplicity, we assume that the respective error rates, f_G, f_T, f_M, and $f_\mathrm{S}\in[0,1]$, are the same for each instance.

Experimentally, we should also take preparation errors into account, but we find they are not a dominating source of error and do not include them here for the sake of simplicity. The framework presented in this paper can handle such errors if desired.

2. Error statistics of measurements at intermediate repeater stations

As argued in Refs. [15,16], errors propagate a distance of at most two repeater stations. Hence, an error on the measurement outcomes c_i, where $i\in\{2,\ldots,N\}$, can arise from six sources: X errors from $\mathcal{F}_\mathrm{G}$ at repeater $i-2$ and from

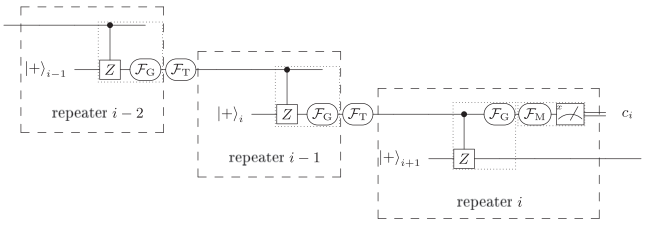

FIG. 8. Adapted from Fig. 3 of Ref. [15]. Sources of undetected errors on the measurement outcome at repeater $i \in \{2, \ldots, N\}$. If an X error occurs on qudit $i-1$ (one gate, one transmission), it induces a Z error on qudit i across the CZ gate. If this happens, or Z errors directly occur on qudit i (two gates, one transmission, one measurement), the measurement outcome might be erroneous.

$\mathcal{F}_T$ between repeaters $i-2$ and $i-1$ and Z errors from $\mathcal{F}_G$ at repeater $i-1$, from $\mathcal{F}_T$ between repeaters $i-1$ and i, as well as from $\mathcal{F}_G$ and $\mathcal{F}_M$ at repeater i; cf. Fig. 8.

Thus, the statistics of Z errors right before the measurement are given by an error probability tensor $P' = (p'_s)$ with entries given by the tensor equation

$$p'_s = M_s{}^a\, G_a{}^b\, T_b{}^c\, G_c{}^d\, T_d{}^e\, G_e{}^f\, p_f. \tag{C1}$$

Thereby, the error probability tensor is initialized to $P = (p_s)$ with $p_s = \delta_{s,0}$, and the tensors M, G, and T, which take measurement, gate, and transmission errors into account, respectively, can be regarded as matrices of the form $\frac{f_\alpha}{D} O + (1 - f_\alpha)\mathbb{1}$, where $\alpha \in \{\mathrm{M}, \mathrm{G}, \mathrm{T}\}$ and O is the $D \times D$ matrix with all entries equal to 1. Because of $O^2 \propto O$, the product of all matrices in Eq. (C1) is also a matrix of the form $aO + b\mathbb{1}$, for some $a, b \in [0, 1]$. Expanding the product of matrices yields $b = (1 - f_T)^2(1 - f_G)^3(1 - f_M)$, and the normalization $Da + b = 1$ determines a. Hence, the entries of P' are $p'_0 = a + b$ and $p'_{s\neq 0} = a$,

$$\begin{aligned} p'_0 &= \frac{1}{D}[1 + (D-1)(1-f_T)^2(1-f_G)^3(1-f_M)], \\ p'_{s\neq 0} &= \frac{1}{D}[1 - (1-f_T)^2(1-f_G)^3(1-f_M)]. \end{aligned} \tag{C2}$$

Note that for measurements at station 1, the error probability tensor $p'_s = M_s{}^a\, G_a{}^b\, T_b{}^c\, G_c{}^d\, p_d$ differs slightly from Eq. (C2) because, in contrast to qudits 1 to $N-1$, qudit A was not exposed to the channels $\mathcal{F}_G$ and $\mathcal{F}_T$ before the first CZ gate.

3. Error statistics of the distributed state

Since the error statistics of measurements at different repeater stations are independent of each other,[4] the probability of a Pauli-frame recovery error follows from the joint probability of measurement errors at the respective repeater stations. In particular, recovery errors give rise to an error channel on qudit B with coefficients $f_{r,s} = f_r^{\text{even}} f_s^{\text{odd}}$ determined by

$$F^{\text{even}}{}_a{}^z = F^{(2)}{}_a{}^b\, F^{(4)}{}_b{}^c\, F^{(6)}{}_c{}^d \ldots F^{(N)}{}_y{}^z, \tag{C3}$$

$$F^{\text{odd}}{}_a{}^z = F^{(1)}{}_a{}^b\, F^{(3)}{}_b{}^c\, F^{(5)}{}_c{}^d \ldots F^{(N-1)}{}_y{}^z, \tag{C4}$$

where $F^{(i)}{}_a{}^b := f^{(i)}_{a-b}$ is the abbreviation introduced in Sec. III B 2. Thereby, $f^{(i)}_{a-b}$ comes from the the measurement error statistics of repeater station i, $f_s^{(i)} := p'_{\pm s}$ as in Eq. (C2), and the signs of the indices come from Eq. (28).[5] The solution of Eq. (C3) and (C4) is

$$\begin{aligned} f_0^{\text{even}} &= \frac{1}{D}\{1 + (D-1)[(1-f_G)^{3N/2}(1-f_T)^N(1-f_M)^{N/2}]\}, \\ f_{r\neq 0}^{\text{even}} &= \frac{1}{D}\{1 - [(1-f_G)^{3N/2}(1-f_T)^N(1-f_M)^{N/2}]\}, \\ f_0^{\text{odd}} &= \frac{1}{D}\{1 + (D-1)[(1-f_G)^{3N/2-1}(1-f_T)^{N-1} \\ &\quad \times (1-f_M)^{N/2}]\}, \\ f_{s\neq 0}^{\text{odd}} &= \frac{1}{D}\{1 - [(1-f_G)^{3N/2-1}(1-f_T)^{N-1}(1-f_M)^{N/2}]\}, \end{aligned} \tag{C5, C6}$$

where $N \geqslant 2$ is even. This noise, f_r^{even} and f_s^{odd}, depolarizes along only the X and Z directions, respectively, as the other part of the (symmetrically) depolarizing noise vanishes since the X errors commute with the X measurements. Since the error statistics of the measurements are independent of those of qudits A and B, the error statistics of the distributed state are given by the truncated error probability tensor $\tilde{P} = (p_{\text{co}((0,r),(0,s))})$ with entries given by

$$\begin{aligned} &F^{\text{local}}{}_r{}^a{}_s{}^b \underbrace{F^{\text{prop}}{}_b{}^c\, F^{\text{odd}}{}_c{}^d}_{=:F^Z{}_b{}^d} \underbrace{F^{\text{even}}{}_a{}^e}_{=:F^X{}_a{}^e} (\delta_{(d,e),(0,0)}) \\ &\quad = f^{\text{local}}_{0,0} f_r^X f_s^Z + f^{\text{local}}_{\text{err}}\left(1 - f_r^X f_s^Z\right), \end{aligned} \tag{C7}$$

where

$$f_k^Z = f_k^X := f_k^{\text{even}} \tag{C8}$$

with f_k^{even} as in Eq. (C5). This finishes the proof of Eq. (29) for unencoded repeaters. Note that this solution can be obtained by taking normalization conditions into account, e.g., $1 = f_0^Z + (D-1) f_{s\neq 0}^Z$. Also note that $F^{\text{local}}{}_r{}^a{}_s{}^b$ is the error probability tensor of a depolarizing channel on qudits A and B with strength parameter

$$f^{\text{local}} := 1 - (1 - f_G)^2(1 - f_S)^N, \tag{C9}$$

[4] Error statistics of non-neighboring repeater stations are independent because errors propagate across at most one CZ gate. Moreover, for the depolarizing channel $f_{r,s} = f_r^X f_s^Z$ holds, where $f_r^X = \sum_s f_{r,s}$ and $f_s^Z = \sum_r f_{r,s}$, since X and Z errors are created independently. Because of this and because only Z errors lead to measurement errors, and only X errors induce Z errors across the CZ gate, the error statistics of measurements at neighboring stations are also independent.

[5] The sign of the index of $p'_{\pm s}$ alternates in i in the following way: $2: -; 4: +; 6: -; \ldots$, and, ...; $N-5: -; N-3: +; N-1: -$. To be more explicit, e.g., $f_2^{(i)} = p'_{-2}$ and $f_4^{(i)} = p'_{+2}$. Note that for depolarizing noise, $f_s^{(i)} = f_{-s}^{(i)}$.

which defines $f_{0,0}^{\text{local}}$ and $f_{\text{err}}^{\text{local}} := f_{(r,s)\neq(0,0)}^{\text{local}}$ via Eq. (8). Moreover, if an X error occurs on qudit N, which can happen at the CZ gate in repeater N and during its transmission to Bob, this X will induce a Z error at qudit B across Bob's CZ gate. This is taken into account via ${F^{\text{prop}}}_b{}^c$, the tensor corresponding to a Z-depolarizing error channel with strength parameter $f^{\text{prop}} = 1-(1-f_{\text{G}})(1-f_{\text{T}})$. Finally, note that Eq. (C7) holds for all even $N \geqslant 0$.

APPENDIX D: ERROR ANALYSIS OF THE QUDIT REPEATER LINE WITH QEC

Here, we derive Eq. (29) from the main text for encoded repeater lines. In particular, we generalize our error analysis to a qudit repeater line where each logical qudit consists of n physical qudits. For each physical qudit, we use the error model of Sec. C 1. Consider an $[\![n,1,d]\!]_D$ QECC with the following properties: It allows transversal CZ gates, it can correct X and Z errors independently, and it has logical operators $X_{\text{L}} = X^{\mathbf{r}}$ and $Z_{\text{L}} = Z^{\mathbf{s}}$, where $\mathbf{r},\mathbf{s} \in (\mathbb{Z}/D\mathbb{Z})^n$ have only invertible entries. Note that, for example, quantum polynomial codes satisfy all of these properties.

1. Error statistics of logical measurements at intermediate repeater stations

At the logical X measurement in a given repeater station, each of the n physical qudits are individually measured in the X basis. Since the CZ gate is transversal, errors do not spread across different blocks of physical qudits. Because of this and our depolarizing noise model, the error statistics of individual physical qudits at the measurement in a repeater station are the same as in Sec. C 2. The probability p_{e_i} that an error $e_i \in \mathbb{Z}/D\mathbb{Z}$ occurs on one of the n measurement outcomes is given in Eq. (C2). In particular, $p_1 = \cdots = p_{(D-1)}$. Thus, the probability of an error $\mathbf{e} = (e_1,\ldots,e_n)$ on the measurement outcomes at this station, is given by

$$p_{\mathbf{e}} = \prod_{i=0}^{n} p_{e_i} = p_0^{n-H(\mathbf{e})} p_1^{H(\mathbf{e})}, \tag{D1}$$

where the Hamming weight $H(\mathbf{e})$ is the number of nonzero digits in $\mathbf{e}$. Since an $[\![n,1,d]\!]_D$ code can correct up to $\lfloor\frac{d-1}{2}\rfloor$ arbitrary single qudit errors, we can consider the following (not necessarily efficient) strategy: If an error $\mathbf{e}$ with $H(\mathbf{e}) \leqslant \lfloor\frac{d-1}{2}\rfloor$ occurs, we identify and correct it. If, on the other hand $H(\mathbf{e}) > \lfloor\frac{d-1}{2}\rfloor$, we assign a random digit to the logical measurement outcome. The probability that a correctable error occurs is

$$p_{\text{cor}} := \sum_{j=0}^{\lfloor\frac{d-1}{2}\rfloor} (D-1)^j \binom{n}{j} p_0^{n-j}\, p_1^j, \tag{D2}$$

where $(D-1)^j\binom{n}{j}$ is the number of vectors in $(\mathbb{Z}/D\mathbb{Z})^n$ with exactly j nonzero entries. It follows that the probability of a particular logical error $e_{\text{L}} \neq 0$ is $p_{\text{guess}} = 1 - p_{\text{cor}}/D$, which is independent of e. The error correction is successful if either the error can be corrected or the occurred error was guessed. This happens with probability

$$p_{\text{succ}} = p_{\text{cor}} + p_{\text{guess}} = \frac{1}{D}[1+(D-1)p_{\text{cor}}]. \tag{D3}$$

As before, all error rates are the same for each repeater station except for the first.

2. Error statistics of the distributed logical state

We assume that Bob can perform a (perfect) round of stabilizer measurements before adjusting the Pauli frame according to his and the repeater stations' measurement outcomes. In this way, we reduce the error statistics of the $2n$ physical to just two logical qudits, while preserving all relevant information.

As per our error model, X^r and Z^s errors can be treated separately, and the respective probabilities are also independent of $r,s \neq 0$. Because of this and the fact that the logical state is stabilized by $X_{\text{A}} \otimes Z_{\text{B}}$ and $Z_{\text{A}} \otimes X_{\text{B}}$, each X error on one of Alice's physical qudits can be treated as some Z error on the corresponding physical qubit of Bob, and vice versa. (Here we need $X_{\text{L}} = X^{\mathbf{r}}$ and $Z_{\text{L}} = Z^{\mathbf{s}}$, where $\mathbf{r},\mathbf{s} \in (\mathbb{Z}/D\mathbb{Z})^n$ have only invertible entries.)

As in the unencoded case, errors which are introduced by one gate and one transmission induce Z errors on each physical qudit of Bob. Additionally, local errors on the physical qudits are introduced by two gate and N storage error sources. The probability of an X^r and Z^s error on qudit B right before the stabilizer measurements is therefore ${p^X}_r = {S^{(N)}}_r{}^a\, {G^{(2)}}_a{}^b\, \delta_{b,0}$ and ${p^Z}_s = {S^{(N)}}_s{}^a\, {G^{(3)}}_a{}^b\, {T^{(1)}}_b{}^c\, \delta_{c,0}$, respectively. Analogous to Eq. (C2), the solution of these tensor equations is

$$\begin{aligned}
p_0^X &= \frac{1}{D}[1+(D-1)(1-f_{\text{G}})^2(1-f_{\text{S}})^N],\\
p_{r\neq 0}^X &= \frac{1}{D}[1-(1-f_{\text{G}})^2(1-f_{\text{S}})^N],\\
p_0^Z &= \frac{1}{D}[1+(D-1)(1-f_{\text{G}})^2(1-f_{\text{S}})^N(1-f_{\text{T}})],\\
p_{s\neq 0}^Z &= \frac{1}{D}[1-(1-f_{\text{G}})^2(1-f_{\text{S}})^N(1-f_{\text{T}})].
\end{aligned} \tag{D4}$$

Employing the same correction strategy as before, the probability of a successful correction of X and Z errors is p_{succ}^X and p_{succ}^Z, analogous to Eq. (D2), and the probability of a specific error is $p_{\text{err}}^{X,Z} = (1-p_{\text{succ}}^{X,Z})/D$. Hence, the probability of a logical X^rZ^s error on Bob's qudit after the stabilizer measurement is

$$p_{r,s} = \begin{cases} p_{\text{succ}}^X p_{\text{succ}}^Z & \text{if } r=0, s=0\\ p_{\text{succ}}^X p_{\text{err}}^Z & \text{if } r=0, s\neq 0\\ p_{\text{err}}^X p_{\text{succ}}^Z & \text{if } r\neq 0, s=0\\ p_{\text{err}}^X p_{\text{err}}^Z & \text{if } r\neq 0, s\neq 0 \end{cases}. \tag{D5}$$

After the Pauli-frame adjustment, the error statistics of the distributed state finally become

$$p_{\text{co}((0,r),(0,s))} = {F^{\text{even}}}_r{}^a\, {F^{\text{odd}}}_s{}^b\, p_{a,b}, \tag{D6}$$

where $\mathcal{F}^{\text{even}}$ and $\mathcal{F}^{\text{odd}}$ are the error channels defined in Eqs. (C3) and (C4), respectively, but this time with the error rates of measurements on the *logical* level. In this way,

TABLE II. The number of accepted configurations $\alpha(2, 13, k_{\max}; m)$. Using a brute-force search over all matrices, $A \in \mathbb{F}_2^{N\times n}$, we obtain the values $\alpha(N, n, k_{\max}; m) = \#\{(a_{i,j}) \in \mathbb{F}_2^{N\times n} | m = \#\{a_{i,j} = 0\}, \forall i \in \{1, \ldots, N\} : k_{\max} \geqslant \#\{j | a_{i,j} a_{i-1,j} = 0\}\}$, for $N = 2$ and $n = 13$.

	$m=0$	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$	$m=6$	$m=7$	$m=8$	$m=9$
$k_{\max}=0$	1	0	0	0	0	0	0	0	0	0
$k_{\max}=1$	1	26	13	0	0	0	0	0	0	0
$k_{\max}=2$	1	26	325	312	78	0	0	0	0	0
$k_{\max}=3$	1	26	325	2600	3510	1716	286	0	0	0
$k_{\max}=4$	1	26	325	2600	14 950	24 596	17 446	5720	715	0

Eq. (D6) gets the same form as Eq. (C7), the analytical result for the unencoded repeater line. In particular, this finishes the proof of Eq. (29) for encoded repeaters.

APPENDIX E: ERROR ANALYSIS OF THE QUDIT REPEATER LINE WITH QEC AND ABORTION STRATEGY

Here, we adapt our error analysis to repeaters with an abortion strategy; cf. Sec. IV C. Recalling Eq. (31), a photon is absorbed during its transmission from repeater station $i-1$ to i with probability f_{abs}, and its absence is detected at the measurement of the corresponding qudit. The outcomes of such measurements at repeater stations i and $i+1$ are marked with a "?". The probability that k of the n measurement outcomes are marked as "?" at the first repeater station is given by

$$P_?^{\text{first}}(k) := \binom{n}{k} f_{\text{abs}}^k (1 - f_{\text{abs}})^{n-k}, \tag{E1}$$

and for every following repeater station by

$$P_?(k) := \binom{n}{k} [1 - (1 - f_{\text{abs}})^2]^k [(1 - f_{\text{abs}})^2]^{n-k}. \tag{E2}$$

The outcomes which are marked as "?" are discarded, and the remaining Dits constitute a classical error-correcting code with a Hamming distance of at least $d-k$ (equality if the original code does not inherit unnecessary redundancy). Hence, the logical measurement outcome is obtained by decoding the $n-k$ remaining physical outcomes according to a $[n-k, 1, d-k]_D$ error-correcting code. The probability of successfully correcting a given error with such a code is given by

$$p_{\text{cor},?}(k) := \sum_{j=0}^{\lfloor \frac{d-k-1}{2} \rfloor} (D-1)^j \binom{n-k}{j} p_0^{n-k-j} \, p_1^j. \tag{E3}$$

The quality of the distributed state can be improved if the protocol is aborted if too many noticed errors occur. Given that at most $k_{\max} < d$ qudits are discarded, the probability that repeater station $i \in \{2, \ldots, N\}$ can correct an error is

$$p_{\text{cor},k_{\max}} = \sum_{k=0}^{k_{\max}} \left(\frac{P_?(k)}{\sum_{k=0}^{k_{\max}} P_?(k)} \right) p_{\text{cor},?}(k), \tag{E4}$$

and likewise for the first repeater station. This is because, in the case that the protocol is not aborted, which happens with probability $\sum_{k=0}^{k_{\max}} P_?(k)$, the conditional probability that k qudits are discarded is $\frac{P_?(k)}{\sum_k P_?(k)}$.

Assume that Alice and Bob do not know the number of noticed errors at the repeater stations. Then, the rest of the analysis is analogous to Appendix D, where p_{cor} in Eq. (E3) is replaced by $p_{\text{cor},k_{\max}}$.

The probability of distributing the state

Here, we outline our approach for computing the probability of not aborting the protocol. There are N logical qudits transmitted, each of which is encoded into n physical qudits (photons). Therefore, there are Nn photons transmitted in total.

As the probabilities of the individual repeater stations not to abort the protocol depend on each other, the overall probability of successfully distributing the state (none of the repeater stations aborts) has to be computed via

$$P_{k_{\max}}^{\text{distr}} := \sum_{m=0}^{Nn} \alpha(N, n, k_{\max}; m) f_{\text{abs}}^m (1 - f_{\text{abs}})^{Nn-m}, \tag{E5}$$

where $\alpha(N, n, k_{\max}; m)$ is the number of configurations with exactly m absorbed photons, for which the protocol is not aborted (no logical measurement with more than $k_{\max}$ physical outcomes marked as "?"). We formalize this combinatorial problem in the following way. To each possible configuration of absorbed photons, we assign an $N \times n$ matrix $A = (a_{i,j})$. If, at the transmission from repeater $i-1$ to i, the jth qudit is absorbed, the corresponding matrix entry is set to 0. Otherwise, it is set to 1. With this, a matrix A corresponds to a successful distribution attempt if, for each of its rows $i \in \{1, \ldots, N\}$, the number of columns j fulfilling $a_{i,j} a_{i-1,j} = 0$ (the number of outcomes at repeater i marked as "?") is at most $k_{\max}$, where we set $a_{0,j} = 1$ for $1 \leqslant j \leqslant n$ (as there is no transmission before repeater 1). Thus, $\alpha(N, n, k_{\max}; m)$ can be computed as the number of matrices, $A \in \mathbb{F}_2^{N\times n}$, which correspond to a successful distribution attempt with exactly m zero entries. For $N = 2$ and $n = 13$, we find the values of $\alpha(N, n, k_{\max}; m)$ via a brute force computer search; see Table II.

[1] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. **26**, 1484 (1997).

[2] L. K. Grover, Quantum Mechanics Helps in Searching For a Needle in a Haystack, Phys. Rev. Lett. **79**, 325 (1997).

[3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and Coin Tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore* (IEEE, Piscataway, NJ, 1984), pp. 175–179.

[4] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[5] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).

[6] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, Phys. Rev. Lett. **81**, 5932 (1998).

[7] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Optimal architectures for long distance quantum communication, Sci. Rep. **6**, 20463 (2016).

[8] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, Long-Range Big Quantum-Data Transmission, Phys. Rev. Lett. **120**, 030503 (2018).

[9] D. Bruß and C. Macchiavello, Optimal Eavesdropping in Cryptography with Three-Dimensional Quantum States, Phys. Rev. Lett. **88**, 127901 (2002).

[10] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-Level Systems, Phys. Rev. Lett. **88**, 127902 (2002).

[11] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301 (2010).

[12] B. Brecht, D. V. Reddy, C. Silberhorn, and M. G. Raymer, Photon Temporal Modes: A Complete Framework for Quantum Information Science, Phys. Rev. X **5**, 041017 (2015).

[13] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding, New J. Phys. **17**, 022002 (2015).

[14] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[15] M. Epping, H. Kampermann, and D. Bruß, On the error analysis of quantum repeaters with encoding, Appl. Phys. B **122**, 54 (2016).

[16] M. Epping, H. Kampermann, and D. Bruß, Large-scale quantum networks based on graphs, New J. Phys. **18**, 53036 (2016).

[17] S. Janardan, Y. Tomita, M. Gutiérrez, and K. R. Brown, Analytical error analysis of Clifford gates by the fault-path tracer method, Quantum Inf. Proc. **15**, 3065 (2016).

[18] D. Gottesman, The Heisenberg representation of quantum computers, in *Proceedings of the 12th International Colloquium on Group Theoretical Methods in Physics: Group22*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.

[19] D. Gottesman, Fault-tolerant quantum computation with higher-dimensional systems, Chaos Solitons Fractals **10**, 1749 (1999).

[20] V. Gheorghiu, Standard form of qudit stabilizer groups, Phys. Lett. A **378**, 505 (2014).

[21] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Quantum communication without the necessity of quantum memories, Nat. Photon. **6**, 777 (2012).

[22] M. Epping, H. Kampermann, and D. Bruß, Robust entanglement distribution via quantum network coding, New J. Phys. **18**, 103052 (2016).

[23] A. N. Glaudell, E. Waks, and J. M. Taylor, Serialized quantum error correction protocol for high-bandwidth quantum repeaters, New J. Phys. **18**, 093008 (2016).

[24] D. A. Lidar and T. A. Brun, *Quantum Error Correction* (Cambridge University Press, Cambridge, UK, 2013).

[25] R. Cleve, D. Gottesman, and H. K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).

[26] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error rate, SIAM J. Comput. **38**, 1207 (2008).

[27] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inf. Theory **52**, 4892 (2006).

[28] A. W. Cross, Fault-tolerant quantum computer architectures using hierarchies of quantum error-correcting codes, Ph.D. thesis, Massachusetts Institute of Technology (2008).

[29] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Quantum repeater with encoding, Phys. Rev. A **79**, 032325 (2009).

[30] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, Surface Code Quantum Communication, Phys. Rev. Lett. **104**, 180503 (2010).

[31] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Quantum repeaters and quantum key distribution: Analysis of secret-key rates, Phys. Rev. A **87**, 052315 (2013).

[32] F. Ewert and P. van Loock, Ultrafast fault-tolerant long-distance quantum communication with static linear optics, Phys. Rev. A **95**, 012327 (2017).

[33] S. Muralidharan, C. L. Zou, L. Li, J. Wen, and L. Jiang, Overcoming erasure errors with multilevel systems, New J. Phys. **19**, 013026 (2017).

[34] S. Muralidharan, C. L. Zou, L. Li, and L. Jiang, One way quantum repeaters with quantum Reed-Solomon codes, Phys. Rev. A **97**, 052316 (2018).

[35] S. Bratzik, H. Kampermann, and D. Bruß, Secret key rates for an encoded quantum repeater, Phys. Rev. A **89**, 032335 (2014).

[36] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[37] R. H. Hadfield, Single-photon detectors for optical quantum information applications, Nat. Photon. **3**, 696 (2009).

[38] A. Uhlmann, The "transition probability" in the state space of a *-algebra, Rep. Math. Phys. **9**, 273 (1976).

[39] R. Jozsa, Fidelity for mixed quantum states, J. Mod. Opt. **41**, 2315 (1994).

[40] G. Vidal and R. F. Werner, Computable measure of entanglement, Phys. Rev. A **65**, 032314 (2002).

[41] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, Underwater quantum key distribution in outdoor conditions with twisted photons, arXiv:1801.10299.

[42] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[43] B. Eastin and S. T. Flammia, Q-circuit tutorial, arXiv:quant-ph/0406003.

[44] E. Moorhouse, Reed-Solomon codes, applied algebra (MATH 3500), http://ericmoorhouse.org/handouts/reed_solomon.pdf.

[45] N. Macon and A. Spitzbart, Inverses of Vandermonde matrices, Amer. Math. Monthly **65**, 95 (1958).

Appendix C

Comment on "Fully device-independent conference key agreement"

Title:	Comment on "Fully device-independent conference key agreement"
Authors:	Timo Holz, Daniel Miller, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review A
Impact factor:	2.907 (2018)
Date of submission:	04 June 2019
Publication status:	Published
Contribution by TH:	First author (input approx. 85%)

This publication corresponds to Ref. [HMKB19]. A summary of the results is presented in Chap. 7. In the course of my own research regarding multipartite DIQKD, I studied Ref. [RMW18] and discovered fundamental issues concerning central aspects of this publication. I regularly discussed the current state of my research with my co-authors who gave valuable input. In the form of a theorem, I established an incompatibility of perfect multipartite correlations in the presented QKD protocol and the required Bell type inequality violation which invalidated a significant portion of Ref. [RMW18], including the main result. I performed the entire analytical proof of this theorem. A requirement for the proof were Eqs. (3) and (8) of our article, which were established in collaboration with DM who provided its form for general N. The remaining analytical calculations were done by me. Furthermore, all numerical programs and computations were written and carried out by me. I wrote the entire manuscript which was proofread and improved by my co-authors.

Comment on "Fully device-independent conference key agreement"

Timo Holz,* Daniel Miller, Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany

(Received 4 June 2019; published 26 August 2019)

In this Comment we discuss the device-independent conference key agreement (DICKA) protocol [Phys. Rev. A **97**, 022307 (2018)]. We show that the suggested honest implementation fails, because perfectly correlated measurement results and the required Bell-inequality violation cannot be achieved simultaneously, in contradiction to what is claimed. We further show via semidefinite programming that there cannot exist *any* suitable honest implementation in the tripartite setting, rendering the DICKA protocol incomplete.

DOI: 10.1103/PhysRevA.100.026301

In Ref. [1], Ribeiro *et al.* proposed a protocol to generate a secret key among multiple parties, called device-independent conference key agreement (DICKA). The security proof crucially depends on the observation of genuine multipartite entanglement certified by a particular violation of a multipartite Bell inequality, the Mermin-Ardehali-Belinskiĭ-Klyshko (MABK) inequality [2–4]. Here, we analytically prove that the honest implementation of the DICKA protocol cannot yield a nonzero secret-key rate for an odd number of parties and provide numerical evidence that the first nontrivial even-numbered case fails as well. Finally, we use semidefinite programming (SDP) to prove that there cannot exist *any* honest implementation that leads to a nonvanishing secret-key rate for three parties, thus proving the incompleteness of the DICKA protocol. We use the same notation as Ref. [1].

MABK inequality. Consider a Bell setup with N parties called Paul$_i$ with two dichotomic observables P_0^i, P_1^i $\forall i \in [N] := \{1, \ldots, N\}$. We require an explicit expression for the odd-partite MABK operator. Let $\mathbb{F}_2 = \{0, 1\}$ denote the finite field with two elements, from which we obtain the vector space $\mathbb{F}_2^N$ of bit strings of length N. We define the Hamming weight

$$H(\boldsymbol{x}) := |\{1 \leqslant i \leqslant N | x_i = 1\}| \tag{1}$$

of a bit string $\boldsymbol{x} = (x_1, \ldots, x_N)$. For now, let N be an odd integer and define the set

$$\mathcal{L}_N := \left\{ \boldsymbol{x} \in \mathbb{F}_2^N \middle| H(\boldsymbol{x}) = \frac{N-1}{2} \mod 2 \right\}, \tag{2}$$

i.e., if $(N-1)/2$ is odd (even) the set $\mathcal{L}_N$ contains all bit strings $\boldsymbol{x}$ with an odd (even) number of bits 1.

Proposition. Let $N \geqslant 3$ be odd. An explicit form of the N-MABK operator is given by

$$MK_N = \frac{1}{\mathcal{N}_N} \sum_{\boldsymbol{x} \in \mathcal{L}_N} (-1)^{\xi_N(\boldsymbol{x})} \bigotimes_{i=1}^{N} P_{x_i}^i, \tag{3}$$

where $\xi_N(\boldsymbol{x}) := \frac{N-1}{4} - \frac{H(\boldsymbol{x})}{2}$ and $\mathcal{N}_N := 2^{\frac{N-1}{2}}$.

A single application of the recursion rule in Eq. (8) of Ref. [1] yields the MABK operator for N even. For all $N \geqslant 3$ the N-MABK inequality is given by the corresponding MABK operator MK_N, according to

$$\mathcal{MK}_N := \left| \mathrm{tr}\left(MK_N \rho_{\mathcal{P}_{(1\ldots N)}} \right) \right| \leqslant 2^{\frac{m-1}{2}}, \tag{4}$$

where $\rho_{\mathcal{P}_{(1\ldots N)}}$ denotes the quantum state shared among all N parties and $m \in [N]$ indicates the maximum number of parties that are entangled via $\rho_{\mathcal{P}_{(1\ldots N)}}$. A violation of the bound for $m = N-1$ certifies genuine N-partite entanglement [5], which is crucial for the security proof of the DICKA protocol.

There are $|\mathcal{L}_N| = 2^{N-1}$ different operators in the sum of Eq. (3). Thus, the N-MABK value $\mathcal{MK}_N$ contains $E_N = 2^{N-1}$ different expectation values. For general $N \geqslant 2$, the number of different expectation values E_N and the normalization factor $\mathcal{N}_N$ are given by

$$E_N = 2^{2\lfloor \frac{N}{2} \rfloor}, \quad \text{and} \quad \mathcal{N}_N = 2^{\lfloor \frac{N}{2} \rfloor}. \tag{5}$$

DICKA protocol and honest implementation. Alice has a measurement device with two inputs $X \in \{0, 1\}$, and each Bob$_k$ has three inputs $Y_{(k)} \in \{0, 1, 2\}$ for $k \in [N-1]$. The DICKA protocol consists of two different types of measurement rounds, one for key generation (type 0), where $(X, Y_{(1\ldots N-1)}) = (0, 2, \ldots, 2)$, and one for parameter estimation (type 1), where $X, Y_{(k)}$ are chosen uniformly at random from $\{0, 1\}$. In the honest implementation and in the asymptotic limit, the parties have access to infinitely many copies of the pure N-Greenberger-Horne-Zeilinger (GHZ) state $\mathrm{GHZ}_N := |\mathrm{GHZ}_N\rangle\langle\mathrm{GHZ}_N|$, with $|\mathrm{GHZ}_N\rangle := \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}$, which are distributed to the parties. Alice and the Bobs measure the observables (see the section between Protocol 2 and Theorem 4 of the Ref. [1]):

(i) For $X = 0$ ($X = 1$) Alice's observable is σ_z (σ_x).

(ii) For type-0 measurement rounds, i.e., for $Y_{(k)} = 2$, all Bobs measure the observable σ_z. And for type 1, i.e., $Y_{(k)} \in \{0, 1\}$, they measure observables "that are defined by a strategy that maximally violates the N-MABK inequality when the measurements are performed on an N-GHZ state."

We want to emphasize the following remarks. First, note that in any DI quantum key distribution (QKD) protocol, at least one party, say, Alice, is obliged to incorporate at least one

*holzt@uni-duesseldorf.de

measurement setting that is used for key generation rounds also in the parameter estimation rounds, to detect a potential preprogramming of the devices by the adversary. And second, in order to minimize the error correction information that is publicly communicated, and given that the N-GHZ state is measured, every party necessarily needs to measure the observable σ_z in type-0 rounds of the protocol, see Theorem 1 of Ref. [6]. Therefore, Alice has to use $A_0 = \sigma_z$ in both types of measurements. We claim that under these conditions there exist no measurement settings for the Bobs such that the N-MABK value exceeds the bound $2^{\frac{m-1}{2}}$ for $m = N-1$ in inequality (4), at least for odd N. Hence, the security of the DICKA protocol cannot be guaranteed.

Let $\mathcal{P}_N$ denote the N-qubit Pauli group. We define

$$\mathcal{S} := \{S \in \mathcal{P}_N |\ \ S|\mathrm{GHZ}_N\rangle = |\mathrm{GHZ}_N\rangle\}, \tag{6}$$

i.e., $\mathcal{S}$ denotes the stabilizer group of the N-GHZ state. The group $\mathcal{S}$ is generated by the N independent operators

$$G_1 := \sigma_x^{\otimes N}, \quad \text{and for all } j \in \{2, \ldots, N\}: \tag{7a}$$

$$G_j := \bigotimes_{i=1}^{j-2} \mathbb{1}_2^{(i)} \otimes \sigma_z^{(j-1)} \otimes \sigma_z^{(j)} \otimes \bigotimes_{i=j+1}^{N} \mathbb{1}_2^{(i)}, \tag{7b}$$

where the superscript denotes the corresponding subsystems. In general, the projector of any stabilizer state can be written as the normalized sum of all of its stabilizer operators [7,8]. We obtain for GHZ_N and with $\boldsymbol{s} := (s_1, \ldots, s_N)$ the representation:

$$\mathrm{GHZ}_N = \frac{1}{2^N} \sum_{\boldsymbol{s} \in \mathbb{F}_2^N} \left(\sigma_x^{s_1}\right)^{\otimes N} \left(\sigma_z^{s_2} \otimes \sigma_z^{s_2+s_3} \otimes \cdots \otimes \sigma_z^{s_{N-1}+s_N} \otimes \sigma_z^{s_N}\right). \tag{8}$$

No-go theorem for N odd. With the general form of the pure N-GHZ state in Eq. (8) and the properties of the N-MABK inequality, cf. Eq. (5), we state our initial claim:

Theorem 1. Let $N \geqslant 3$ be odd and let the N parties perform the honest implementation of the DICKA protocol. Then, the N-MABK value cannot exceed the bound that certifies genuine multipartite entanglement among all N parties.

Proof. Let $N \in \mathbb{N}$ be an odd integer and let

$$B_{Y_{(k)}}^{(k)} := \boldsymbol{\beta}_{Y_{(k)}}^{(k)T} \boldsymbol{\sigma}, \quad \forall k \in [N-1], \quad Y_{(k)} \in \{0, 1\} \tag{9}$$

be a general qubit measurement, where

$$\boldsymbol{\beta}_{Y_{(k)}}^{(k)} := (\beta_1, \beta_2, \beta_3)_{Y_{(k)}}^{(k)T} \equiv (\beta_x, \beta_y, \beta_z)_{Y_{(k)}}^{(k)T}, \tag{10a}$$

$$\boldsymbol{\sigma} := (\sigma_1, \sigma_2, \sigma_3)^T \equiv (\sigma_x, \sigma_y, \sigma_z)^T \tag{10b}$$

denote normalized Bloch vectors and a vector that contains the Pauli matrices. Recall that the product of Pauli matrices is given by

$$\sigma_j \sigma_k = \delta_{j,k} \mathbb{1}_2 + i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l, \tag{11}$$

where $\delta_{j,k}$ and ϵ_{jkl} denote the Kronecker delta and the Levi-Civita tensor, respectively. With Eq. (8) and for $A_0 = \sigma_z$, we obtain for the expectation value

$$\left\langle A_0 \bigotimes_{k=1}^{N-1} B_{Y_{(k)}}^{(k)} \right\rangle = \sum_{\boldsymbol{s} \in \mathbb{F}_2^N} \frac{2}{2^N} \delta_{s_1,0}\, \delta_{s_2,1}\, \mathrm{tr}\big(B_{Y_{(1)}}^{(1)} \sigma_x^{s_1} \sigma_z^{s_2+s_3} \otimes \cdots \otimes B_{Y_{(N-1)}}^{(N-1)} \sigma_x^{s_1} \sigma_z^{s_N}\big), \tag{12}$$

for all $Y_{(k)} \in \{0, 1\}$, where we used Eq. (11) and the fact that Pauli matrices are traceless to establish

$$\mathrm{tr}\big(\sigma_z \sigma_x^{s_1} \sigma_z^{s_2}\big) = 2\delta_{s_1,0}\delta_{s_2,1}. \tag{13}$$

Therefore, only operators with components $s_1 = 0$ and $s_2 = 1$ in Eq. (8) yield a nonvanishing contribution to the expectation value in Eq. (12). Now consider

$$B_{Y_{(1)}}^{(1)} \sigma_x^{s_1} \sigma_z^{s_2+s_3} = \sum_{i=1}^{3} \beta_{i,Y_{(1)}}^{(1)} \sigma_i \sigma_x^{s_1} \sigma_z^{s_2+s_3} \tag{14}$$

and note that we only get a nonvanishing contribution to the expectation value in Eq. (12), if there remains no nontrivial Pauli matrix in this expression. As $s_1 = 0$ and $s_2 = 1$, we see that $s_3 = 0$ needs to hold. Repeating this argument reveals that the only term in Eq. (8) that potentially gives a nonzero contribution to the expectation value is the bit string $\boldsymbol{s}$ with alternating entries of 0 and 1. Here, we observe a fundamental difference between odd and even numbers N. For N odd, the alternating pattern in $\boldsymbol{s}$ implies $s_N = 0$, thus for the observable of Bob_{N-1} in Eq. (12), we obtain $B_{Y_{(N-1)}}^{(N-1)} \sigma_x^{s_1} \sigma_z^{s_N} = B_{Y_{(N-1)}}^{(N-1)} \mathbb{1}$, which is traceless. Hence, the expectation value in Eq. (12) necessarily vanishes if $A_0 = \sigma_z$, i.e., for all $N \geqslant 3$ odd, we obtain

$$\left\langle \sigma_z \otimes \bigotimes_{k=1}^{N-1} B_{Y_{(k)}}^{(k)} \right\rangle_{\mathrm{GHZ}_N} = 0. \tag{15}$$

The structure of the N-MABK inequality (4) is such that half of the expectation values E_N include the observable $A_0 = \sigma_z$. Thus, only $E_N/2$ nonzero expectation values, each of them upper bounded by $+1$, can be present. A multiple application of the triangle inequality leads to

$$\mathcal{MK}_N = |\mathrm{tr}(MK_N \rho)| \leqslant \frac{1}{2} \frac{E_N}{\mathcal{N}_N} = 2^{\frac{N-3}{2}} \tag{16}$$

as a generous upper bound on the N-MABK value. A comparison with the bound that certifies genuine N-partite entanglement, cf. inequality (4) for $m = N-1$, reveals

$$\mathcal{MK}_N \leqslant 2^{\frac{N-3}{2}} < 2^{\frac{N-2}{2}}, \tag{17}$$

which finishes the proof. ∎

The even-partite case. The even-numbered analogon to Eq. (15) is given by

$$\left\langle \sigma_z \otimes \bigotimes_{k=1}^{N-1} B_{Y_{(k)}}^{(k)} \right\rangle_{\mathrm{GHZ}_N} = \prod_{k=1}^{N-1} \beta_{z,Y_{(k)}}^{(k)}, \tag{18}$$

which is in general nonvanishing and thus prohibits an analogous analytical proof of a similar no-go theorem for even N. Numerical optimization procedures, however, can be utilized to find the maximum possible N-MABK value, where the maximization is done over all Bloch components of all

observables but A_0 under the constraints of normalization for each Bloch vector. For $N = 4$, the maximization yields an upper bound of 1 for the maximum 4-MABK value, which constitutes the classical bound. Thus, we obtain numerical evidence, that in the first nontrivial even-numbered case of multipartite DICKA, the honest implementation fails as well.

A device-independent generalization. The results presented so far hint at fundamental problems of the DICKA protocol employing the MABK inequality. More precisely, perfect classical correlations and certified genuine multipartite entanglement via an MABK-inequality violation seem to be incompatible. So let us move away from the honest implementation. All we demand is that there exists a set of observables and a quantum state that perfectly correlate the measurement results of all parties in type-0 measurement rounds of the DICKA protocol. Besides this premise, no specific structure on the quantum state and the (projective, dichotomic) measurements are imposed. In this sense, it is a DI way to reinforce the results presented so far. To do this, we employ the Navasqués-Pironio-Acín (NPA) hierarchy [9], whose generality comes at the cost of being numerically expensive. We thus restrict the discussion to $N = 3$ parties. Note, however, that the extension to larger N is straightforward.

Theorem 2. Given a 3-partite quantum state ρ and a set of observables $(A_X, B^{(1)}_{Y_{(1)}}, B^{(2)}_{Y_{(2)}})$ that lead to perfectly correlated measurement results among all parties in type-0 measurement rounds of the DICKA protocol, then

$$\mathcal{MK}_3 \leqslant 2^{\frac{1}{2}} \tag{19}$$

holds, i.e., the 3-MABK value cannot exceed the bound that certifies genuine multipartite entanglement.

To show this theorem, let without loss of generality the indices $(X, Y_{(1)}, Y_{(2)}) = (0, 2, 2)$ indicate the set of inputs that yields perfect classical correlations. Let $A_0^{\pm}$, $B_2^{(1)\pm}$, and $B_2^{(2)\pm}$ denote the projectors onto the ± 1 eigenstate of the corresponding observables and define

$$\mathcal{C} := A_0^{+} \otimes B_2^{(1)+} \otimes B_2^{(2)+} + A_0^{-} \otimes B_2^{(1)-} \otimes B_2^{(2)-}. \tag{20}$$

The solution of the following SDP, for which we use Ref. [10], is the maximum 3-MABK value in this general setting, subject to the constraint of perfect correlations,

$$\begin{aligned} &\max_{A_X, B^{(1)}_{Y_{(1)}}, B^{(2)}_{Y_{(2)}}, \rho} \quad |\mathrm{tr}(MK_3\rho)| \\ &\text{subject to:} \quad \mathrm{tr}(\mathcal{C}\rho) = 1. \end{aligned} \tag{21}$$

The upper bound on the 3-MABK value obtained via the solution of the SDP (21) coincides with the bound that certifies genuine multipartite entanglement within numerical precision. Thus, there cannot exist a quantum state and a set of observables that simultaneously perfectly correlate all parties and lead to the required 3-MABK-inequality violation, which proves Theorem 2. The N-partite generalization of the SDP (21) can be carried out for arbitrary integers N at a proper hierarchy level.

Conclusion. We presented an analytical proof that the honest implementation of the DICKA protocol proposed in Ref. [1] fails for an odd number N of parties and provided numerical evidence that the protocol fails in the first nontrivial even-numbered case as well. We furthermore proved via SDP that there cannot exist *any* honest implementation of the DICKA protocol relying on the violation of the MABK inequality for $N = 3$ parties, thus proving its incompleteness. We finally conjecture that the N-partite generalization of Theorem 2 holds also true, which suggests that there cannot exist *any* honest implementation of the N-partite DICKA protocol that leads to a nonzero secret-key rate.

Acknowledgment. The authors acknowledge support from the Federal Ministry of Education and Research BMBF, (Project Q.Link.X).

[1] J. Ribeiro, G. Murta, and S. Wehner, Phys. Rev. A **97**, 022307 (2018).
[2] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[3] M. Ardehali, Phys. Rev. A **46**, 5375 (1992).
[4] A. V. Belinskiĭ and D. N. Klyshko, Phys. Usp. **36**, 653 (1993).
[5] R. F. Werner and M. M. Wolf, Phys. Rev. A **61**, 062102 (2000).
[6] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, New J. Phys. **19**, 093012 (2017).
[7] D. Gottesman, arXiv:quant-ph/9705052.
[8] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel, *Entanglement in Graph States and its Applications*, Proceedings of the International School of Physics "Enrico Fermi" Vol. 162 (IOS Press, Amsterdam, Netherlands), pp. 115–218.
[9] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).
[10] P. Wittek, ACM Trans. Math. Softw. **41**, 21 (2015).

Appendix D

Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters

Title:	Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters
Authors:	Daniel Miller, Timo Holz, Hermann Kampermann, and Dagmar Bruß
Journal:	Quantum
Date of submission:	14. June 2019
Impact factor:	There is no official impact factor yet.
Publication status:	Submitted
Contribution by TH:	Second author (input approx. 10%)

This publication corresponds to Ref. [MHKB19]. A summary of the results is presented in Chap. 7. The main research objective was jointly established by and regularly discussed among all authors. I helped identifying a figure of merit and suitable parameter regimes based on which we performed the presented systematic analysis. DM and I devised in collaboration the error model for the pure-loss channel for Fock encoded qudits. Beyond that, DM and I developed a physical understanding of how the experimental parameters manifest themselves in the results, as explained in the article. Furthermore, I wrote small parts of the manuscript. Finally, I helped proofreading and improving the entire article.

Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters

Daniel Miller, Timo Holz, Hermann Kampermann, and Dagmar Bruß

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

June 13, 2019

A potential quantum internet would open up the possibility of realizing numerous new applications, including provably secure communication. Since losses of photons limit long-distance, direct quantum communication and widespread quantum networks, quantum repeaters are needed. The so-called PLOB-repeaterless bound [Pirandola et *al.*, Nat. Commun. **8,** 15043 (2017)] is a fundamental limit on the quantum capacity of direct quantum communication. Here, we analytically derive the quantum-repeater gain for error-corrected, one-way quantum repeaters based on higher-dimensional qudits for two different physical encodings: Fock and multimode qudits. We identify parameter regimes in which such quantum repeaters can surpass the PLOB-repeaterless bound and systematically analyze how typical parameters manifest themselves in the quantum-repeater gain. This benchmarking provides a guideline for the implementation of error-corrected qudit repeaters.

Contents

Daniel Miller: daniel.miller@hhu.de

1 Introduction

The prospect of an eventual world-spanning quantum internet motivates tremendous interest and investments [1-3]. A quantum internet offers—among an increasing number of other applications [3-7]—the possibility of quantum key distribution (QKD), a cryptographic procedure whose security is not based on computational hardness assumptions but on the laws of quantum mechanics [8-10]. Although state-of-the-art experiments can perform fiber-based direct-transmission QKD across a few hundred kilometers [11], they face fundamental limitations [12-14]. The so-called PLOB-repeaterless bound (named after Pirandola, Laurenza, Ottaviani and Banchi) states that the quantum capacity of a fiber directly connecting two parties is exponentially suppressed in their distance [14]. As the quantum capacity is closely related to the amount of transmissible quantum information, direct transmission channels are not well suited for long distance quantum connections. To overcome these limitations, quantum repeaters have been proposed [15-20]. They shorten the distance of direct transmissions by introducing intermediate repeater stations such that losses and errors can be tackled using entanglement heralding, quantum memories, entanglement distillation, or quantum error-correcting codes (QECCs) [20]. Recent investigations have shown that quantum repeaters based on currently available technology have the potential to surpass the PLOB-repeaterless bound, even with a single intermediate repeater station [21-26]. Laboratory experiments have been reported which prove that it is in principle possible to surpass the PLOB-repeaterless bound over distances of tens and hundreds of kilometers [27-29].

For world-spanning quantum communication, error-corrected, one-way [17-19] (also known as third generation [20]) quantum repeaters are promising candidates. Since the implementation of such quantum repeaters will be demanding and expensive, it is crucial to identify under which circumstances they can be superior to direct quantum communication. Here, we address this problem in the case of error-corrected, one-way quantum repeaters based on qudits (discrete variable quantum systems of dimension $D \geq 2$), as such higher-dimensional qudits offer the advantage that more noise can be tolerated before entanglement is lost [30]. (See Refs. [31-34] for previous investigations in quantum repeaters based on qudits.) To conclude that a quantum repeater can overcome the PLOB-repeaterless bound, it is instrumental to find a lower bound on the achievable quantum capacity of quantum repeaters. In previous approaches [21-26], this figure of merit usually was given by the secret key rate achievable with a specific protocol; see also Refs. [35-39] for earlier investigations in secret key rates of quantum repeaters. In this paper, we use a different approach by exploiting that the quantum capacity of an error-corrected quantum repeater can be lower bounded by $\log_2(D) - H(P)$, where $H(P)$ is the Shannon entropy of the error probability distribution P of the state distributed by the repeater [14, 40]. There are numerous parameters influencing the performance of quantum repeaters, e.g., total distance, number of intermediate repeater stations, various error rates and choice of a QECC. In Ref. [33], we derived an expression of the error probability distribution P in terms of these parameters. Here, we identify and discuss parameter regimes in which error-corrected, one-way quantum repeaters based on qudits can beat the PLOB-repeaterless bound.

This paper is structured as follows. In Sec. 2, we explain our method to assess the quantum capacity of quantum repeaters. In Sec. 3, we identify parameter regions where error-corrected qudit repeaters can surpass the PLOB-repeaterless bound. Finally, in Sec. 4 we conclude and give an outlook on possible future work.

2 Identification of genuine quantum repeaters

Consider two remote parties called Alice and Bob. A quantum channel $\mathcal{E}$ from Alice to Bob is a completely positive, trace-preserving map from the space of density operators on Alice's Hilbert space to that of Bob. The (two-way) *quantum capacity*, $\mathcal{C}(\mathcal{E})$, quantifies how much quantum information Alice can transmit asymptotically to Bob through $\mathcal{E}$ using adaptive local operations and classical communications. See Ref. [14] for the formal definition. We call such a quantum channel a *genuine quantum repeater* if it has a quantum capacity that is larger than that of any direct transmission. In Sec. 2.1, we explain how this characterization depends on the encoding of qudits into photons by relating it to the multimode PLOB-repeaterless bound. In Sec. 2.2, we recall a more abstract description of qudits which we will use throughout this paper. In Sec. 2.3, we present the here-considered protocol for an error-corrected qudit repeater and define its *quantum-repeater gain*. If this figure of merit is positive, a genuine quantum repeater is identified.

2.1 Bosonic qudits and the PLOB-repeaterless bound

Consider a photonic mode with a bosonic creation operator $b^\dagger$. The *pure-loss channel* $\mathcal{E}_{\text{loss}}^{(\eta)} : b^\dagger \mapsto \sqrt{\eta}\, b^\dagger + \sqrt{1-\eta}\, b_{\text{E}}^\dagger$, mixes such a mode with a vacuum mode via a beam splitter with transmissivity η, where $b_{\text{E}}^\dagger$ is the creation operator of an environmental bosonic mode initialized in the zero-photon state $|0\rangle_{\text{E}}$ [41, 42]. The *PLOB-repeaterless bound* states that the quantum capacity of every quantum channel $\mathcal{E}$ is limited by that of $\mathcal{E}_{\text{loss}}^{(\eta)}$,

$$\mathcal{C}(\mathcal{E}) \leq \mathcal{C}(\mathcal{E}_{\text{loss}}^{(\eta)}) = -\log_2(1-\eta), \tag{1}$$

provided there exists a decomposition of the form $\mathcal{E} = \mathcal{E}_{\text{B}} \circ \mathcal{E}_{\text{loss}}^{(\eta)} \circ \mathcal{E}_{\text{A}}$ for some quantum channels $\mathcal{E}_{\text{A}}$ and $\mathcal{E}_{\text{B}}$ [14]. As this type of decomposition is typical for direct quantum communication scenarios, this bound is fundamental. Moreover, such decompositions are known for all Gaussian channels [14, 42].

The pure-loss channel transforms a pure Fock number state $|k\rangle = \frac{1}{\sqrt{k!}}(b^\dagger)^k |0\rangle$ into

$$\mathcal{E}_{\text{loss}}^{(\eta)}\left(|k\rangle\langle k|\right) = \sum_{j=0}^{k} \binom{k}{j} \eta^j (1-\eta)^{k-j}\ |j\rangle\langle j|\,. \tag{2}$$

Let $\mathcal{E}_{\text{Fock};D}^{(\eta)}$ denote the D-dimensional restriction of the pure-loss channel to inputs with $k \leq D-1$ photons. This channel possesses a decomposition $\mathcal{E}_{\text{Fock};D}^{(\eta)} = \mathcal{E}_{\text{CV}\to\text{DV}} \circ \mathcal{E}_{\text{loss}}^{(\eta)} \circ \mathcal{E}_{\text{DV}\to\text{CV}}$, where $\mathcal{E}_{\text{DV}\to\text{CV}}$ is the inclusion map from $\mathbb{C}^D$ to the single mode Fock space, i.e., $\mathcal{E}_{\text{DV}\to\text{CV}}$ sends a computational basis state to the state with the corresponding photon number, and similarly for $\mathcal{E}_{\text{CV}\to\text{DV}}$, cf. Ref. [14]. Thus, the PLOB-repeaterless bound yields

$$\mathcal{C}\left(\mathcal{E}_{\text{Fock},D}^{(\eta)}\right) \leq \mathcal{C}(\mathcal{E}_{\text{loss}}^{(\eta)}) = -\log_2(1-\eta), \tag{3}$$

where equality is reached in the limit $D \to \infty$. However, if D is finite, the inequality is strict, as not the full potential of the pure-loss channel is exploited.

Instead of encoding a D-dimensional qudit into the Fock basis, one could also use time-bin encoding [43-46], temporal modes (TM) [47,48] or modes of orbital angular momentum (OAM) [49-51]. For any of these implementations—to which we will from now on refer to as *multimode encoding*—the computational basis states are given by a single photon in one of D modes, i.e.,

$$|m\rangle := b_m^\dagger\, |\text{vac}\rangle\,, \tag{4}$$

where $b_m^\dagger$ is the creation operator of a bosonic mode labeled by $m \in \{0, \ldots, D-1\}$ and $|\text{vac}\rangle = |0, \ldots, 0\rangle$ is the vacuum state of all D modes. Sending such a qudit through a beam splitter gives rise to the D-dimensional erasure channel,

$$\mathcal{E}^{(\eta)}_{\text{erase};D} : \rho \longmapsto \eta\,\rho + (1-\eta)\,|\text{vac}\rangle\langle\text{vac}|\,. \tag{5}$$

Its quantum capacity is known to be $\mathcal{C}\left(\mathcal{E}^{(\eta)}_{\text{erase};D}\right) = \eta \log_2(D)$ [14]. If D bosonic modes are employed, the quantum capacity $\mathcal{E}_{\text{rep}}$ of a genuine quantum repeater has to beat the *multimode PLOB-repeaterless bound*,

$$\mathcal{C}(\mathcal{E}_{\text{direct}}) \leq -D \times \log_2(1-\eta), \tag{6}$$

which is the ultimate limit of direct quantum communication using D bosonic modes through free space or an optical fiber with transmissivity η because the quantum capacity of the pure loss channel is additive. At high loss $\eta \approx 0$, the multimode PLOB-repeaterless bound scales linearly in the transmissivity according to $-D \times \log_2(1-\eta) \approx 1.44 D\eta$ [14].

2.2 Abstract description of qudits

Formally, a qudit is a quantum system with a Hilbert space of dimension $D \geq 2$. We label its computational basis states $|j\rangle$ by elements j in $\mathbb{Z}/D\mathbb{Z} = \{0, 1, \ldots, D-1\}$, the ring of integers modulo D. For example,

$$|+\rangle := \frac{1}{\sqrt{D}} \sum_{j \in \mathbb{Z}/D\mathbb{Z}} |j\rangle\,, \tag{7}$$

is the equally weighted superposition of all computational basis states. Up to a global phase, the generalized Pauli-operators of a qudit are products of

$$X := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} |k+1\rangle\langle k| \qquad \text{and} \quad Z := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} \omega^k\,|k\rangle\langle k|\,, \tag{8}$$

where $\omega := \mathrm{e}^{2\pi i/D}$, i.e., the generalized Pauli-operators are of the form

$$X^r Z^s = \sum_{k \in \mathbb{Z}/D\mathbb{Z}} \omega^{ks}\,|k+r\rangle\langle k|\,, \tag{9}$$

where $r, s \in \mathbb{Z}/D\mathbb{Z}$. They constitute a basis of the vector space of complex $D \times D$ matrices [53, 54]. The generalized Pauli-error channel, given an error probability distribution $P = (p_{r,s})_{r,s \in \mathbb{Z}/D\mathbb{Z}}$ with $\sum_{r,s} p_{r,s} = 1$, is defined as the quantum channel,

$$\mathcal{E}_P : \rho \longmapsto \sum_{r,s \in \mathbb{Z}/D\mathbb{Z}} p_{r,s} (X^r Z^s) \rho (X^r Z^s)^\dagger, \tag{10}$$

with Kraus operators $\sqrt{p_{r,s}} X^r Z^s$. It corresponds to the random application of a Pauli-operator $X^r Z^s$ to the state ρ with probability $p_{r,s}$. The depolarizing channel,

$$\mathcal{E}^{(1-f)}_{\text{depol};D} : \rho \longmapsto (1-f)\rho + f\frac{\mathbb{1}}{D}, \tag{11}$$

is an example of a generalized Pauli-error channel where the trivial error $X^0 Z^0 = \mathbb{1}$ occurs with probability $p_{0,0} = 1 - f + f/D^2$ and any other error occurs with probability f/D^2 [33]. The controlled-Z gate,

$$\text{CZ} := \sum_{k \in \mathbb{Z}/D\mathbb{Z}} |k\rangle\langle k| \otimes Z^k \tag{12}$$

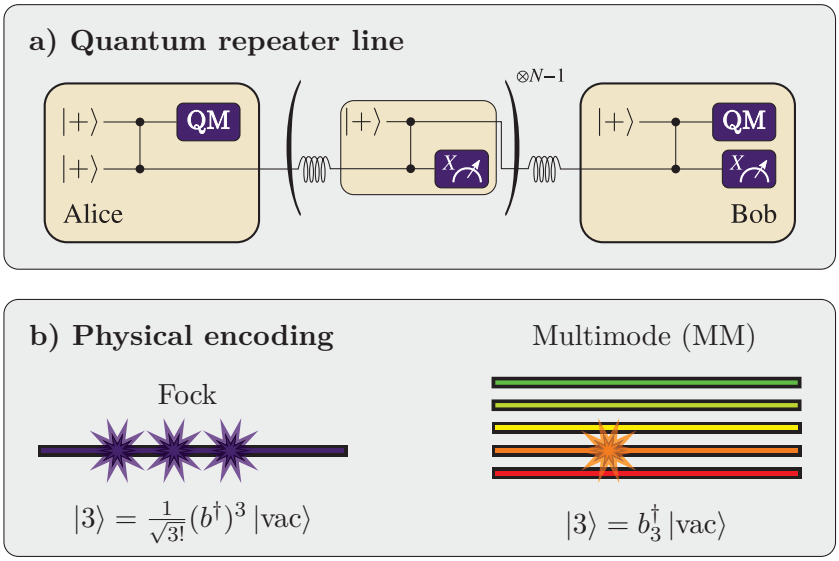

Figure 1: **a)** An error-corrected, one-way qudit quantum repeater line with $N-1$ intermediate repeater stations [33,37-39]. Alice produces the two-qudit state $|\Phi\rangle = \mathrm{CZ}\,|+\rangle^{\otimes 2}$, stores one qudit into a quantum memory (QM), and sends the other qudit to the first intermediate repeater station. At every repeater station, the incoming qudit is entangled via a CZ gate with a new qudit prepared in the $|+\rangle$ state. Then, the previous qudit is measured in the X basis and the other qudit is sent to the next repeater station. After N transmissions, Bob receives the last qudit, entangles it with his own $|+\rangle$ state, measures it, and stores the remaining qudit in his own QM. As a result, Alice and Bob have stored an entangled qudit pair in their QMs. The protocol takes place on a logical level where each logical qudit consists of n physical qudits. **b)** Visualization of two different encoding methods into photons.

is a two-qudit Clifford gate which can be used to produce the maximally-entangled state,

$$|\Phi\rangle := \mathrm{CZ}\,|+\rangle^{\otimes 2} = \frac{1}{D}\sum_{j,k\in\mathbb{Z}/D\mathbb{Z}} \omega^{jk}\,|j\rangle\otimes|k\rangle\,, \tag{13}$$

from two copies of the $|+\rangle$ state.

2.3 Error-corrected qudit repeaters and the quantum-repeater gain

Assume that Alice and Bob make use of the one-way quantum repeater protocol described in the caption of Fig. 1. In the ideal case, they obtain a maximally entangled state $B^\dagger\,|\Phi\rangle$ in their quantum memories (QMs) which only differs from $|\Phi\rangle$ of Eq. (13) by the application of the byproduct operator $B = X^{c_{\mathrm{even}}} Z^{c_{\mathrm{odd}}}$ to Bob's qudits, where the number of elementary links N is even. The exponents

$$c_{\mathrm{even}} := \sum_{i=1}^{N/2}(-1)^i c_{2i} \qquad \text{and} \qquad c_{\mathrm{odd}} := \sum_{i=1}^{N/2}(-1)^{i+1} c_{N+1-2i}, \tag{14}$$

are computed from the measurement outcomes c_i at the i-th repeater station, i.e., c_{even} depends on the measurement outcomes of even-numbered repeater stations and likewise for c_{odd}. See Ref. [33] for more details.

To overcome the limit of direct quantum communication, the quantum repeater employs logical qudits which are encoded using an $[\![n,1,d]\!]_D$ QECC such that each qudit is replaced by n physical qudits of dimension D. The code distance d determines the number t of

correctable errors by the QECC according to $t = \lfloor (d-1)/2 \rfloor$, see Ref. [55] for its formal definition. Note that QECCs do not exist for all code parameters, e.g., all QECCs fulfill the quantum singleton bound $2d-1 \leq n$. However, if D is a prime number and $d \leq (D-1)/2$, an explicit construction of $[\![2d-1, 1, d]\!]_D$ QECCs saturating the quantum singleton bound is known in the form of quantum polynomial codes [56-59]. We focus on this encoding because quantum polynomial codes can give an advantage over other QECCs for quantum repeaters [31, 32].

At every repeater station, the (logical) X measurement is performed as follows. All physical qudits are measured individually in the eigenbasis of the X operator. If the number of erroneous measurement results is smaller than or equal to t, the error pattern can be corrected successfully. Otherwise, the repeater station guesses a random measurement result. It turns out [33] that all repeater stations (except for the first) have the same probability $p_{\text{succ}}^{\text{rep}}$ of a successful correction. For the first repeater station, where fewer error sources contribute, we denote this probability by $p_{\text{succ}}^{1.\text{rep}}$. To simplify the error analysis, we furthermore assume that Bob performs a (perfect) round of stabilizer measurements. As quantum polynomial codes belong to the class of Calderbank-Shor-Steane codes [59], Bob can independently correct X and Z errors. Again, if the number of X (Z) errors exceeds t, Bob guesses a recovery operation. Otherwise, with probability $p_{\text{succ}}^{\text{Bob},X}$ ($p_{\text{succ}}^{\text{Bob},Z}$), he can successfully reveal the error pattern and applies the appropriate recovery operation. In the final step of the entanglement swapping protocol, Bob has to apply the byproduct operator $B = X^{c_{\text{even}}} Z^{c_{\text{odd}}}$. In doing so, errors on the measurement results of the even-numbered repeater stations propagate to X errors on Bob's qudit which gives rise to an X dephasing channel, $\rho \mapsto p_{\text{succ}}^{\text{rep}} \rho + \frac{1-p_{\text{succ}}^{\text{rep}}}{D} \sum_{r \in \mathbb{Z}/D\mathbb{Z}} X^r \rho X^{-r}$. Likewise, wrong measurement results at odd-numbered repeater stations induce Z errors on Bob. In conclusion, the overall error statistics are of the form $P = (p_{r,s}^{\text{fin}})_{r,s \in \mathbb{Z}/D\mathbb{Z}} = (p_r^{\text{fin},X} p_s^{\text{fin},Z})_{r,s \in \mathbb{Z}/D\mathbb{Z}}$, where

$$\begin{aligned} p_0^{\text{fin},X} &= \frac{1}{D}\left[1 + (D-1)(p_{\text{succ}}^{\text{rep}})^{\frac{N}{2}} p_{\text{succ}}^{\text{Bob},X}\right] \text{ and} \\ p_{r\neq 0}^{\text{fin},X} &= \frac{1}{D}\left[1 - (p_{\text{succ}}^{\text{rep}})^{\frac{N}{2}} p_{\text{succ}}^{\text{Bob},X}\right] \end{aligned} \tag{15}$$

are the probabilities of X errors on Bob's qudit, and

$$\begin{aligned} p_0^{\text{fin},Z} &= \frac{1}{D}\left[1 + (D-1) p_{\text{succ}}^{1.\text{rep}} (p_{\text{succ}}^{\text{rep}})^{\frac{N}{2}-1} p_{\text{succ}}^{\text{Bob},Z}\right] \text{ and} \\ p_{s\neq 0}^{\text{fin},Z} &= \frac{1}{D}\left[1 - p_{\text{succ}}^{1.\text{rep}} (p_{\text{succ}}^{\text{rep}})^{\frac{N}{2}-1} p_{\text{succ}}^{\text{Bob},Z}\right] \end{aligned} \tag{16}$$

are the probabilities of Z errors. We will explain in Sec. 3.2 how these success probabilities depend on the physical error rates.

The erroneous state distributed by the quantum repeater is $\rho = \mathcal{E}_P(\Phi)$, where $\Phi = |\Phi\rangle\langle\Phi|$ is the projector onto the maximally entangled state defined in Eq. (13), and $\mathcal{E}_P$ is the generalized Pauli-error channel, recall Eq. (10), corresponding to the error distribution P acting on Bob's qudit. The quantum capacity of a generalized Pauli-error channel $\mathcal{C}(\mathcal{E}_P)$ can be lower bounded by

$$\mathcal{C}(\mathcal{E}_{\text{rep}}) = \mathcal{C}(\mathcal{E}_P) \geq \max\{0, \log_2(D) - H(P)\} =: B_{\text{rep}}^{\downarrow}, \tag{17}$$

see suppl. of Ref. [14]. Note that $B_{\text{rep}}^{\downarrow}$ is also a lower bound on the distillible entanglement of $\mathcal{E}_P(\Phi)$ which is achievable with a distillation protocol given in Ref. [40]. Since a logical qudit is encoded into n physical qudits, the number of photonic modes used to connect

two repeater stations is $M = n$ and $M = nD$ for Fock and MM encoding, respectively. Thus, the multimode PLOB-repeaterless upper bound, recall Eq. (6), is given by

$$B^{\uparrow}_{\mathrm{PLOB}} := \begin{cases} -n \times \log_2(1-\eta), & \text{Fock encoding} \\ -nD \times \log_2(1-\eta), & \text{MM encoding} \end{cases}, \tag{18}$$

where η is the transmissivity of a pure-loss channel corresponding to the total distance L from Alice to Bob. Every direct transmission channel employing the same number of photonic modes, as the quantum repeater has a quantum capacity smaller than $B^{\uparrow}_{\mathrm{PLOB}}$. The quantum repeater, on the other hand, has a quantum capacity larger than $B^{\downarrow}_{\mathrm{rep}}$. Hence, the quantum repeater is genuine if (but not necessarily only if) the *quantum-repeater gain*,

$$\Delta := B^{\downarrow}_{\mathrm{rep}} - B^{\uparrow}_{\mathrm{PLOB}}, \tag{19}$$

is positive.

3 Parameter regimes for genuine quantum repeaters

As we have argued in Sec. 2.3, error-corrected, one-way qudit repeaters have a quantum capacity of at least $B^{\downarrow}_{\mathrm{rep}} = \log_2(D) - H(P)$, where the error probability distribution $P = (p^{\mathrm{fin}}_{r,s})_{r,s\in\mathbb{Z}/D\mathbb{Z}}$ depends on various parameters of the quantum repeater such as the qudit dimension D, the distance L between Alice and Bob, the number $N-1$ of repeater stations, and the parameters of the $[\![n, 1, d]\!]_D$ QECC. In Sec. 3.1, we introduce our noise model and derive a worst-case approximation of the pure-loss channel for Fock qudits. In Sec. 3.2, we provide the analytical dependence of P on all these parameters for both Fock and MM encoding. Afterwards, in Secs. 3.3–3.5, we investigate parameter regimes for genuine quantum repeaters.

3.1 Noise model

In a realistic scenario, Alice and Bob have to deal with errors. Each transmission channel from one repeater station to the next is modeled as a pure-loss channel $\mathcal{E}^{(\eta_0)}_{\mathrm{loss}}$ with transmissivity

$$\eta_0 = 10^{-\frac{\alpha L_0}{10}}, \tag{20}$$

where L_0 is the distance between the repeater stations and $\alpha = 0.2$ dB/km is the attenuation of optical fibers at 1550 nm wavelength [60]. We derive an approximation of pure-loss channels with generalized Pauli-error channels in Sec. 3.1.1 as preparation for an error analysis using the framework of Ref. [33].

Besides transmission losses, we also include measurement errors (f_{M}), modeled by a depolarizing channel $\mathcal{E}^{(1-f_{\mathrm{M}})}_{\mathrm{depol};D}$, recall Eq. (11), before each measurement. Unless stated otherwise, we use the value $f_{\mathrm{M}} = 0.01$, as the best single-photon detector efficiencies of about 95% match this order of magnitude [61]. To model gate errors (f_{G}), we furthermore assume that all CZ gates are followed by two depolarizing channels (one on each qudit) with an optimistic error parameter $f_{\mathrm{G}} = 10^{-3}$. Deterministic photon-photon gates for polarization qubits based on light-matter interactions have been demonstrated with an average gate fidelity of $76.2 \pm 3.6\%$ [62]. Two-mode gates for Fock qudits could in principle be realized using Kerr-interactions [63], however, high-fidelity phase gates have only been reported for a single photonic mode [64]. In Sec. 3.4, we will examine how the quantum-repeater gain Δ depends on the operational error rates f_{M} and f_{G}.

Finally, storage errors (f_S) affecting Alice's physical qudits in the QMs are modeled by depolarizing channels, $\mathcal{E}^{(1-f_S)}_{\text{depol};D}$, with

$$1 - f_S = 10^{-\frac{\gamma L/c}{10}}, \tag{21}$$

where γ is the decaying rate of Alice's QM and $c = 200\text{km/ms}$ is the speed of light in a fiber with a refractive index of 1.5. Optical fiber loop QMs, with $\gamma_{\text{fiber}} = \alpha c = 40\text{dB/ms}$, are not useful, as the stored qudits decay with the same rate as the flying qudits. However, matter-based QMs have been demonstrated: Cold atomic ensembles provide QMs with $\gamma_{\text{atom}} = 5\text{dB/ms}$ (50% efficiency in 0.6ms) [65]. Promising candidates are based on nitrogen vacancy centers in diamond which range from $\gamma_{\text{NV}} = 4 \times 10^{-3}\text{dB/ms}$ (coherence time $T_2 \approx 1\text{s}$) [66, 67] to $\gamma_{\text{NV}} = 7 \times 10^{-5}\text{dB/ms}$ ($T_2 \approx 60\text{s}$) [68]. Using trapped ions, decaying rates of $\gamma_{\text{ion}} = 7 \times 10^{-6}\text{dB/ms}$ are possible [69]. Since these proof-of-principle QMs do not take storage-and-retrieval efficiencies into account, we use a more realistic value of $\gamma = 10^{-2}\text{dB/ms}$ ($T_2 \approx 100\text{ms}$ [70]) for our analysis.

3.1.1 Approximation of pure-loss channels with generalized Pauli-channels

Recall from Eq. (5) that the pure-loss channel, $\mathcal{E}^{(\eta_0)}_{\text{loss}}$, acts on MM qudits as an erasure channel which, in turn, can be regarded as a depolarizing channel, as it converts a pure input state $\rho = |\psi\rangle\langle\psi|$ into

$$\mathcal{E}^{(\eta_0)}_{\text{erase};D}(\rho) = \eta_0\rho + (1-\eta_0)\rho^{\perp} \quad = (1-f_{\text{T}})\rho + f_{\text{T}}\frac{\mathbb{1}}{D} = \mathcal{E}^{(1-f_{\text{T}})}_{\text{depol};D}(\rho), \tag{22}$$

where $\rho^{\perp} = \frac{\mathbb{1}-\rho}{D-1}$ is a normalized state orthogonal to $\rho = |\psi\rangle\langle\psi|$, and $f_{\text{T}} = (1-\eta_0)(D-1)/D$ can be interpreted as transmission error rate. Since each of the pure-loss channels between the individual repeater stations is applied exactly once, we can thus replace them by depolarizing channels, $\mathcal{E}^{(1-f_{\text{T}})}_{\text{depol};D}$.

If, on the other hand, the qudits are encoded in the Fock basis, the pure-loss channel introduces errors on the number of photons. Losing exactly r photons can be regarded as an application of the error operator $E = X^{-r}$, recall Eq. (8). For a given input state $|k\rangle$, the probability for this to happen is given by

$$\Pr\left(E = X^{-r} \mid \rho_{\text{in}} = |k\rangle\langle k|\right) = \begin{cases} \binom{k}{r}\eta_0^{k-r}(1-\eta_0)^r, & r \leq k \\ 0, & r > k \end{cases}, \tag{23}$$

where $k, r \in \{0, \ldots, D-1\}$, as we have seen in Eq. (2). To upper bound the X error probabilities, we set

$$p^{\text{appr}}_{-r} := \max_{k\in\{0,\ldots,D-1\}} \Pr\left(E = X^{-r} \mid \rho_{\text{in}} = |k\rangle\langle k|\right) \tag{24}$$

for all $r \neq 0$. If $p^{\text{appr}}_0 := 1 - \sum_{r=1}^{D-1} p^{\text{appr}}_{-r}$ is positive, we can model the pure-loss channel on Fock state qudits of a single bosonic mode by the generalized Pauli-error channel,

$$\mathcal{E}^{(\eta_0)}_{\text{appr};D} : \rho \longmapsto \sum_{r=0}^{D-1} p^{\text{appr}}_{-r} X^{-r}\rho(X^{-r})^{\dagger}, \tag{25}$$

as a worst-case approximation. In the error analysis for Fock-state encoding, we thus replace each pure-loss channel,$\mathcal{E}^{(\eta_0)}_{\text{loss}}$, between any two repeater stations by $\mathcal{E}^{(\eta_0)}_{\text{appr};D}$. Note that this further decreases $B^{\downarrow}_{\text{rep}}$; thus, $\Delta > 0$ will still indicate a genuine quantum repeater.

We will only consider repeater lines for which the repeater stations are spaced close enough such that $p_0^{\text{appr}} \geq 0$, i.e., $\eta_0 \approx 1$. To compute the error probabilities in Eq. (24), we have to find the input state $|k\rangle$ with the highest probability to lose r photons. By differentiating the analytical continuation of Eq. (23), we obtain

$$0 = \frac{\partial}{\partial k}\left[\binom{k}{r}\eta_0^{k-r}(1-\eta_0)^r\right] = \binom{k}{r}\eta_0^{k-r}(1-\eta_0)^r\left(\ln(\eta_0) + H_k - H_{k-r}\right), \tag{26}$$

where

$$H_k := \sum_{j=1}^{k}\frac{1}{j} = \ln(k) + \gamma_{\text{EM}} + \frac{1}{2k} - \frac{1}{12k^2} + \frac{1}{120k^4} - \dots \tag{27}$$

is the kth Harmonic number and $\gamma_{\text{EM}} \approx 0.577$ is the Euler-Mascheroni constant. For large k, the approximation $H_k - H_{k-r} \approx \ln(k) - \ln(k-r)$ yields $k \approx r/(1-\eta_0)$ as the solution of Eq. (26). This is indeed a maximum because the sign of the derivative given in Eq. (26) changes at $k \approx r/(1-\eta_0)$ from plus to minus, when increasing k. This follows from the positivity and the strictly monotonic decrease of the derivative of the analytical continuation of H_k. Let $\text{rd}(x)$ denote the integer that is closest to $x \in \mathbb{R}$. Because of $\eta_0 \approx 1$, the approximation is so good that the integer $\tilde{k}(r,\eta_0) := \min\{\text{rd}\left(r/(1-\eta_0)\right), D-1\}$ is the number of input photons having the highest probability (among inputs of up to $D-1$ photons) to lose exactly r photons. This yields

$$p_{-r}^{\text{appr}} = \binom{\tilde{k}(r,\eta_0)}{r}\eta_0^{\tilde{k}(r,\eta_0)-r}(1-\eta_0)^r \tag{28}$$

as the solution of Eq. (24).

3.2 Error statistics for error-corrected, one-way qudit repeaters

In order to evaluate the quantum-repeater gain defined in Eq. (19), one has to know the error probability distribution P of the entangled state distributed by the quantum repeater. In Sec. 3.2.1 and Sec. 3.2.2, we derive for MM and Fock qudits, respectively, the expression of the success probabilities $p_{\text{succ}}^{1.\text{rep}}$, $p_{\text{succ}}^{\text{rep}}$, $p_{\text{succ}}^{\text{Bob},X}$, and $p_{\text{succ}}^{\text{Bob},Z}$ (recall the paragraph above Eq. (15) for their definitions) from which P follows via Eqs. (15) and (16).

3.2.1 Error statistics for multimode qudits

Here, we review our previous results [33] which hold for error-corrected qudit repeater lines where the qudits are encoded into multiple bosonic modes, e.g., time-bin, TM, and OAM qudits. Recall from Eq. (22) that the pure-loss channel with transmissivity η_0 can be modeled by a depolarizing channel with error rate $f_{\text{T}} = (1-\eta_0)(D-1)/D$. Depolarizing channels can be regarded as sources of discrete X and Z errors which propagate through the repeater line. It turns out that there are six sources from which a Z^{e_i} error at the X measurement of qudit i can originate: two transmission, three gate, and one measurement error channel [33,37-39]. Such an error will change the physical measurement result c_i into $c_i + e_i \in \mathbb{Z}/D\mathbb{Z}$ with probability $p_{e_i}^{\text{rep}}$, where

$$p_{e_i\neq 0}^{\text{rep}} = \frac{1}{D}\left[1 - (1-f_{\text{T}})^2(1-f_{\text{G}})^3(1-f_{\text{M}})\right] \tag{29}$$

and $p_0^{\text{rep}} = 1 - (D-1)p_{e_i\neq 0}^{\text{rep}}$. For the first repeater station, fewer error sources contribute: $p_{e_i\neq 0}^{1.\text{rep}} = \frac{1}{D}\left[1 - (1-f_{\text{T}})(1-f_{\text{G}})^2(1-f_{\text{M}})\right]$ and $p_0^{1.\text{rep}} = 1 - (D-1)p_{e_i\neq 0}^{1.\text{rep}}$. Similarly, the

probability of an X^{e_i} and Z^{e_i} error on Bob's qudit right before the stabilizer measurement is given by $p_{e_i}^{\mathrm{Bob},X}$ and $p_{e_i}^{\mathrm{Bob},Z}$, respectively, where $p_{e_i\neq 0}^{\mathrm{Bob},X} = \frac{1}{D}\left[1-(1-f_{\mathrm{G}})^2(1-f_{\mathrm{S}})\right]$, and $p_{e_i\neq 0}^{\mathrm{Bob},Z} = \frac{1}{D}\left[1-(1-f_{\mathrm{T}})(1-f_{\mathrm{G}})^3(1-f_{\mathrm{S}})\right]$, and $p_0^{\mathrm{Bob},X}$, $p_0^{\mathrm{Bob},Z}$ again follow from normalization. See Ref. [33] for more details.

In the following, let p_{e_i} be either $p_{e_i}^{\mathrm{rep}}$, $p_{e_i}^{1.\mathrm{rep}}$, $p_{e_i}^{\mathrm{Bob},X}$, or $p_{e_i}^{\mathrm{Bob},Z}$, and likewise for p_{succ}. In either situation, n individual measurement results are employed for the error correction attempt based on the $[\![n,1,d]\!]_D$ QECC. Since the error probability of a single error $e_i \in \mathbb{Z}/D\mathbb{Z}$ is given by p_{e_i}, the probability of an error pattern $\mathbf{e} = (e_1,\ldots,e_n)$ at the respective error correction attempt is given by

$$p_{\mathbf{e}} = \prod_{i=0}^{n} p_{e_i} = p_0^{n-\mathrm{wt}(\mathbf{e})} p_{e\neq 0}^{\mathrm{wt}(\mathbf{e})}, \tag{30}$$

where the Hamming weight $\mathrm{wt}(\mathbf{e})$ denotes the number of nonzero entries of $\mathbf{e}$. As the QECC can correct up to $\lfloor (d-1)/2 \rfloor$ errors, the probability of a correctable error pattern is given by

$$p_{\mathrm{succ}} = \sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} (D-1)^k \binom{n}{k} p_0^{n-k} p_{e\neq 0}^{k}. \tag{31}$$

If an error pattern occurs which cannot be corrected, a logical error is guessed with probability $p_{\mathrm{guess}} = (1-p_{\mathrm{succ}})/D$. Combining the respective success probabilities according to Eqs. (15) and (16) yields the final error distribution on the distributed state.

3.2.2 Error statistics for Fock qudits

Here, we adapt the error analysis of Ref. [33] to error-corrected qudit repeater lines with physical qudits encoded in the Fock basis of a single bosonic mode. In this case, the propagation of errors is more complicated, as the error probabilities of $\mathcal{E}_{\mathrm{appr};D}^{(\eta_0)}$ all differ from each other. A logical CZ gate for the $[\![n,1,d]\!]_D$ quantum polynomial code is transversal in the sense that there are invertible elements $s_1,\ldots,s_n \in \mathbb{Z}/D\mathbb{Z}$ such that $\bigotimes_{i=1}^n \mathrm{CZ}^{s_i}(a_i,b_i)$ acts as a CZ gate between two logical qudits a and b, where $\mathrm{CZ}(a_i,b_i)$ denotes a physical CZ gate from the ith physical qudit of the logical qudit a to the ith qudit of b. For MM qudits, in the previous section, this is not important because, at a depolarizing channel, every nontrivial error occurs with the same probability. Here, however, an $X^{s_i^{-1}e_i}$ error, occurring during the transmission to physical qudit i, will induce a Z^{e_i} error to qudit i of the next logical qudit for all $e_i \in \mathbb{Z}/D\mathbb{Z}$. Employing the error tracking tools of Ref. [33] and taking all relevant error sources into account, we obtain that the probability for an error e_i on the measurement result of qudit i at every repeater station but the first is given by

$$p_{e_i}^{\mathrm{rep}} = p_{s_i^{-1}e_i}^{\mathrm{appr}} (1-f_{\mathrm{G}})^3(1-f_{\mathrm{M}}) + \frac{1}{D}\left[1-(1-f_{\mathrm{G}})^3(1-f_{\mathrm{M}})\right], \tag{32}$$

recall Eq. (28) for the definition of p_{-r}^{appr}. For the first repeater station,

$$p_{e_i\neq 0}^{1.\mathrm{rep}} = \frac{1}{D}\left[1-(1-f_{\mathrm{G}})^2(1-f_{\mathrm{M}})\right] \tag{33}$$

and $p_0^{1.\mathrm{rep}}$ follows from normalization; note that transmission errors do not contribute, as they are of X type for the channel $\mathcal{E}^{(\eta_0)}_{\mathrm{appr};D}$. Similarly, $p_{e_i}^{\mathrm{Bob},X}$ and $p_{e_i}^{\mathrm{Bob},Z}$ are given by

$$p_{e_i\neq 0}^{\mathrm{Bob},X} = \frac{1}{D}\left[1-(1-f_{\mathrm{G}})^2(1-f_{\mathrm{S}})\right], \tag{34}$$
$$\text{and} \quad p_{e_i}^{\mathrm{Bob},Z} = p^{\mathrm{appr}}_{s_i^{-1}e_i}(1-f_{\mathrm{G}})^3(1-f_{\mathrm{S}}) + \frac{1}{D}\left[1-(1-f_{\mathrm{G}})^3(1-f_{\mathrm{S}})\right].$$

This time, let p_{e_i} be either $p_{e_i}^{\mathrm{rep}}$ or $p_{e_i}^{\mathrm{Bob},Z}$ (for $p_{e_i}^{1.\mathrm{rep}}$ and $p_{e_i}^{\mathrm{Bob},X}$ we can continue as in Sec. 3.2.1), and likewise for p_{succ}. Again, the probability of an error pattern $\mathbf{e}=(e_1,\ldots,e_n)$ is given by $p_{\mathbf{e}}=\prod_{i=1}^n p_{e_i}$, but here we cannot simplify this expression using the Hamming weight because the nontrivial error probabilities do not coincide. The probability that a correctable error pattern occurs is given by the sum over all probabilities $p_{\mathbf{e}}$ where $\mathrm{wt}(\mathbf{e})\leq\lfloor(d-1)/2\rfloor$. Since the substitution $e_i' := s_i^{-1}e_i$ does not change the Hamming weight, this sum does not depend on the s_i and can be expressed as

$$p_{\mathrm{succ}} = \sum_{k=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{n}{k}p_0^{n-k}\left(\sum_{\mathbf{r}\in\{1,\ldots,D-1\}^k} p_{\mathbf{r}}\right), \tag{35}$$

where $p_{\mathbf{r}} := p_{r_1}p_{r_2}\ldots p_{r_k}$. By combining terms with equal probability in the inner sum over all combinations of nontrivial error patterns $\mathbf{r}=(r_1,\ldots,r_k)$, we find

$$\sum_{\mathbf{r}\in\{1,\ldots,D-1\}^k} p_{\mathbf{r}} = \sum_{\ell_1+\ldots+\ell_{D-1}=k}\binom{k}{\ell_1,\ldots,\ell_{D-1}}p_1^{\ell_1}\ldots p_{D-1}^{\ell_{D-1}}, \tag{36}$$

where for $\ell_1+\ldots+\ell_{D-1}=k$ the multinomial coefficient is defined as

$$\binom{k}{\ell_1,\ldots,\ell_{D-1}} = \frac{k!}{\ell_1!\ldots\ell_{D-1}!}. \tag{37}$$

Note that $s_1=\ldots=s_n=1$ can be assumed for the evaluation of Eq. (36). Because $p_{e_i}\neq p_{e'_i}$ for $e_i\neq e'_i$, no further simplification can be made through combining coinciding terms. As before, the final error distribution follows from the corresponding success probabilities.

3.3 Optimizing the quantum-repeater gain

In order to identify genuine quantum repeaters, we want to find parameter regions where the quantum-repeater gain, $\Delta = B_{\mathrm{rep}}^{\downarrow} - B_{\mathrm{PLOB}}^{\uparrow}$, takes values which are significantly larger than zero. The first parameter we focus on is the repeater spacing L_0. In Fig. 2, Δ is plotted as a function of L_0 for a quantum repeater line of total length $L=200$km, a distance large enough that Δ takes positive values while the M-mode PLOB-repeaterless bound, $B_{\mathrm{PLOB}}^{\uparrow}\approx 1.44M\times 10^{-4}$, still has a recognizable influence. The selected QECCs have parameters $[\![D,1,(D+1)/2]\!]_D$, i.e., they saturate the quantum singleton bound. Note that this also is the largest possible code distance for which quantum polynomial codes are available at a given dimension D, where D is a prime number. Thus, the considered QECCs are the best available for a given qudit dimension. The prime dimensions $D\in\{13,17,29,37\}$ are selected such that the code distance $d=(D+1)/2$ of the QECC is odd, as this ensures that the number of correctable single qudit errors is $t=(d-1)/2$ (and not $t=(d-2)/2$). For large D, the error correction capabilities perform sufficiently good, such that $H(P)$, the Shannon entropy of the error probability distribution, is almost

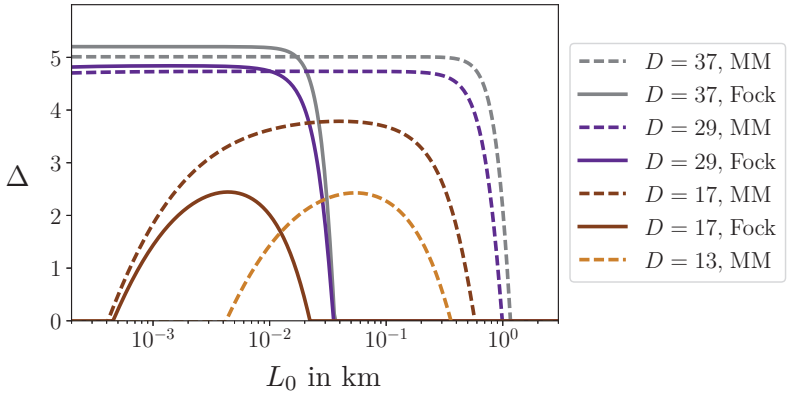

Figure 2: Quantum-repeater gain $\Delta = B^{\downarrow}_{\text{rep}} - B^{\uparrow}_{\text{PLOB}}$ in terms of the spacing L_0 between adjacent repeater stations for a quantum repeater line of total length $L = 200$km. The qudits are encoded with a $[\![D, 1, (D+1)/2]\!]_D$ QECC where the qudit dimension D is color coded. Dashed and solid curves correspond to MM and Fock qudits, respectively. Note that Δ is negative for $D = 13$ Fock qudits because it cannot be ensured that sufficiently many errors can be corrected. We use the error model of Sec. 3.1 with $\alpha = 0.2$dB/km, $f_{\text{M}} = 10^{-2}$, $f_{\text{G}} = 10^{-3}$, and $\gamma = 10^{-2}$dB/ms, i.e., $f_{\text{S}} \approx 2.3 \times 10^{-3}$.

zero, i.e., Alice and Bob have almost perfect knowledge about the state of their qudits. In this saturated regime, where Δ does not significantly change with respect to L_0 over some orders of magnitude, the height of the plateau, $\max_{L_0} \Delta = \log_2(D) - H(P) - B^{\uparrow}_{\text{PLOB}} \approx \log_2(D) - B^{\uparrow}_{\text{PLOB}}$, is, by Eq. (18), larger for Fock qudits than for MM qudits because logical Fock qudits employ only $M = D$ modes while MM qudits require $M = D^2$ modes. Thus, for short distances L_0, the repeaterless quantum capacity is larger for MM qudits. Indeed, the gap between the Fock and the MM plateau is given by

$$B^{\uparrow}_{\text{PLOB}}(\text{MM}) - B^{\uparrow}_{\text{PLOB}}(\text{Fock}) \approx 1.44 \times 10^{-4} \times (D^2 - D) \approx \begin{cases} 0.2 & \text{for } D = 37 \\ 0.1 & \text{for } D = 29 \end{cases} . \tag{38}$$

As L_0 further increases, transmission losses start to significantly deteriorate the error correction procedure, causing a sudden drop of Δ. The largest possible repeater spacing for which the PLOB-repeaterless bound is surpassed is on the order of $L_0 \sim 1$km for MM qudits and $L_0 \sim 0.01 - 0.1$km for Fock qudits, respectively. For Fock qudits, the quantum-repeater gain is more vulnerable to transmission losses because of our worst-case approximation of the corresponding pure-loss channel, recall Eq. (25). On the other hand, for repeater lines with a very small repeater spacing L_0, operational errors (gate and measurement errors) start to play a critical role, as more repeater stations increase the number of error sources, until eventually the lower bound on the repeater's quantum capacity, $B^{\downarrow}_{\text{rep}}$, vanishes and Δ coincides with $-B^{\uparrow}_{\text{PLOB}}$. Since we assume depolarizing noise for operational errors in both encodings, repeaters based on MM and Fock qudits qualitatively show the same behavior for small L_0. For small D, the code distance d is too small, both transmission losses and operational errors deteriorate the error correction procedure, which prohibits the formation of a plateau where $\Delta(L_0)$ is constant. We stress that the repeater spacing L_0 can be raised tremendously if the intended quantum-repeater gain Δ is sub-optimal, e.g., $B^{\downarrow}_{\text{rep}} = 0.9 \times B^{\downarrow\text{max}}_{\text{rep}}$.

In Fig. 3, we display the quantum-repeater gain Δ (color coded) for quantum repeater lines of varying total length L (abscissa) and qudit dimension D (ordinate). We vary D in steps of 4 such that the considered $[\![D, 1, (D+1)/2]\!]_D$ QECCs have an odd code distance d, in between, we interpolate. The corresponding values of L_0 are included in

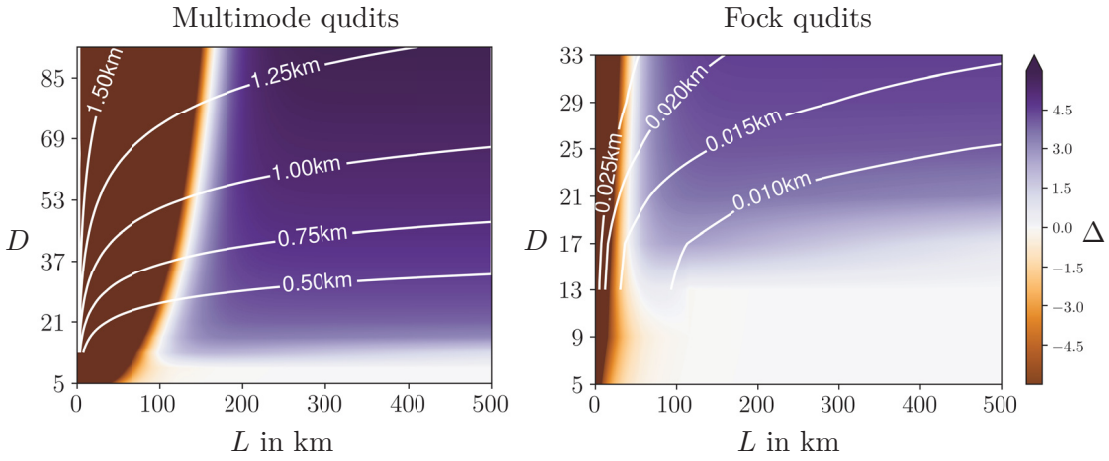

Figure 3: Quantum-repeater gain $\Delta = B^{\downarrow}_{\text{rep}} - B^{\uparrow}_{\text{PLOB}}$ and corresponding repeater spacing L_0 (white lines) for D-dimensional qudits based on MM (left) and Fock (right) encoding, The qudits are encoded with a $[\![D, 1, (D+1)/2]\!]_D$ QECC where the qudit dimension varies in steps of 4 from $D = 5$ to $D = 93$ and $D = 33$ for MM and Fock encoding, respectively. Note that the computational complexity of Eq. (35) limits $D \leq 33$ for Fock qudits. The total distance between Alice and Bob varies from $L = 0$km to $L = 500$km and the repeater spacing $L_0 = L/N$ is adjusted such that $B^{\downarrow}_{\text{rep}} = 0.9 \times B^{\downarrow\text{max}}_{\text{rep}}$. We use the error model of Sec. 3.1 with $\alpha = 0.2$dB/km, $f_{\text{M}} = 10^{-2}$, $f_{\text{G}} = 10^{-3}$, and $\gamma = 10^{-2}$dB/ms.

Fig. 3 via white contour lines. For MM and Fock qudits, respectively, the repeater spacing is on the order of $L_0 \sim 1$km and $L_0 \sim 0.01$km, respectively. If the total length L of the repeater line is shortened, transmission losses become less important and operational errors begin to dominate. Thus, to reach $B^{\downarrow}_{\text{rep}} = 0.9 \times B^{\downarrow\text{max}}_{\text{rep}}$, the spacing L_0 between two adjacent repeater stations is increased, as this decreases the number of operational error sources. The spacing L_0 also increases with D because QECCs with a higher code distance $d = (D+1)/2$ can correct more errors.

We find three distinct regions in Fig. 3, each with a typical signature: (i) For small L, the PLOB-repeaterless bound cannot be surpassed, i.e., $\Delta < 0$. (ii) For large L and a large code distance $d = (D+1)/2$ we observe $\Delta > 0$. (iii) For large L and small d we find $\Delta \approx 0$. We now discuss the signatures of these three regions:

(i) $[\Delta < 0]$ At the brown region on the left, the M-mode PLOB-repeaterless bound is much larger than $\log_2(D) \geq B^{\downarrow}_{\text{rep}}$. Asymptotically, it is even unbounded,

$$B^{\uparrow}_{\text{PLOB}} = -M \times \log_2(1-\eta) \xrightarrow{L\to 0} \infty. \tag{39}$$

As logical $[\![D, 1, (D+1)/2]\!]_D$ MM qudits are encoded into $M = D^2$ modes, this region extends to longer total lengths L of the repeater line if the qudit dimension D is larger, e.g., $L(\Delta < 0, D = 13) \lesssim 100$km and $L(\Delta < 0, D = 85) \lesssim 150$km. For Fock qudits, which only require $M = D$ modes, this effects is barely noticeable and $L(\Delta < 0) \lesssim 50$km for all D.

(ii) $[\Delta > 0]$ At the purple region on the upper right, quantum repeaters can surpass the PLOB-repeaterless bound because $B^{\uparrow}_{\text{PLOB}} \approx 0$ while $B^{\downarrow}_{\text{rep}} > 0$. The quantum-repeater gain $\Delta = B^{\downarrow}_{\text{rep}} - B^{\uparrow}_{\text{PLOB}} \approx \log_2(D) - H(P)$ increases (for a fixed L) in D if the distance $d = (D+1)/2$ of the QECC is large enough, as this causes $H(P) \approx 0$. Genuine MM quantum repeaters are possible for $D \geq 13$, whereby the minimal repeater length increases with the number of modes $M = D^2$, as already discussed for region (i). For quantum repeaters with Fock encoding, the PLOB-repeaterless

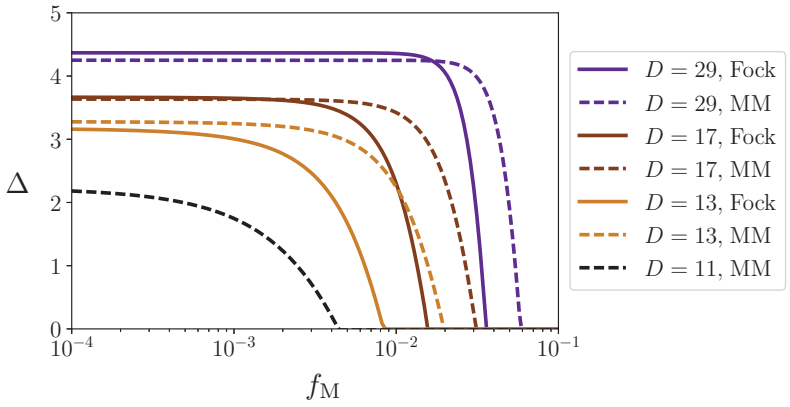

Figure 4: The quantum-repeater gain Δ in terms of the measurement error rate f_{M}. The other error parameters are fixed to $\alpha = 0.2\mathrm{dB/km}$, $f_{\mathrm{G}} = 10^{-3}$, and $\gamma = 0.01\mathrm{dB/ms}$, i.e., $f_{\mathrm{S}} \approx 2.3 \times 10^{-3}$. The qudits are encoded with a $[\![D, 1, (D+1)/2]\!]_D$ QECC. The repeater line has a total length of $L = 200\mathrm{km}$ and the repeater spacing $L_0 = L/N$ is adjusted such that $B^{\downarrow}_{\mathrm{rep}} = 0.9 \times B^{\downarrow\mathrm{max}}_{\mathrm{rep}}$.

bound can be outperformed for $D \geq 17$ and $L > 50\mathrm{km}$. For $D = 13$, we observe a small quantum-repeater gain $\Delta \in (0.1, 0.5)$ for quantum repeater lines with a total length L between 60km and 110km.

(iii) [$\Delta \approx 0$] At the white region on the lower right, the total length L is too large and the code distance d is too small such that $B^{\uparrow}_{\mathrm{PLOB}} \approx 0$ and $B^{\downarrow}_{\mathrm{rep}} = 0$, respectively. Recall that we consider $[\![D, 1, (D+1)/2]\!]_D$ quantum polynomial codes, as they have the highest code distance for a given dimension, as well as transversal CZ gates and transversal X measurements. For $D \leq 9$, we find $B^{\downarrow}_{\mathrm{rep}} = 0$ which implies $\Delta \approx 0$.

Let us summarize what can be learned from Figs. 2 and 3. Using higher-dimensional qudits, it is possible to reach a larger quantum-repeater gain because the ideal quantum capacity of the quantum repeater is given by $\log_2(D)$. In many cases, this optimum can be reached by an appropriate choice of L_0. Since the code distance of the best known QECCs also grows with the qudits' dimension, a side effect of higher-dimensional qudits is the possibility to increase the distance L_0 between two neighboring repeater stations. For MM qudits, L_0 is two orders of magnitude larger than for Fock qudits, which could be due to our worst-case Pauli-approximation of the pure-loss channel for Fock qudits. Within our error model, Fock and MM quantum repeaters can surpass the PLOB-repeaterless bound for $L > 50\mathrm{km}$ and $L > 100 - 150\mathrm{km}$, respectively. MM repeaters require a larger total length because the PLOB-repeaterless bound is higher for a larger number of modes.

3.4 Influence of operational errors on the quantum-repeater gain

As it is easier to implement a $[\![D, 1, (D+1)/2]\!]_D$ QECC for smaller qudit dimension D, it is desirable to lower the demands on error correction. One way to achieve this is the improvement of operational error rates. As we have shown in Sec. 3.2, operational errors mainly originate from intermediate repeater stations, where gate and measurement errors enter via $(1 - f_{\mathrm{G}})^3$ and $(1 - f_{\mathrm{M}})$, respectively, recall Eqs. (29) and (32). Thus, gate errors affect the quantum-repeater gain three times as large as measurement errors do, but they otherwise lead to the same qualitative behavior of Δ. Hence, we restrict the investigation of the influence of operational errors to the measurement error rate f_{M} and fix $f_{\mathrm{G}} = 10^{-3}$, as before. Figure 4 shows the quantum-repeater gain as a function of the measurement error rate f_{M}. We observe a similar pattern for all curves: At low error rates $f_{\mathrm{M}} \leq 10^{-3}$ the

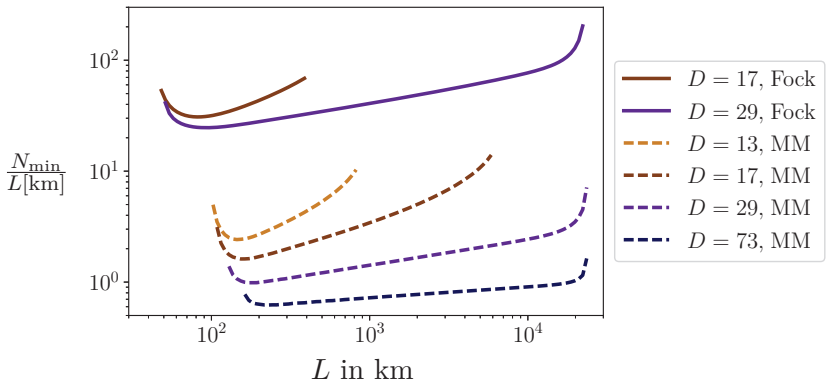

Figure 5: The minimal number of repeater stations per km for which the PLOB-repeaterless bound can be just surpassed by a quantum repeater line of total length L with MM and Fock qudits encoded by a $[\![D, 1, (D+1)/2]\!]_D$ QECC. The error parameters are $\alpha = 0.2\mathrm{dB/km}$, $f_{\mathrm{M}} = 10^{-2}$, $f_{\mathrm{G}} = 10^{-3}$, and $\gamma = 10^{-2}\mathrm{dB/ms}$.

quantum-repeater gain Δ is almost constant. As f_{M} increases, the smaller the dimension D, the sooner the corresponding quantum-repeater gain drops to zero, as fewer errors can be corrected by the QECC. In terms of quantum-repeater gain and in direct comparison, the MM encoding is more tolerant towards measurement errors than the Fock encoded repeater line. As expected, lower operational error rates allow genuine quantum repeaters with smaller dimension D, as fewer errors need to be corrected. In this range of f_{M}, the smallest dimension for which genuine quantum repeaters are possible is $D = 11$ with MM qudits.

3.5 Estimate of resources

For a resource-efficient use of quantum repeaters it is crucial to identify cost-saving candidates. Naturally, the costs of developing and maintaining a single repeater station will increase with D, as a $[\![D, 1, (D+1)/2]\!]_D$ QECC is employed. However, higher-dimensional qudits have the advantage of better error correction capabilities, thus, the number of necessary repeater stations is lower. Table 1 provides the minimal requirement on the number

	D	13	17	29	73
MM	$N_{\min}$	325	228	155	118
	$L(N_{\min})$	120km	130km	140km	170km
Fock	$N_{\min}$	-	2070	1705	?
	$L(N_{\min})$		56km	60km	

Table 1: The minimal number $N_{\min}$ of repeater stations for which the PLOB-repeaterless bound can be just surpassed by a quantum repeater line of a total length $L(N_{\min})$, see also Fig. 5. We use the error model of Sec. 3.1 with $\alpha = 0.2\mathrm{dB/km}$, $f_{\mathrm{M}} = 10^{-2}$, $f_{\mathrm{G}} = 10^{-3}$, and $\gamma = 10^{-2}\mathrm{dB/ms}$. For $D = 13$ Fock qudits, the PLOB-repeaterless bound is not surpassed, and for $D = 73$ Fock qudits, the corresponding minimum cannot be evaluated due to the computational complexity of Eq. (35).

of repeater stations of a genuine error-corrected qudit repeater.

A relevant figure of merit to compare different quantum repeater lines is the minimum number of repeater stations per unit length $N_{\min}/L$, which we plot in Fig. 5 as a function of the total length L for various encodings. All curves qualitatively show the same behavior: For very small L, the PLOB-repeaterless bound is not surpassed, as direct quantum com-

munication is still possible. Eventually, with increasing L, the PLOB-repeaterless bound has dropped to a quantum capacity which can be surpassed by $B^{\downarrow}_{\text{rep}}$. At this minimal total length L_{min}, the curves in Fig. 5 begin. For Fock qudits, L_{min} is smaller than for MM qudits because fewer modes are used, consistent with previous observations above. If L is slightly above L_{min}, the PLOB-repeaterless bound $B^{\uparrow}_{\text{PLOB}}$ quickly approaches zero. Thus, the lower bound on the quantum capacity of the repeater, $B^{\downarrow}_{\text{rep}} = \log_2(D) - H(P)$, is allowed to decrease as well, which leads to the possibility of setting up the quantum repeater with fewer repeater stations per unit length. This explains the initial drop of the curves for $L \gtrsim L_{\text{min}}$. At some point, the global minima from Tab. 1 are reached. For larger L, the regime $B^{\uparrow}_{\text{PLOB}} \approx 0$ is entered. Since we consider $0 \lesssim \Delta$, this implies $H(P) \lesssim \log_2(D)$. That is, the number of repeater stations is adjusted such that the Shannon entropy of the error distribution on the distributed state is kept slightly below $\log_2(D)$. If, in this regime, L is increased, the amount of error correction overhead has to be adjusted accordingly. Therefore, the minimal number of repeater stations per unit length increases with L. The (log-log) slope of the corresponding curves in this intermediate region decreases with D because QECCs with a larger code distances can more readily cope with the additional transmission losses. For $D = 73$ MM qudits, the code distance $d = 37$ of the QECC is large enough such that the curve just barely grows. Eventually, so many storage errors of Alice's quantum memory have accumulated that the pseudothreshold[1] of the respective QECC is reached. In that region, storage errors strongly influence $H(P)$ until the condition $H(P) \lesssim \log_2(D)$ cannot be fulfilled for any choice of N/L. This explains the sudden growth of the curves in Fig. 5 for large values of L and is clearly visible in Fig. 6.

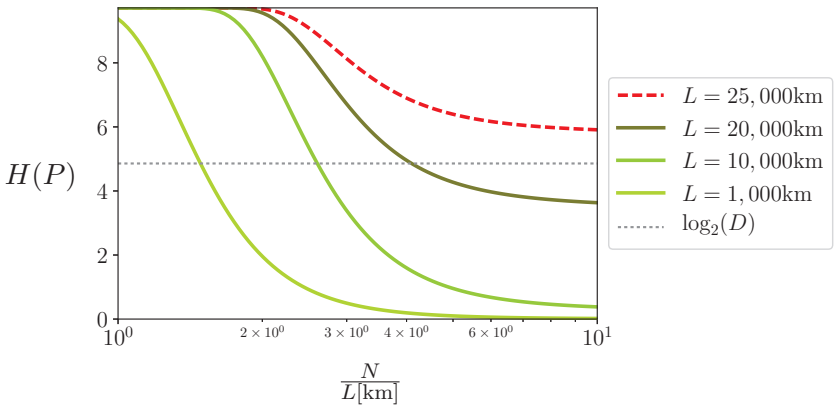

Figure 6: The Shannon entropy $H(P)$ of the error distribution of a state distributed by a $[\![29, 1, 15]\!]_{29}$ error-corrected MM quantum repeater for different total lengths L as a function of the inverse repeater spacing $1/L_0 = N/L$. Perfect error correction means $H(P) = 0$. For $L \leq 20,000$km, one can reach $H(P) \lesssim \log_2(D)$ by an adjustment of N/L. Since the global minimum of $H(P)$ grows in L, the value of N/L where $\log_2(D)$ intersects $H(P)$ exponentially increases. For $L = 25,000$km, $B^{\downarrow}_{\text{rep}} = \max\{\log_2(D) - H(P), 0\}$ is zero for any choice of N/L, i.e., the quantum-repeater gain Δ is negative. As in Fig. 5, we use $\alpha = 0.2$dB/km, $f_{\text{M}} = 10^{-2}$, $f_{\text{G}} = 10^{-3}$, and $\gamma = 10^{-2}$dB/ms.

[1]The (code capacity) pseudothreshold of a QECC is the error rate at which the physical error rate is equal to the logical error rate, in Eq. (31) with $f_{\text{S}} = p_{e\neq 0}$. For $[\![29, 1, 15]\!]_{29}$ and $[\![73, 1, 37]\!]_{73}$ QECCs, our calculations show that this pseudothreshold is approximately 20%. By Eq. (21), $f_{\text{S}} = 0.2$ is reached for $L \approx 20,000$km since $\gamma = 10^{-2}$dB/ms.

In conclusion of this subsection, we observe that for our error model and existing QECCs, genuine error-corrected qudit repeater lines require at least about 10^2 and 10^3 repeater stations for MM and Fock qudits, respectively. For a total length L between 10^2km and 10^4km, the PLOB-repeaterless bound can be surpassed while the minimum number of repeater stations per unit length, $N_{\min}/L$, gradually increases in L. This increase is less pronounced for quantum repeaters with better error-correcting capabilities, i.e., for a higher qudit dimension D.

4 Conclusion and Outlook

In this paper, we have analyzed the applicability of error-corrected quantum repeaters based on higher-dimensional qudits as long-term candidates of a quantum communication infrastructure. By making explicit how the PLOB-repeaterless bound relates to the encoding of abstract qudits into photonic modes, we obtain a bound on the capacity of the quantum repeater using the Shannon entropy of the error distribution of the final state. We defined the quantum repeater-gain as a figure of merit and used it to identify genuine quantum repeaters by a systematic analysis of its dependency on a variety of parameters.

We derived an analytical solution of the quantum-repeater gain for error-corrected, one-way qudit repeaters based on two different types of physical encoding: Fock encoding, where each qudit is encoded into a single photonic mode; and multimode encoding, where each computational basis state of a qudit has its own mode. While Fock encoding is interesting from a theoretical perspective, as it allows to surpass the PLOB-repeaterless bound over shorter distances by harnessing higher photon numbers of the photonic mode, multimode qudits pose the more realistic way of implementing error-corrected qudit repeaters, as they are more readily available in the form of e.g., time-bin qudits, temporal modes, and modes of orbital angular momentum. We found that genuine quantum repeaters are feasible if the distance L_0 between adjacent repeater stations is on the order of 1km for multimode encoding, independent of its total length. For Fock qudits, we can only prove that $L_0 \sim 10$m is sufficient however, we expect that this is due to our worst-case approximation of the pure-loss channel and that Fock repeaters can also surpass the PLOB-repeaterless bound with $L_0 \sim 100\text{m} - 1\text{km}$.

We have shown that an improvement of operational error rates makes it possible to decrease the necessary number of physical qudits per logical qudit, as well as the qudit dimension. For realistic error rates, the smallest qudit dimension with which a genuine quantum repeater could be realized within our error model is $D = 13$ and $D = 11$ for Fock and MM qudits, respectively. Although theoretical proposals for the generation of Fock states with an arbitrary photon number exist [71], high-quality Fock states have experimentally only been realized up to four photons, i.e., $D_{\text{Fock}} \leq 5$, and no significant improvement was made over the last 10-15 years [72,73]. For MM qudits, on the other hand, the state-of-the-art continuously progresses: Qudits based on temporal modes, orbital angular momentum and time bin can be realized up to $D_{\text{TM}} \leq 7$ [48], $D_{\text{OAM}} \lesssim 100$ [52], and $D_{\text{time-bin}} \lesssim 10^5$ [45, 46], respectively. An experimental challenge that has to be overcome to realize the here-considered protocol is the development of high-fidelity, two-photon controlled-phase gates, as well as the preparation of multipartite entangled photons, in particular in the logical $|+\rangle$ state of a quantum polynomial code.

While near-term candidates such as the so-called single photon scheme based on a nitrogen vacancy architecture [23] and twin-field quantum key distribution [24-26] are within experimental reach, they are spatially restricted to tens and hundreds of kilometers, respectively. As we showed here, error-corrected qudit repeaters, on the other hand, have

the potential to overcome the PLOB-repeaterless bound over length scales on the same order of magnitude as the Trans-Siberian railroad, i.e., 10^4km. These length scales are sufficient to connect any two points on earth.

Here, we have focused on subspace quantum error-correcting codes (QECCs) [55], in particular, quantum polynomial codes [56-59]. However, recently it was shown that subsystem QECCs can have an advantage in fighting leakage errors in ion trap quantum computers [74]. It would be interesting to find out whether subsystem codes, such as Bacon-Shor codes [75-77], subsystem surface codes [78], 2D compass codes [79], and optimal generalized Bacon-Shor codes [80], also have an advantage in coping with photon losses in an error-corrected quantum repeater protocol.

Acknowledgments

The authors thank Federico Grasselli for helpful discussions and Eric Sabo for feedback on the manuscript. The authors acknowledge support from the Federal Ministry of Education and Research (BMBF, Project Q.Link.X).

References

[1] M. Riedel, D. Binosi, R. Thew, and T. Calarco, *The European quantum technologies flagship programme*, Quantum Sci. Technol. **2,** 030501 (2017).

[2] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. Riedel, P. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F. Wilhelm, *The quantum technologies roadmap: a European community view*, New J. Phys. **20,** 080201 (2018).

[3] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead*, Science **362,** 6412 (2018).

[4] V. Giovannetti, S. Lloyd, and L. Maccone, *Quantum-enhanced positioning and clock synchronization*, Nature **412,** 417 (2001).

[5] M. Christandl and S. Wehner, *Quantum Anonymous Transmissions*, ASIACRYPT 2005, 217-235 (2005).

[6] D. Gottesman, T. Jennewein, and S. Croke, *Longer-Baseline Telescopes Using Quantum Repeaters*, Phys. Rev. Lett. **109,** 070503 (2012).

[7] E. Khabiboulline, J. Borregaard, K. De Greve, and M. Lukin, *Nonlocal Optical Interferometry with Quantum Networks*, arXiv:1809.01659 [quant-ph] (2018).

[8] C. Bennett, G. Brassard, *Public Key Distribution and Coin Tossing*, IEEE Proc. Int. Conf. Computers, Systems and Signal Processing, 175-179 (1984).

[9] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67,** 661 (1991).

[10] D. Bruß, *Optimal Eavesdropping in Quantum Cryptography with Six States*, Phys. Rev. Lett. **81,** 3018 (1998).

[11] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussiŕes, M. Li, D. Nolan, A. Martin, and H. Zbinden, *Secure Quantum Key Distribution over 421 km of Optical Fiber*, Phys. Rev. Lett. **121,** 190502, (2018).

[12] M. Takeoka, S. Guha, and M. Wilde, *Fundamental rate-loss tradeoff for optical quantum key distribution*, Nat. Comm. **5,** 5235 (2014).

[13] M. Christandl and A. Müller-Hermes, *Relative Entropy Bounds on Quantum, Private and Repeater Capacities*, Commun. Math. Phys. **353,** 821 (2017).

[14] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental limits of repeaterless quantum communications*, Nat. Commun. **8,** 15043 (2017).

[15] H. Briegel, W. Dür, J. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81,** 5932 (1998).

[16] P. van Loock, T. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. Munro, and Y. Yamamoto, *Hybrid Quantum Repeater Using Bright Coherent Light*, Phys. Rev. Lett. **96,** 240501 (2006).

[17] L. Jiang, J. Taylor, K. Nemoto, W. Munro, R. Van Meter, and M. Lukin, *Quantum repeater with encoding*, Phys. Rev. A **79,** 032325 (2009).

[18] A. Fowler, D. Wang, C. Hill, T. Ladd, R. Van Meter, and L. Hollenberg, *Surface Code Quantum Communication*, Phys. Rev. Lett. **104,** 180503 (2010).

[19] S. Muralidharan, J. Kim, N. Lütkenhaus, M Lukin, and L. Jiang, *Ultrafast and Fault-Tolerant Quantum Communication across Long Distances*, Phys. Rev. Lett. **112,** 250501 (2014).

[20] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. Lukin and L. Jiang, *Optimal architectures for long distance quantum communication*, Sci Rep. **6,** 20463 (2016).

[21] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, *Overcoming lossy channel bounds using a single quantum repeater node*, Appl. Phys. B 112: 96 (2016).

[22] F. Rozpędek., K. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, Quantum Sci. Technol. **3,** 034002 (2018).

[23] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, *Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission*, Phys. Rev. A **99,** 052330 (2019).

[24] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, *Overcoming the rate-distance limit of quantum key distribution without quantum repeaters*, Nature **557,** 400 (2018).

[25] M. Curty, K. Azuma, and H. Lo, *Simple security proof of twin-field type quantum key distribution protocol*, arXiv:1807.07667 [quant-ph] (2018).

[26] F. Grasselli and M. Curty, *Practical decoy-state method for twin-field quantum key distribution*, arXiv:1902.10034 [quant-ph] (2019).

[27] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, *Experimental quantum key distribution beyond the repeaterless secret key capacity*, Nat. Photonics **13,** 334 (2019).

[28] S. Wang, D. He, Z. Yin, F. Lu, C. Cui, W. Chen, Z. Zhou, G. Guo, and Z. Han, *Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System*, Phys. Rev. X **9,** 021046 (2019).

[29] X. Zhong, J. Hu, M. Curty, L. Qian, and H. Lo, *Proof-of-principle experimental demonstration of twin-field type quantum key distribution*, arXiv:1902.10209 [quant-ph] (2019).

[30] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, *Entanglement distribution beyond qubits or: How I stopped worrying and learned to love the noise*, arXiv:1904.01552 [quant-ph] (2019).

[31] S. Muralidharan, C. Zou, L. Li, J. Wen, and L. Jiang, *Overcoming erasure errors with multilevel systems*, New J. Phys. **19,** 013026 (2017).

[32] S. Muralidharan, C. Zou, L. Li, and L. Jiang, *One-way quantum repeaters with quantum Reed-Solomon codes*, Phys. Rev. A **97,** 052316 (2018).

[33] D. Miller, T. Holz, H. Kampermann, and D. Bruß, *Propagation of generalized Pauli errors in qudit Clifford circuits*, Phys. Rev. A **98,** 052316 (2018).

[34] M. Bergmann and P. van Loock, *Hybrid quantum repeater for qudits*, Phys. Rev. A **99,** 032349 (2019).

[35] S. Abruzzo, S. Bratzik, N. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, *Quantum repeaters and quantum key distribution: Analysis of secret-key rates*, Phys. Rev. A **87,** 052315 (2013).

[36] S. Bratzik, H. Kampermann, and D. Bruß, *Secret key rates for an encoded quantum repeater*, Phys. Rev. A **89,** 032335 (2014).

[37] M. Epping, H. Kampermann, and D. Bruß, *On the error analysis of quantum repeaters with encoding*, Appl. Phys. B 122: 54 (2016).

[38] M. Epping, H. Kampermann, and D. Bruß, *Large-scale quantum networks based on graphs*, New J. Phys. **18,** 53036 (2016).

[39] M. Epping, H. Kampermann, and D. Bruß, *Robust entanglement distribution via quantum network coding*, New J. Phys. **18,** 103052 (2016).

[40] K. Vollbrecht and M. Wolf, *Efficient distillation beyond qubits*, Phys. Rev. A **67,** 012303 (2003).

[41] S. Braunstein and P. van Loock, *Quantum information with continuous variables*, Rev. Mod. Phys. **77,** 513 (2005).

[42] C. Weedbrook, S. Pirandola, R. García-Patrón, N. Cerf, T. Ralph, J. Shapiro, and S. Lloyd, *Gaussian quantum information*, Rev. Mod. Phys. **84,** 621 (2012).

[43] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, *Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication*, Phys. Rev. Lett. **82,** 2594 (1999).

[44] H. de Riedmatten, I. Marcikic, H. Zbinden, and N. Gisin, *Creating high dimensional time-bin entanglement using mode-locked lasers*, Quant. Inf. Comp. **2,** 425 (2002).

[45] T. Zhong, H. Zhou, R. Horansky, C. Lee, V. Verma, A. Lita, A. Restelli, J. Bienfang, R. Mirin, T. Gerrits, S. Nam, F. Marsili, M. Shaw, Z. Zhang, L. Wang, D. Englund, G. Wornell, J. Shapiro, and F. Wong, *Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding*, New J. Phys. **17,** 022002 (2015).

[46] N. Montaut, O. Magaña-Loaiza, T. Bartley, V. Verma, S. Nam, R. Mirin, C. Silberhorn, and T. Gerrits, *Compressive characterization of telecom photon pairs in the spatial and spectral degrees of freedom*, Optica **5,** 1418 (2018).

[47] B. Brecht, D. Reddy, C. Silberhorn and M. Raymer, *Photon Temporal Modes: A Complete Framework for Quantum Information Science*, Phys. Rev. X **5,** 041017 (2015).

[48] V. Ansari, J. Donohue, M. Allgaier, L. Sansoni, B. Brecht, J. Roslund, N. Treps, G. Harder, and C. Silberhorn, *Tomography and Purification of the Temporal-Mode Structure of Quantum Light*, Phys. Rev. Lett. **120,** 213601 (2018).

[49] L. Allen, M. Beijersbergen, R. Spreeuw, and J. Woerdman, *Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes*, Phys. Rev. A **45,** 8185 (1992).

[50] G. Calvo, A. Picón, and E. Bagan, *Quantum field theory of photons with orbital angular momentum*, Phys. Rev. A **73,** 013805 (2006).

[51] W. Plick, M. Krenn, R. Fickler, S. Ramelow, and A. Zeilinger, *Quantum orbital angular momentum of elliptically symmetric light*, Phys. Rev. A **87,** (2013).

[52] M. Krenn, M. Malik, M. Erhard, and A. Zeilinger, *Orbital angular momentum of photons and the entanglement of Laguerre–Gaussian modes*, Phil. Trans. R. Soc. A **375:** 20150442 (2017).

[53] E. Knill, *Group Representations, Error Bases and Quantum Codes*, Technical Report LAUR-96-2807, Los Alamos National Laboratory, arXiv:9608049 [quant-ph] (1996).

[54] D. Gottesman, *Fault-Tolerant Quantum Computation with Higher-Dimensional Systems*, Chaos Solitons Fractals **10,** 1749-1758 (1999).

[55] D. Lidar and T. Brun, *Quantum Error Correction*, Cambridge University Press (2013).

[56] R. Cleve, D. Gottesman and H. Lo, *How to share a quantum secret*, Phys. Rev. Lett. **83,** 648 (1999).

[57] D. Aharonov and M. Ben-Or, *Fault-Tolerant Quantum Computation with Constant Error Rate*, SIAM J. Comput. **38(4),** 1207 (2008).

[58] A. Ketkar, A. Klappenecker, S. Kumar and P. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inf. Theory, **52(11),** 4892 (2006).

[59] A. Cross, *Fault-tolerant quantum computer architectures using hierarchies of quantum error-correcting codes*, MIT 1721.1/44407 (2008).

[60] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74,** 145 (2002).

[61] R. Hadfield, *Single-photon detectors for optical quantum information applications*, Nat. Photonics **3,** 696 (2009).

[62] B. Hacker, S. Welte, G. Rempe, and S. Ritter, *A photon–photon quantum gate based on a single atom in an optical resonator* Nature **536,** 193 (2016).

[63] G. Alber, A. Delgado, N. Gisin, and I. Jex, *Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces*, J. Phys. A: Math. Gen. **34** 8821 (2001).

[64] R. Heeres, B. Vlastakis, E. Holland, S. Krastanov, V. Albert, L. Frunzio, L. Jiang, and R. Schoelkopf, *Cavity State Manipulation Using Photon-Number Selective Phase Gates*, Phys. Rev. Lett. **115,** 137002 (2015).

[65] Y. Cho, G. Campbell, J. Everett, J. Bernu, D. Higginbottom, M. Cao, J. Geng, N. Robins, P. Lam, and B. Buchler, *Highly efficient optical quantum memory with long coherence time in cold atoms*, Optica **3,** 100 (2016).

[66] P. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Yao, S. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. Twitchen, J. Cirac, and M. Lukin, *Room-Temperature Quantum Bit Memory Exceeding One Second*, Sci Rep. **336,** 6086 1283 (2012).

[67] M. Abobeih, J. Cramer, M. Bakker, N. Kalb, M. Markham, D. Twitchen, and T. Taminiau, *One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment*, Nat. Comm. **9,** 2552 (2018).

[68] C. Bradley, J. Randall, M. Abobeih, R. Berrevoets, M. Degen, M. Bakker, M. Markham, D. Twitchen, T. Taminiau, *A 10-qubit solid-state spin register with quantum memory up to one minute*, arXiv:1905.02094 [quant-ph] (2019).

[69] Y. Wang, M. Um, J. Zhang, S. An, M. Lyu, J. Zhang, L. Duan, D. Yum, and K. Kim, *Single-qubit quantum memory exceeding ten-minute coherence time*, Nat. Photonics **11,** 646 (2017).

[70] M. Körber, O. Morin, S. Langenfeld, A. Neuzner, S. Ritter, and G. Rempe, *Decoherence-protected memory for a single-photon qubit*, Nat. Photonics **12,** 18 (2018).

[71] K. Brown, K. Dani, D. Stamper-Kurn, and K. Whaley, *Deterministic optical Fock-state generation*, Phys. Rev. A **67,** 043818 (2003).

[72] E. Waks, E. Diamanti, and Y. Yamamoto, *Generation of photon number states*, New J. Phys. **8,** 4 (2006).

[73] J. Tiedau, T. Bartley, G. Harder, A. Lita, S. Nam, T. Gerrits, and C. Silberhorn, *On the scalability of parametric down-conversion for generating higher-order Fock states*, arXiv:1901.03237 [quant-ph] (2019).

[74] N. Brown, M. Newman, and K. Brown, *Handling Leakage with Subsystem Codes*, arXiv:1903.03937 [quant-ph] (2019).

[75] P. Shor, *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52,** R2493(R) (1995).

[76] D. Bacon, *Operator quantum error-correcting subsystems for self-correcting quantum memories*, Phys. Rev. A **73,** 012340 (2006).

[77] P. Aliferis and A. Cross, *Subsystem Fault Tolerance with the Bacon-Shor Code*, Phys. Rev. Lett. **98,** 220502 (2007).

[78] S. Bravyi, G. Duclos-Cianci, D. Poulin, and M. Suchara, *Subsystem surface codes with three-qubit check operators*, Quant. Inf. Comp. **13,** 963 (2013).

[79] M. Li, D. Miller, M. Newman, Y. Wu, and K. Brown, *2D Compass Codes*, Phys. Rev. X **9,** 021041 (2019).

[80] T. Yoder, *Optimal quantum subsystem codes in 2-dimensions*, Phys. Rev. A **99,** 052333 (2019).

Appendix E

A Genuine Multipartite Bell Inequality for Device-independent Conference Key Agreement

Title:	A Genuine Multipartite Bell Inequality for Device-independent Conference Key Agreement
Authors:	Timo Holz, Hermann Kampermann, and Dagmar Bruß
Journal:	Physical Review Letters
Impact factor:	9.227 (2019)
Date of submission:	31 October 2019
Publication status:	Submitted
Contribution by TH:	First author (input approx. 85%)

This publication corresponds to Ref. [HKB19]. A summary of the results is presented in Chap. 7. The general research objective was established in collaboration with my co-authors and frequently discussed with them. Based on a preceding publication, Ref. [HMKB19], App. C, the concept of a Bell inequality for DIQKD was put forward by me. I discovered the resulting family of genuine multipartite Bell inequalities and derived its final form. The proof of the classical bounds of the inequality, was conceptualized by me and I carried out the majority of the analytical proof. Furthermore, I characterized the remaining properties of the Bell inequality discussed in the article and performed the corresponding calculations myself. Exceptions are Eqs. (9) and (10) in the article which were derived by HK based on Eq. (41) that was established by me. For the numerical calculations of the secret-key rates, HK provided a program for the bipartite case which was generalized to the multipartite case by me. Moreover, I developed the remaining programs, carried out all numerical computations, and created all plots and figures in the article. I wrote the entire manuscript which was proofread and improved by my co-authors.

A Genuine Multipartite Bell Inequality for Device-independent Conference Key Agreement

Timo Holz,* Hermann Kampermann, and Dagmar Bruß
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany
(Dated: October 28, 2019)

In this work, we present a new class of genuine multipartite Bell inequalities, that is particularly designed for multipartite device-independent (DI) quantum key distribution (QKD), also called DI conference key agreement. We prove the classical bounds of this inequality, discuss how to maximally violate it and show its usefulness by calculating achievable conference key rates via the violation of this Bell inequality. To this end, semidefinite programming techniques based on [Nat. Commun. 2, 238 (2011)] are employed and extended to the multipartite scenario. Our Bell inequality represents a nontrivial multipartite generalization of the Clauser-Horne-Shimony-Holt inequality and is motivated by the extension of the bipartite Bell state to the n-partite Greenberger-Horne-Zeilinger state. For DIQKD, we suggest an honest implementation for any number of parties and study the effect of noise on achievable asymptotic conference key rates.

Introduction.— Among a variety of quantum technology applications [1–3], quantum key distribution (QKD) is one of the most prominent concepts, in particular for multiple parties in a quantum network [4]. Early proposed QKD protocols [5–7] have high demands on experimental assumptions which are difficult to guarantee. Device-independent (DI) QKD aims at establishing a secret key without making detailed assumptions about the inner working processes of the quantum devices [8–12]. The security of DIQKD protocols is based on a loophole-free violation of a Bell inequality [11–18]. A connection between the DI secret-key rate and the violation of the associated Clauser-Horne-Shimony-Holt (CHSH) inequality [19] was established in [11, 12] for the bipartite setting. In Ref. [18], a protocol to generate a secret key among n parties, called DI conference key agreement (DICKA) was introduced, which relies on the violation of the Parity-CHSH inequality. Hereby, nonlocality is certified via an effective Bell test of two parties depending on the measurement results of the remaining ones.

Not all multipartite Bell inequalities are suitable for DIQKD because measurements and quantum resources are required that allow a sufficiently large Bell-inequality violation and at the same time provide highly correlated measurement results among all parties. Moreover, at least one party has to use one measurement for key generation *and* for the Bell test, to detect a potential tampering of the devices. Achieving these requirements simultaneously should therefore be guaranteed by the very structure of the Bell inequality. This constraint disqualifies several known Bell inequalities as a viable option for a Bell test in DIQKD with certain quantum states. For instance, the archetypical n-partite Greenberger-Horne-Zeilinger (GHZ) state [20] can maximally violate the n-partite Mermin-Ardehali-Belinskiĭ-Klyshko (MABK) inequality [21–23] and also the Bell inequality most recently introduced in Ref. [24]. However, as proven in Ref. [4], perfectly correlated measurement results with the n-GHZ state can only be obtained if and only if all parties measure in the σ_z eigenbasis, which then excludes maximum violation of the Bell inequalities in Refs. [21–24], see [25]. In this work, we specifically design a novel class of multipartite Bell inequalities that fulfills the aforementioned conditions. We prove the classical bounds of this inequality and discuss some features of it, in particular how to obtain a large Bell-inequality violation. To demonstrate the usefulness of our Bell inequality, we quantify achievable conference key rates based on its violation. For this, we use the approach of Ref. [13], which employs the Navasqués-Pironio-Acin (NPA) hierarchy [26, 27], together with a multipartite constraint. We propose an honest implementation for a multipartite DIQKD protocol and briefly discuss how noise affects the achievable asymptotic DI secret conference key rates.

A genuine multipartite Bell inequality.— We impose the following condition on the Bell test: Its structure has to be such that it allows to simultaneously yield highly correlated measurement results and sufficiently large Bell-inequality violation for certain quantum states. These are crucial ingredients in any DIQKD protocol.

Consider a setup of n parties, called Alice and Bob$^{(j)}$ for $j \in \{2,\dots,n\} =: [n]$, cf. Fig. 1. Let each party measure two dichotomic observables A_x and $B^{(j)}_{y^{(j)}}$, with inputs $x, y^{(j)} \in \{0,1\}$. We define a set that contains all ordered possibilities to choose l out of the labels $\{2,\dots,n\}$ for the Bobs:

$$\mathcal{S}_l^{(n)} \coloneqq \Big\{ \boldsymbol{\alpha}_l^{(n)} \coloneqq \Big(\alpha_{l,1}^{(n)},\dots,\alpha_{l,l}^{(n)}\Big) \Big|\ \alpha_{l,j}^{(n)} < \alpha_{l,j+1}^{(n)} \quad \forall j \in \{1,\dots,l-1\}, \alpha_{l,j}^{(n)} \in [n] \Big\}, \tag{1}$$

for all $n \in \mathbb{N}, l \in \{1,\dots,n-1\}$, with vectors $\boldsymbol{\alpha}_l^{(n)}$ of length l, whose ordered components $\alpha_{l,j}^{(n)}$ label a specific Bob; e.g., $\mathcal{S}_2^{(4)} = \{(2,3),(2,4),(3,4)\}$. For the sake of legibility, we also use the abbreviation

$$B_{\pm}^{(j)} \coloneqq \frac{1}{2}\big(B_0^{(j)} \pm B_1^{(j)}\big). \tag{2}$$

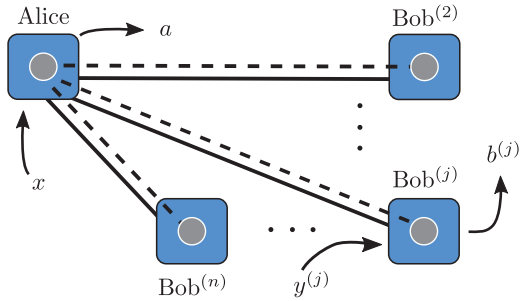

FIG. 1. A multipartite DIQKD setting, with parties Alice and $\{\mathrm{Bob}^{(j)}\}_{j=2}^{n}$. Alice distributes a multipartite quantum state via quantum channels (dashed lines). The parties communicate over classical channels (solid lines) and they perform measurements on their part of the quantum resource, specified via an input $x, y^{(j)} \in \{0,1\}$ that yields a result $a, b^{(j)} \in \{\pm 1\}$.

Definition. (Genuine multipartite Bell inequality) Let $n \geqslant 3$ be an integer and $\mathcal{S}_l^{(n)}$ the set defined in Eq. (1).

$$\begin{aligned}\mathcal{B}^{(n)} \coloneqq & \left\langle A_1 \bigotimes_{j=2}^{n} B_+^{(j)} \right\rangle - \delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \left\langle A_0 \bigotimes_{j=2}^{n} B_-^{(j)} \right\rangle \\ & - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\left\langle A_0 \otimes \sum_{\boldsymbol{\alpha}_{2k-1}^{(n)} \in \mathcal{S}_{2k-1}^{(n)}} \bigotimes_{j=1}^{2k-1} B_-^{\left(\alpha_{2k-1,j}^{(n)}\right)} \right\rangle \right. \\ & \left. + \left\langle \sum_{\boldsymbol{\alpha}_{2k}^{(n)} \in \mathcal{S}_{2k}^{(n)}} \bigotimes_{j=1}^{2k} B_-^{\left(\alpha_{2k,j}^{(n)}\right)} \right\rangle \right] \quad \begin{cases} \leqslant g_{\mathrm{cl}}^{(n)\downarrow} \\ \geqslant g_{\mathrm{cl}}^{(n)\uparrow} \end{cases}\end{aligned} \tag{3}$$

defines a genuine multipartite Bell inequality, with upper and lower classical bound $g_{\mathrm{cl}}^{(n)\downarrow}$ and $g_{\mathrm{cl}}^{(n)\uparrow}$, respectively.

Remember that $B_+^{(j)}$ and $B_-^{(j)}$ depend on each other, see Eq. (2). In the Suppl. Mat., we elaborate in detail on the construction of the Bell inequality. To make it more accessible, we state the Bell correlator for $n = 3$,

$$\begin{aligned}\mathcal{B}^{(3)} = & \left\langle A_1 B_+^{(2)} B_+^{(3)} \right\rangle - \left\langle A_0 \left(B_-^{(2)} + B_-^{(3)} \right) \right\rangle \\ & - \left\langle B_-^{(2)} B_-^{(3)} \right\rangle,\end{aligned} \tag{4}$$

and visualize it in Fig. 2 for $n = 4$.

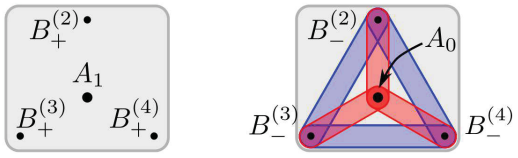

FIG. 2. Graphical representation of the correlators in the Bell inequality (3) for $n = 4$, which highlights the special role of Alice and the symmetry of the inequality w.r.t. to the Bobs. Vertices denote observables, and each hyperedge symbolizes a correlator the contains the corresponding observables.

Lemma. (Reduction of party number) For all $n \geqslant 2$, $\mathcal{B}^{(n-1)}$ is recovered from $\mathcal{B}^{(n)}$ via $B_0^{(n)} = B_1^{(n)} = \mathbb{1}$.

Proof. We have $B_-^{(n)} = 0$, hence

$$\bigotimes_{j=1}^{l} B_-^{\left(\alpha_{l,j}^{(n)}\right)} = 0 \quad \forall\, \boldsymbol{\alpha}_l^{(n)} \in \mathcal{S}_l^{(n)} \setminus \mathcal{S}_l^{(n-1)}. \tag{5}$$

Therefore, the sum over the set $\mathcal{S}_l^{(n)}$ is converted into a sum over $\mathcal{S}_l^{(n-1)}$. For n odd, the term $\langle A_0 \bigotimes_{j=2}^{n-1} B_-^{(j)} \rangle$ emerges from the sum in inequality (3) for $k = \frac{n-1}{2}$. As $B_+^{(n)} = \mathbb{1}$, the proof is complete. ■

By iteration, $\mathcal{B}^{(k)}$ is obtained from $\mathcal{B}^{(n)}$ for all $k < n$.

Theorem. (Classical Bounds) In any classical theory, the lower and upper bounds on $\mathcal{B}^{(n)}$ are given by

$$g_{\mathrm{cl}}^{(n)\uparrow} = -\left(2^{n-1} - 1\right) \quad \text{and} \quad g_{\mathrm{cl}}^{(n)\downarrow} = 1 \quad \forall n \in \mathbb{N}. \tag{6}$$

Note that the upper bound is independent of n. See Suppl. Mat. for the analytical proof, whose idea is to consider all classical deterministic strategies, which can be significantly reduced by exploiting the invariance of $\mathcal{B}^{(n)}$ under arbitrary relabeling of Bobs.

Here, some remarks are due. First, note that for $n = 2$, $\mathcal{B}^{(n)}$ and the classical bounds reproduce the CHSH inequality (normalized with a factor $\frac{1}{2}$). Furthermore, the Parity-CHSH inequality [18] is in fact a subclass of our Bell inequality, that is recovered via the choice $B_0^{(j)} = B_1^{(j)} =: B^{(j)}$ for all $j \geqslant 3$. Also, note that the lower classical bound on $\mathcal{B}^{(n)}$ is close to the algebraic minimum of -2^{n-1}. As we did not find a way to violate the lower bound, a *violation* of the Bell inequality (3) refers to the upper bound throughout this paper. Beyond that, a characterization of the maximum Bell value achievable with quantum correlations, the Tsirelson bound $g_{\mathrm{qm}}^{(n)}$ [28], is desirable. However, there is no general approach known that yields a tight Tsirelson bound for an arbitrary Bell inequality, as mentioned in Ref. [29]. An upper bound on the Tsirelson bound can be found by using the NPA hierarchy [27]. Usually, this procedure is numerically expensive, which is why we only calculate this bound for the first nontrivial odd- and even-numbered case, i.e., for $n \in \{3, 4\}$:

$$g_{\mathrm{qm}}^{(3)} = 1.5 \quad \text{and} \quad g_{\mathrm{qm}}^{(4)} \approx 1.5539. \tag{7}$$

These bounds are tight within numerical precision, cf. Table I. The Bell inequality (3) is particularly designed for the state $|\mathrm{GHZ}_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$, under the condition that the choice $A_0 = \sigma_z$ does not prohibit a violation of this inequality. The optimal measurements can be chosen to be in the $\sigma_z - \sigma_x$ plane of the Bloch sphere, as further argued in the Suppl. Mat., in detail,

$$A_0 = \sigma_z, \qquad B_0^{(j)} = \sin(\theta)\sigma_x + \cos(\theta)\sigma_z, \tag{8a}$$

$$A_1 = \sigma_x, \qquad B_1^{(j)} = \sin(\theta)\sigma_x - \cos(\theta)\sigma_z, \tag{8b}$$

for all $j \in [n]$, where the optimal value of the polar angle θ depends on the number of parties n. Note that, due to the symmetry of the Bell correlator and the target state, θ does not depend on j. This choice allows a straightforward calculation of the Bell value achievable with the n-GHZ state, which reads

$$g_{\mathrm{GHZ}}^{(n,\mathrm{odd})} = 1 - (1+\cos(\theta))^{n-1} + \sin^{n-1}(\theta)\,, \tag{9a}$$

$$g_{\mathrm{GHZ}}^{(n,\mathrm{even})} = 1 - (1+\cos(\theta))^{n-1} + \frac{\cot(\theta/2)\sin^{n}(\theta)}{1+\cos(\theta)}. \tag{9b}$$

Table I displays some quantities of interest for $n \leqslant 7$.

TABLE I: Maximum Bell value $g_{\mathrm{GHZ}}^{(n)}$ achievable with n-GHZ state, cf. Eq. (9), the ratio of $g_{\mathrm{GHZ}}^{(n)}$ and $g_{\mathrm{GHZ}}^{(n-1)}$, and the corresponding polar angle θ for all Bobs. The quantum-to-classical ratio is given by $g_{\mathrm{GHZ}}^{(n)}$, as $g_{\mathrm{cl}}^{(n)\downarrow} = 1$ for all n. The values are rounded to the fourth decimal place.

$\mathcal{B}^{(n)}$	$g_{\mathrm{GHZ}}^{(n)}$	$g_{\mathrm{GHZ}}^{(n)}/g_{\mathrm{GHZ}}^{(n-1)}$	θ
$\mathcal{B}^{(2)}$	$\sqrt{2} \approx 1.4142$		$\frac{3\pi}{4} \approx 2.3562$
$\mathcal{B}^{(3)}$	1.5	$\frac{3}{2\sqrt{2}} \approx 1.0607$	$\frac{2\pi}{3} \approx 2.0944$
$\mathcal{B}^{(4)}$	1.5539	1.0359	1.9786
$\mathcal{B}^{(5)}$	1.5926	1.0249	1.9106
$\mathcal{B}^{(6)}$	1.6224	1.0187	1.8650
$\mathcal{B}^{(7)}$	1.6464	1.0148	1.8318

For a given number of parties n, the corresponding relation in (9) can be numerically optimized w.r.t. θ and the limits become

$$\lim_{n\to\infty} g_{\mathrm{GHZ}}^{(n)} = 2 \qquad \text{and} \qquad \lim_{n\to\infty} \theta^{(n)} = \frac{\pi}{2}, \tag{10}$$

which is visualized in Fig. 3.

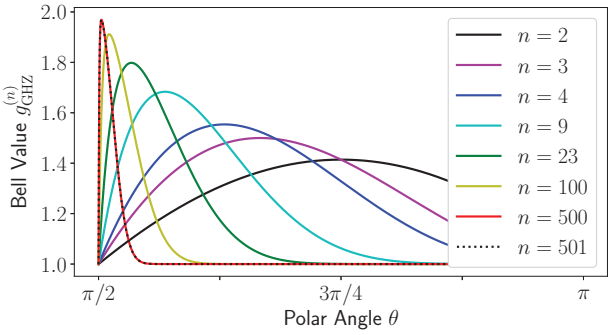

FIG. 3. Achievable Bell value $g_{\mathrm{GHZ}}^{(n)}$ according to Eq. (9) as a function of the polar angle θ for various number of parties n.

From Table I, we notice that the Bell value $g_{\mathrm{GHZ}}^{(n)}$ for $n \in \{3,4\}$ coincides with the Tsirelson bound in Eq. (7). Due to the symmetry and construction of the Bell inequality, we conjecture that this holds for general n. If this is true, finding the Tsirelson bound to our Bell inequality boils down to a simple numerical optimization over the parameter θ in Eq. (9). To conclude this discussion, consider the Bell inequality for $n = 3$ parties. States of the form $\rho = \rho_{AB^{(2)}} \otimes \rho_{B^{(3)}}$ do not allow to exceed the Tsirelson bound for $n = 2$ parties, which one can verify – either analytically or via the NPA hierarchy – by taking all classical deterministic strategies for Bob$^{(3)}$ into account. Thus, $\sqrt{2}$ is a Svetlichny bound [30] which can certify genuine tripartite entanglement. Likewise, one observes that states of the form $\rho = \rho_A \otimes \rho_{B^{(2)}B^{(3)}}$ cannot violate the classical bound. Beyond the tripartite case, we have numerical indication for analogous statements concerning biseparable splits, cf. Outlook.

Bounding Eves guessing probability.— Finally, we want to apply our Bell inequality (3) for DIQKD. As preparation, we briefly describe how to obtain a lower bound on the DI conference key rates. We focus on asymptotic secret-key rates and assume that quantum devices behave identically and independently in each round (i.i.d.). Let $\mathcal{G}^{(n)}$ denote the Bell operator corresponding to our Bell inequality (3), i.e., $\mathcal{B}^{(n)} = \mathrm{tr}\left(\mathcal{G}^{(n)}\rho_{\boldsymbol{AB}}\right)$, where $\rho_{\boldsymbol{AB}} \coloneqq \rho_{AB^{(2)}\ldots B^{(n)}}$ represents the quantum state shared among all parties. Let Alice use measurement input $x = 0$ for raw key generation and define $\boldsymbol{B_y} \coloneqq (B^{(2)}_{y^{(2)}}, \ldots, B^{(n)}_{y^{(n)}})$. Eve's guessing probability $P_{\mathrm{g}}(\boldsymbol{a}|\mathcal{E})$ about Alice's A_0-measurement results $\boldsymbol{a}$ conditioned on her information $\mathcal{E}$ can be upper bounded by a function f of the observed Bell violation $g_{\mathrm{obs}}^{(n)}$, i.e., $P_{\mathrm{g}}(\boldsymbol{a}|\mathcal{E}) \leqslant f(g_{\mathrm{obs}}^{(n)})$. For fixed $g_{\mathrm{obs}}^{(n)}$, it amounts to the solution of the SDP [13, 27, 31]

$$\begin{aligned} &\max_{\rho_{\boldsymbol{AB}}, A_x, \boldsymbol{B_y}} \ \mathrm{tr}\left(A_0\rho_{\boldsymbol{AB}}\right) \\ &\text{subject to: } \mathrm{tr}\left(\mathcal{G}^{(n)}\rho_{\boldsymbol{AB}}\right) = g_{\mathrm{obs}}^{(n)}. \end{aligned} \tag{11}$$

For classical-quantum states $\rho_{A\mathcal{E}}$, the guessing probability is connected to the quantum min-entropy via $H_{\min}(\boldsymbol{a}|\mathcal{E}) = -\log_2 P_{\mathrm{g}}(\boldsymbol{a}|\mathcal{E})$ [32], from which we obtain a lower bound on the DI asymptotic secret-key rate, $r_{\infty,n}^{\mathrm{SDP}} \geqslant -\log_2 f\left(g_{\mathrm{obs}}\right) - h\left(Q\right)$, where $h(p) \coloneqq -p\log_2(p) - (1-p)\log_2(1-p)$ and Q denote the binary entropy and the quantum bit error rate (QBER), respectively. The noisiest channel determines the QBER [4], hence

$$Q = \max_{j\in[n]}\left(Q_{AB^{(j)}}\right), \tag{12}$$

where $Q_{AB^{(j)}}$ is the QBER between Alice and Bob$^{(j)}$. The bound established by the SDP (11) is valid against the most general attacks the eavesdropper can perform [13] but they are in general rather loose. Recent development promises improvement in this regard [33].

Application: DI conference key agreement.— Here, we present achievable DI secret-key rates for $n \in \{2,3,4\}$ parties with a DIQKD protocol similar to the one in Ref. [34]. In the honest implementation, the quantum state distributed in each round of the protocol is the n-

GHZ state. To minimize the error-correction information, all parties measure σ_z in key generation rounds. To test for Bell-inequality violation, the parties choose observables as proposed in Eq. (8) that lead to a maximum violation. The protocol is aborted if the Bell inequality (3) is not violated. For a realistic scenario, we assume local depolarizing noise, that corrupts each qubit subsystem ρ_i according to

$$\mathcal{D}_{\text{dep}}(\rho_i) = (1-p)\rho_i + \frac{p}{2}\mathbb{1}_2, \tag{13}$$

where $p \in [0,1]$ denotes the noise parameter. In this scenario, the marginal probability distribution of Alice's A_0 measurement is uniform, i.e., $\langle A_0 \rangle = 0$. Since we consider binary outcomes, we can lower bound the Von Neumann entropy in terms of the guessing probability via $H(\boldsymbol{a}|\mathcal{E}) \geqslant 2\,(1 - P_{\text{g}}(\boldsymbol{a}|\mathcal{E}))$ [33, 35], which in turn yields

$$r_\infty^{\mathcal{B}^{(n)}} \geqslant 2\,(1 - P_{\text{g}}(\boldsymbol{a}|\mathcal{E})) - h\,(Q)\,. \tag{14}$$

Figure 4 displays the lower bound on the asymptotic DI

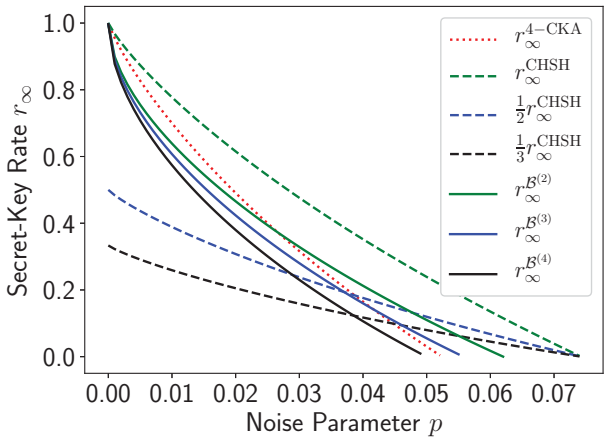

FIG. 4. Asymptotic DI secret-key rates according to Eq. (14) in dependence of the noise parameter p (solid lines) for $n \in \{2,3,4\}$. In bottleneck networks and for low noise, the multipartite DIQKD protocol outperforms multiple bipartite DIQKD protocols, Eq. (15), (dashed lines). The dotted line corresponds to the analytical bounds of Ref. [18], Eq. (4) for $n = 4$ in the same implementation. In terms of key rates calculated via SDP, however, our Bell inequality leads to better results compared to the Parity-CHSH inequality (not shown in this Figure), an advantage that increases with the noise parameter p. For example for $n = 3$ and $p \in \{3,4,5\}\%$, key rates based on $\mathcal{B}^{(3)}$ are larger by approximately $\{1.2, 3.6, 16.8\}\%$.

secret-key rate, Eq. (14), as a function of the parameter p of the noise model in Eq. (13). To put these key rates into perspective, we consider the same comparison as in Ref. [18], where the conference key rates are compared with multiple bipartite key rates, described by [11]

$$r_\infty^{\text{CHSH}} \geqslant 1 - h\,(Q) - h\left(\frac{1+\sqrt{S^2/4-1}}{2}\right), \tag{15}$$

where S denotes the violation of the CHSH inequality. For illustration, we consider the Bell state $|\phi^+\rangle \propto |00\rangle + |11\rangle$ under the noise model in Eq. (13), which connects S with Q according to $S = 2\sqrt{2}\,(1-2Q)$. The QBER Q as defined in Eq. (12) is related to the noise parameter via $Q = p\,(1-p/2)$ for all n. Under the assumption that Alice cannot perform the bipartite QKD protocols with every Bob simultaneously, which can be the case in bottleneck networks, cf. Ref. [4], the bipartite key rates get a prefactor of $(n-1)^{-1}$.

As mentioned, the bounds on the guessing probability in terms of SDPs are often too pessimistic. Therefore, we cannot beat the analytical results of Ref. [18]. In direct comparison via the SDP, however, our Bell inequality leads to slightly better conference key rates than the Parity-CHSH inequality, see caption of Fig. 4.

Conclusion and Outlook.— In this manuscript, we introduced a novel family of genuine multipartite Bell inequalities, that is specifically tailored to the n-GHZ state, while maintaining the possibility to maximally violate it with σ_z measurements. As argued, an application is to use this Bell inequality for a Bell test in a DIQKD protocol, because there highly correlated measurement results and maximal violation are required at the same time. We established the classical bounds of this Bell inequality and suggested measurements that lead to the maximal Bell value, given the n-GHZ state is measured. Finally, we calculated via semidefinite programming conference key rates based on the violation of our Bell inequality and discussed its robustness against depolarizing noise.

For future work, a more thorough study of our Bell inequality (3) is desirable. A starting point is to clarify the role of partially entangled states and the existence of associated intermediate bounds in our Bell inequality, similar to the MABK case [36]. We conjecture that the maximum Bell value $\mathcal{B}^{(n)}$ for n parties with biseparable states where at most $k-1$ Bobs are entangled with Alice, is determined by the maximum Bell value $\mathcal{B}^{(k)}$ for k parties. In this case a Bell value larger then $\mathcal{B}^{(k)}$ is a DI witness for entanglement of at least $k+1$ parties, one of them being Alice. An important goal would be to find an analytical bound on the Von Neumann entropy in terms of the violation of our Bell inequality (3). As we provided a nontrivial genuinely multipartite generalization of the CHSH inequality – in a similar spirit as the n-GHZ state represents a multipartite generalization of the Bell state – we hope that our contribution paves the way for further insight into multipartite quantum communication.

The authors acknowledge support from the Federal Ministry of Education and Research BMBF (Project Q.Link.X and HQS) and from ML4Q Excellence Cluster of DFG. We thank Reinhard Werner, Gláucia Murta, and Lucas Tendick for helpful discussions.

Supplemental Material

We split the Suppl. Mat. into four parts. First, we prove the classical upper and lower bounds of our Bell inequality. Afterwards, we elaborate on the construction of the Bell inequality and discuss optimal measurements to achieve a maximum Bell value with the n-GHZ state. Finally we state the DIQKD protocol for completeness. We recall our Bell inequality for convenience:

$$
\begin{aligned}
-\left(2^{n-1}-1\right) \leqslant \left\langle A_1 \bigotimes_{j=2}^{n} B_+^{(j)} \right\rangle - \delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \left\langle A_0 \bigotimes_{j=2}^{n} B_-^{(j)} \right\rangle \\
- \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\left\langle A_0 \otimes \sum_{\boldsymbol{\alpha}_{2k-1}^{(n)} \in \mathcal{S}_{2k-1}^{(n)}} \bigotimes_{j=1}^{2k-1} B_-^{\left(\alpha_{2k-1,j}^{(n)}\right)} \right\rangle + \left\langle \sum_{\boldsymbol{\alpha}_{2k}^{(n)} \in \mathcal{S}_{2k}^{(n)}} \bigotimes_{j=1}^{2k} B_-^{\left(\alpha_{2k,j}^{(n)}\right)} \right\rangle \right] \leqslant 1.
\end{aligned} \tag{16}
$$

Proof of the Theorem

The maximal and minimal classical value is achieved for deterministic strategies. To establish the classical bounds, we thus consider the variables A_x and $B_{y^{(j)}}^{(j)}$ for $x, y^{(j)} \in \{0,1\}$, $j \in \{2,\ldots,n\}$ to take on values from the set $\{\pm 1\}$ and denote with the vector $\left(\boldsymbol{A}, \boldsymbol{B}^{(j)}\right)$ a strategy from the set that contains every possible combination of ± 1 as components for this $2n$-dimensional vector. We also define

$$
\tilde{\mathcal{B}}^{(n)} := -\delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} A_0 \prod_{j=2}^{n} B_-^{(j)} - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[A_0 \sum_{\boldsymbol{\alpha}_{2k-1}^{(n)} \in \mathcal{S}_{2k-1}^{(n)}} \prod_{j=1}^{2k-1} B_-^{\left(\alpha_{2k-1,j}^{(n)}\right)} + \sum_{\boldsymbol{\alpha}_{2k}^{(n)} \in \mathcal{S}_{2k}^{(n)}} \prod_{j=1}^{2k} B_-^{\left(\alpha_{2k,j}^{(n)}\right)} \right], \tag{17}
$$

such that we can write $\mathcal{B}^{(n)} = A_1 \prod_j B_+^{(j)} + \tilde{\mathcal{B}}^{(n)}$ for the classical Bell value. We make the important observation, that any strategy $\left(\boldsymbol{A}, \boldsymbol{B}^{(j)}\right)$ that leads to $A_1 \prod_j B_+^{(j)} \neq 0$, eliminates the value of $\tilde{\mathcal{B}}^{(n)}$ as this requires that $B_+^{(j)} \neq 0$ (and thus $B_-^{(j)} = 0$) for all $j \in [n]$. Therefore, we can maximize and minimize the expressions $A_1 \prod_j B_+^{(j)}$ and $\tilde{\mathcal{B}}^{(n)}$ independently. This distinction into cases allows us, to map the strategies for the maximization (minimization) of $\tilde{\mathcal{B}}^{(n)}$ from $\left(\boldsymbol{A}, \boldsymbol{B}^{(j)}\right) \in \{\pm 1\}^{2n}$ to $\left(A_0, \boldsymbol{B}_-^{(j)}\right)$ with $A_0 \in \{\pm 1\}$ and $B_-^{(j)} = \frac{1}{2}\left(B_0^{(j)} - B_1^{(j)}\right) \in \{\pm 1, 0\}$. For the proof we require three important properties of the binomial coefficients:

$$
\sum_{l=0}^{n} \binom{n}{l} = 2^n \qquad \text{(Normalization)}, \tag{18a}
$$

$$
\binom{n}{l} = \binom{n-1}{l} + \binom{n-1}{l-1} \qquad \text{(Pascal triangle)}, \tag{18b}
$$

$$
\binom{n}{l} = \sum_{j=0}^{l} \binom{m}{j} \binom{n-m}{l-j} \qquad \text{(Chu-Vandermonde identity)}. \tag{18c}
$$

Note, that we make use of the conventions $0! = 1$ and $\binom{n}{l} = 0$ $\forall l > n, l < 0$. We divide the proof into two parts, one for the lower and one for the upper bound.

(i) Lower bound. To establish the lower classical bound, note that the minimization of $A_1 \prod_j B_+^{(j)}$ leads only to the value of -1. A minimization of $\tilde{\mathcal{B}}^{(n)}$, however, is given by the choice $B_-^{(j)} = +1$ for all j and $A_0 = +1$, as this turns every contribution in Eq. (17) negative, in detail

$$
\tilde{\mathcal{B}}^{(n)} = -\delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\binom{n-1}{2k-1} + \binom{n-1}{2k} \right] = -\delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} - \sum_{k=1}^{2\lfloor \frac{n-1}{2} \rfloor} \binom{n-1}{k}, \tag{19}
$$

where we used the cardinality $\#\mathcal{S}_l^{(n)} = \binom{n-1}{l}$. Via the normalization condition, Eq. (18a), the expression above simplifies for both n odd and even to $-\left(2^{n-1}-1\right)$, as claimed.

(ii) Upper bound. A maximization of $A_1 \prod_j B{+}^{(j)}$ leads to the value of 1, but a priori it is not clear that this is indeed the maximum possible $\mathcal{B}^{(n)}$-value. We start by counting all possible strategies for $\tilde{\mathcal{B}}^{(n)}$ and categorize them, such that we can calculate its value by a distinction of cases. There are $2 \times 3^{n-1}$ different possibilities to choose a strategy $\left(A_0, \boldsymbol{B}_-^{(j)}\right)$, however, we notice that the expression $\tilde{\mathcal{B}}^{(n)}$ in Eq. (17) is invariant under permutation of Bobs, i.e., we only need to calculate the $\tilde{\mathcal{B}}^{(n)}$-value for a subset of strategies $\left(A_0, \boldsymbol{B}_-^{(j)}\right)$, that cannot be converted into each other by permutation of Bobs. This reduces the number of different deterministic strategies to only $n(n+1)$. As a final remark before we work through the different strategies note that the amount of nonzero values for the variables $B_-^{(j)}$ determines which summands give a nontrivial contribution to $\tilde{\mathcal{B}}^{(n)}$. To be more specific, let $q_\pm$ denote the amount of ±1-values in the strategy $\left(A_0, \boldsymbol{B}_-^{(j)}\right)$, and let $q_+ + q_- =: q \leqslant n-1$ be the amount of nonzero $B_-^{(j)}$-values. Due to the permutational invariance of $\tilde{\mathcal{B}}^{(n)}$ we order without loss of generality the strategy $\left(A_0, \boldsymbol{B}_-^{(j)}\right)$ such that $B_-^{(j)} = 0$ for all $j > q+1$. Then, every product in Eq. (17) associated to a label $\boldsymbol{\alpha}_l^{(n)} \in \mathcal{S}_l^{(n)} \setminus \mathcal{S}_l^{(q+1)}$ vanishes, as it contains at least one Bob$^{(j)}$ with $B_-^{(j)} = 0$. This converts the sum over the set $\mathcal{S}_l^{(n)}$ into a sum over the set $\mathcal{S}_l^{(q+1)}$ of cardinality $\binom{q}{l}$. The expression $A_0 \prod_{j=2}^{n} B_-^{(j)}$ always vanishes for $q < n-1$.

(a) $q \leqslant n-1, q = q_\pm$. For these cases, $B_-^{(j)} = B_-^{(k)}$ holds for all $j,k \in \{2,\dots,q+1\}$. Applying this strategy, yields

$$\begin{aligned}\tilde{\mathcal{B}}^{(n)} &= -\delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \delta_{n-1,q} A_0 (\pm1)^{n-1} - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[A_0 \sum_{\alpha_{2k-1}^{(q+1)} \in \mathcal{S}_{2k-1}^{(q+1)}} (\pm1)^{2k-1} + \sum_{\alpha_{2k}^{(q+1)} \in \mathcal{S}_{2k}^{(q+1)}} (\pm1)^{2k} \right] \\ &= -\delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \delta_{n-1,q} A_0 (\pm1)^{n-1} - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\pm A_0 \binom{q}{2k-1} + \binom{q}{2k} \right]. \end{aligned} \tag{20}$$

To proceed, let n be an odd integer, hence $\delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} = 0$. Then, the best Alice can do is to choose her variable $A_0 \in \{\pm1\}$ such that the sum is minimized, because of the global minus sign in Eq. (20). Exploiting identity (18b), leads to

$$\tilde{\mathcal{B}}^{(n)} = -\sum_{k=1}^{\frac{n-1}{2}} \left[-\binom{q-1}{2k-2} + \binom{q-1}{2k} \right], \tag{21}$$

where the only nonvanishing term is $\binom{q-1}{0}$ and thus results in $\tilde{\mathcal{B}}^{(n)} = 1$. For n even, we can make a similar argument. Choosing the value for A_0 that maximizes the total expression leads us to

$$\tilde{\mathcal{B}}^{(n)} = \delta_{n-1,q} + \binom{q-1}{0} - \binom{q-1}{n-2} = \delta_{n-1,q} + 1 - \delta_{n-1,q} = 1. \tag{22}$$

(b) $q_+ + q_- = q \leqslant n-1, q_\pm \geqslant 1$. For the remaining cases, at least one variable $B_-^{(j)}$ is $+1$ and at least one is -1. From Eq. (17) we obtain with this strategy

$$\tilde{\mathcal{B}}^{(n)} = (-1)^{q_-+1} \delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}}\, \delta_{n-1,q}\, A_0 - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[A_0 \sum_{r=0}^{2k-1} (-1)^r \binom{q_+}{2k-1-r} \binom{q_-}{r} + \sum_{r=0}^{2k} (-1)^r \binom{q_+}{2k-r} \binom{q_-}{r} \right]. \tag{23}$$

Recall, that in the case where all Bobs have the same value, we have $\#\mathcal{S}_l^{(q+1)}$ combinations to attribute the value ±1 to all l out of q Bobs. Here, the sum still has $\binom{q}{l}$ many terms, but some multiply to $+1$, while others to -1, depending on how many elements are drawn from q_-. To correctly count the numbers of combinations leading to the sign ±1, we use the Chu-Vandermonde identity (18c). The idea here is to divide the total amount of options q into two subsets q_+ and q_-, and then count all possible combinations to draw elements from these subsets. But due to the negativity of elements from the set q_-, we need to include a negative sign for $\binom{q_-}{r}$ if r is odd. Important is, that due to the alternating sign, almost all terms in Eq. (23) cancel each other. In fact, the following two relations hold

$$\sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\sum_{r=0}^{2k-1} (-1)^r \binom{q_+}{2k-1-r} \binom{q_-}{r} \right] = (-1)^{q_-+1} \delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \delta_{n-1,q} \qquad \text{and} \tag{24a}$$

$$\sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \left[\sum_{r=0}^{2k} (-1)^r \binom{q_+}{2k-r} \binom{q_-}{r} \right] = -1 \qquad \forall\ n \in \mathbb{N},\ q_\pm \geqslant 1,\ q_+ + q_- \leqslant n-1. \tag{24b}$$

Showing the validity of these relations concludes the prove, as inserting them into Eq. (23) leads to the maximum of $\tilde{\mathcal{B}}^{(n)} = 1$. To prove Eq. (24a) we order the left-hand side of it by positive and negative contributions

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{2k-1}(-1)^r\binom{q_+}{2k-1-r}\binom{q_-}{r}\right] = \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{k-1}\binom{q_+}{2k-1-2r}\binom{q_-}{2r}\right] \tag{25a}$$

$$- \sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{k-1}\binom{q_+}{2k-1-(2r+1)}\binom{q_-}{2r+1}\right]. \tag{25b}$$

The idea is to use the Pascal triangle relation (18b), to eliminate the problems that arise due to the alternating sign. Via Eq. (18b) we thus split the right-hand side of Eq. (25a) into the following two expressions:

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\sum_{r=0}^{k-1}\binom{q_- - 1}{2r}\left[\binom{q_+ - 1}{2k-1-2r} + \binom{q_+ - 1}{2(k-1)-2r}\right] = \sum_{x=0}^{2\lfloor\frac{n-1}{2}\rfloor-1}\sum_{r=0}^{\lfloor\frac{x}{2}\rfloor}\binom{q_- - 1}{2r}\binom{q_+ - 1}{x-2r}, \tag{26a}$$

$$\sum_{k=2}^{\lfloor\frac{n-1}{2}\rfloor}\sum_{r=1}^{k-1}\binom{q_- - 1}{2r-1}\left[\binom{q_+ - 1}{2(k-1)-(2r-1)} + \binom{q_+ - 1}{2(k-1)-1-(2r-1)}\right] = \sum_{x=1}^{2\lfloor\frac{n-1}{2}\rfloor-2}\sum_{r=1}^{\lfloor\frac{x+1}{2}\rfloor}\binom{q_- - 1}{2r-1}\binom{q_+ - 1}{x-(2r-1)}, \tag{26b}$$

where we introduced a new index of summation x to simplify both expressions. We dropped the contributions from $k = 1$ and $r = 0$ in Eq. (26b), as they vanish anyway. To proceed, we add the right-hand sides of Eqs. (26a) and (26b). All integers from $r = 0$ up to $r = x$, for all $x \in \{0, \ldots, 2\lfloor\frac{n-1}{2}\rfloor - 2\}$ appear in this sum. Therefore, the right-hand side of Eq. (25a) is given by

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{k-1}\binom{q_+}{2k-1-2r}\binom{q_-}{2r}\right] = \sum_{x=0}^{2\lfloor\frac{n-1}{2}\rfloor-2}\sum_{y=0}^{x}\binom{q_- - 1}{y}\binom{q_+ - 1}{x-y} + \sum_{r=0}^{\lfloor\frac{n-1}{2}\rfloor-1}\binom{q_- - 1}{2r}\binom{q_+ - 1}{2\lfloor\frac{n-1}{2}\rfloor - 1 - 2r}, \tag{27}$$

where we used $\lfloor\lfloor\frac{n-1}{2}\rfloor - \frac{1}{2}\rfloor = \lfloor\frac{n-1}{2}\rfloor - 1$. To simplify Eq. (27), note that the second sum only yields a nontrivial contribution, if $2r \leqslant q_- - 1$ and $2r \geqslant 2\lfloor\frac{n-1}{2}\rfloor - q + q_-$, which is only possible if $q \geqslant 2\lfloor\frac{n-1}{2}\rfloor + 1$. As we additionally have the constraint $q \leqslant n-1$, we require $q = n-1$ and n needs to be an even integer. In this case, the only nonvanishing term in the second sum in Eq. (27) is a single expression equal to $+1$, corresponding to $r = \frac{q_- - 1}{2}$, which can only be a valid integer if q_- is odd. Beyond this, we use the Chu-Vandermonde identity (18c) to simplify the first expression of the right-hand side in Eq. (27) and obtain

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{k-1}\binom{q_+}{2k-1-2r}\binom{q_-}{2r}\right] = \sum_{x=0}^{2\lfloor\frac{n-1}{2}\rfloor-2}\binom{q-2}{x} + \delta_{n-1,q}\delta_{\lfloor\frac{n}{2}\rfloor,\frac{n}{2}}\delta_{\lfloor\frac{q_- - 1}{2}\rfloor,\frac{q_- - 1}{2}}. \tag{28}$$

The same procedure can be applied to the right-hand side of Eq. (25b). Ultimately, it leads to

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{k-1}\binom{q_+}{2k-1-(2r+1)}\binom{q_-}{2r+1}\right] = \sum_{x=0}^{2\lfloor\frac{n-1}{2}\rfloor-2}\binom{q-2}{x} + \delta_{n-1,q}\delta_{\lfloor\frac{n}{2}\rfloor,\frac{n}{2}}\delta_{\lfloor\frac{q_-}{2}\rfloor,\frac{q_-}{2}}, \tag{29}$$

where the additional contribution is now only obtained if q_- is an even integer. The difference between Eqs. (28) and (29) represents the left-hand side of Eq. (25a). We thus obtain

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{2k-1}(-1)^r\binom{q_+}{2k-1-r}\binom{q_-}{r}\right] = \delta_{n-1,q}\delta_{\lfloor\frac{n}{2}\rfloor,\frac{n}{2}}\left(\delta_{\lfloor\frac{q_- - 1}{2}\rfloor,\frac{q_- - 1}{2}} - \delta_{\lfloor\frac{q_-}{2}\rfloor,\frac{q_-}{2}}\right) = (-1)^{q_- + 1}\delta_{n-1,q}\delta_{\lfloor\frac{n}{2}\rfloor,\frac{n}{2}}, \tag{30}$$

which proves identity (24a). Essentially the same approach now leads to the prove of relation (24b). Only minor and straightforward adjustments for the index of summations are needed, which then leads to

$$\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\sum_{r=0}^{2k}(-1)^r\binom{q_+}{2k-r}\binom{q_-}{r}\right] = -\binom{q-2}{0} + \binom{q-2}{2\lfloor\frac{n-1}{2}\rfloor - 1} - \delta_{n-1,q}\delta_{\lfloor\frac{n}{2}\rfloor,\frac{n}{2}} = -1, \tag{31}$$

because the second binomial coefficient is $+1$ if n is even and $q = n-1$, and 0 otherwise. This concludes the proof. ■

On the Construction of the Bell Inequality

The Bell inequality (16) is constructed around two central restrictions we impose on the Bell setting. First, we want to achieve a large Bell value if the quantum resource is given by an n-GHZ state and second, that this Bell value is achievable if Alice measures $A_0 = \sigma_z$. As the Bell inequality is tested for violation in a DIQKD protocol, these restrictions are clearly motivated by Theorem 1 of Ref. [4], which states that maximum correlation among all n parties with a GHZ state requires all parties to measure σ_z. We set the stage by discussing known multipartite Bell inequalities and introducing some notation. A priori, it is not clear, how to devise a useful Bell inequality, that is particularly well suited for the n-GHZ state. The MABK inequality [21–23] for instance allows a maximum violation by the n-GHZ state, as discussed in Ref. [37]. For DIQKD however, the MABK inequality is not suitable because the very structure of it prohibits to simultaneously achieve perfectly correlated measurement results among all parties and sufficiently high Bell-inequality violation, see Ref. [25] for details. Also most recently, Ref. [24] introduces a Bell inequality which is tailored to be maximally violated by an n-GHZ state of any local dimension d. However, at least for $d = 2$ and $m = 2$ measurement settings, this inequality suffers from the same drawbacks as the MABK inequality. Imposing the additional constraint on the Bell setting, that Alice should in principle be able to measure $A_0 = \sigma_z$ without compromising the possibility to violate the Bell inequality has led us to our inequality (16). Another Bell inequality which embraces this idea, is the Parity-CHSH inequality [18]

$$\mathcal{B}^{(n)}_{\text{Parity}} \coloneqq A_1 \otimes \frac{B^{(2)}_0 + B^{(2)}_1}{2} \bigotimes_{j=3}^{n} B^{(j)} - A_0 \otimes \frac{B^{(2)}_0 - B^{(2)}_1}{2} \leqslant 1 \leqslant \sqrt{2}, \tag{32}$$

where each $\text{Bob}^{(j)}$ for $j \geqslant 3$ only has one observable. In fact, the Parity-CHSH inequality can be reproduced from our Bell inequality (16), by choosing $B^{(j)}_0 = B^{(j)}_1$ for all $j \geqslant 3$ and therefore $B^{(j)}_- = 0$ and $B^{(j)}_+ = B^{(j)}_0 =: B^{(j)}$.

We briefly recall the notation we already introduced in Ref. [25], as it is crucial for the construction of the Bell inequality (16). Let $\mathbb{F}_2 = \{0, 1\}$ denote the finite field with two elements, which allows us to define the vector space $\mathbb{F}_2^n$ of bit strings of length n. Let further $\mathcal{P}_n$ denote the n-qubit Pauli group. We define the stabilizer group

$$\mathcal{S} \coloneqq \Big\{ S \in \mathcal{P}_n \;\Big|\; S\,|\text{GHZ}_n\rangle = |\text{GHZ}_n\rangle \Big\} \tag{33}$$

of the n-GHZ state $\chi_n = |\text{GHZ}_n\rangle\langle\text{GHZ}_n|$. The group $\mathcal{S}$ is generated by the n independent operators

$$G_1 \coloneqq \sigma_x^{\otimes n}, \quad \text{and for all } j \in [n]: \tag{34a}$$

$$G_j \coloneqq \bigotimes_{i=1}^{j-2} \mathbb{1}_2^{(i)} \otimes \sigma_z^{(j-1)} \otimes \sigma_z^{(j)} \otimes \bigotimes_{i=j+1}^{n} \mathbb{1}_2^{(i)}, \tag{34b}$$

where the superscript denotes the corresponding subsystems. In general, the projector of any stabilizer state can be written as the normalized sum of all of its stabilizer operators [38, 39]. We obtain for χ_n with $\boldsymbol{s} \coloneqq (s_1, \ldots, s_n) \in \mathbb{F}_2^n$ the representation:

$$\chi_n = \frac{1}{2^n} \sum_{\boldsymbol{s} \in \mathbb{F}_2^n} (\sigma_x^{s_1})^{\otimes n} \big(\sigma_z^{s_2} \otimes \sigma_z^{s_2 + s_3} \otimes \cdots \otimes \sigma_z^{s_{n-1} + s_n} \otimes \sigma_z^{s_n} \big). \tag{35}$$

The sum in Eq. (35) consists of 2^n individual terms, where 2^{n-1} of them contain only Pauli σ_z and identity operators (namely those with $s_1 = 0$), while the other 2^{n-1} ones consists of only Pauli σ_x and σ_y operators. The *weight* of such operators is given by the number of nontrivial Pauli matrices it contains. For $s_1 = 1$, the operators always have full weight, while for $s_1 = 0$ the weight of the operators is always an even number, but all possible combinations (with respect to the subsystems) of all even numbers $2k \leqslant n$ of σ_z occur. For the construction of our Bell inequality, we pursue a strategy which matches the restrictions we initially imposed on the Bell setting. To obtain a large quantum value with the n-GHZ state, the idea is to gain a contribution from as many operators as possible from the representation in Eq. (35). To quantify this, recall that Pauli matrices are traceless and that their product is given by

$$\sigma_j \sigma_k = \delta_{j,k} \mathbb{1}_2 + i \sum_{l=1}^{3} \epsilon_{jkl} \sigma_l, \tag{36}$$

where $\delta_{j,k}$ and ϵ_{jkl} denote the Kronecker delta and the Levi-Civita tensor, respectively. As we require $A_0 = \sigma_z$ and because of relation (36) the expression

$$\mathrm{tr}\left[A_0 \bigotimes_{j\in\mathcal{I}} \left(B_0^{(j)} - B_1^{(j)}\right) \sum_{\boldsymbol{s}\in\mathbb{F}_2^n, s_1=1} \left(\sigma_x\sigma_z^{s_2} \otimes \cdots \otimes \sigma_x\sigma_z^{s_n}\right)\right] = 0 \tag{37}$$

always vanishes, for any index subset $\mathcal{I} \subseteq \{2,\ldots,n\}$, for all $\boldsymbol{s}$ with $s_1 = 1$ and for all dichotomic observables $B_i^{(j)}$. The counterpart of expression (37) for $s_1 = 0$ however, is nonvanishing if the observables have an even weight. The same argument can be done for the corresponding expression without an observable of Alice. As all possible combinations occur in the n-GHZ state, we also include all possible combinations of observables with respect to the parties for expectation values in our Bell inequality. This explains the term

$$-\sum_{k=1}^{\lfloor\frac{n-1}{2}\rfloor}\left[\left\langle A_0 \otimes \sum_{\boldsymbol{\alpha}_{2k-1}^{(n)}\in\mathcal{S}_{2k-1}^{(n)}} \bigotimes_{j=1}^{2k-1} B_-^{\left(\alpha_{2k-1,j}^{(n)}\right)}\right\rangle + \left\langle \sum_{\boldsymbol{\alpha}_{2k}^{(n)}\in\mathcal{S}_{2k}^{(n)}} \bigotimes_{j=1}^{2k} B_-^{\left(\alpha_{2k,j}^{(n)}\right)}\right\rangle\right] \tag{38}$$

in our Bell inequality. The expression $-\delta_{\lfloor\frac{n}{2}\rfloor,\frac{n}{2}}\left\langle A_0 \bigotimes_{j=2}^n B_-^{(j)}\right\rangle$ is included due to a fundamental difference between the odd- and even-numbered n-GHZ state. For n even, the operator $\sigma_z^{\otimes n}$ occurs in the GHZ state representation in Eq. (35), while for n odd, this is not the case. Finally, since operators with $s_1 = 1$ have full weight, we include one additional expectation value in the Bell inequality that contains observables of all parties, hence the first term in our Bell inequality.

Optimal Measurements and Properties of the Bell Inequality

As our main goal was to establish a useful Bell inequality for multipartite device-independent quantum key distribution (DIQKD), our focus is not the complete characterization of our Bell inequality. For completeness, however, we want to address some properties, in particular we suggest measurement observables for all parties that lead to a maximum Bell value if the n-GHZ state is measured, because this is relevant for QKD. Further properties which could be worth investigating are, if it is possible to analytically derive the Tsirelson bounds [28], if the Bell inequalities constitute facets of the classical polytope [40], or if there exist intermediate bounds for separable states with respect to different splits of parties, as it is the case for the MABK inequality [36]. For $n = 3$ we discovered that $\mathcal{B}^{(3)}$ is in fact a facet inequality, as one can show with the methods presented in Ref. [41]. As already mentioned in the main article, we conjecture that there exist intermediate bounds.
To motivate the optimal choices for the observables given the GHZ state χ_n is measured, recall that a general qubit observable can be parametrized as

$$B_i^{(j)} = \cos\left(\varphi_i^{(j)}\right)\sin\left(\theta_i^{(j)}\right)\sigma_x + \sin\left(\varphi_i^{(j)}\right)\sin\left(\theta_i^{(j)}\right)\sigma_y + \cos\left(\theta_i^{(j)}\right)\sigma_z, \tag{39}$$

and analogously for A_1. Note that $B_0^{(j)}, B_1^{(j)}$ always appear as $B_-^{(j)} \propto B_0^{(j)} - B_1^{(j)}$ in our Bell inequality, if paired with A_0 or if no observable of Alice is included. To maximize the corresponding expectation values, it is best to eliminate the contribution of all $B_-^{(j)}$ in σ_x and σ_y direction, as this part vanishes anyway due to the structure of the GHZ state in Eq. (35). This translates to $\varphi_0^{(j)} = \varphi_1^{(j)}$ for all $j \in [n]$, as a necessary condition to guarantee $B_- \propto \sigma_z$. Likewise, the expression $B_+^{(j)} \propto B_0^{(j)} + B_1^{(j)}$ appears only in combination with A_1. Because all operators with $s_1 = 1$ in Eq. (35) have full weight, we might as well take that A_1 and all $B_+^{(j)}$ expressions have no contribution in σ_z direction, to gain a large contribution to the Bell value from $\left\langle A_1 \bigotimes_{j=2}^n B_+^{(j)}\right\rangle$. Due to $\cos(\alpha) = -\cos(\pi \pm \alpha)$, we extract $\theta_1^{(j)} = \pi \pm \theta_0^{(j)}$ for all $j \in [n]$ from the representation (39), as a necessary condition to eliminate the σ_z contribution of $B_+^{(j)}$. Beyond that, we note that $\sin(\pi \pm \alpha) = \mp\sin(\alpha)$. Together with $\varphi_0^{(j)} = \varphi_1^{(j)}$, the choice $\theta_1^{(j)} = \pi + \theta_0^{(j)}$ eliminates $B_+^{(j)}$, which is why we use $\theta_1^{(j)} = \pi - \theta_0^{(j)}$ in the following. Finally, we numerically find that for a given choice of A_1, the actual value of the azimuthal angle $\varphi_0^{(j)}, \varphi_1^{(j)}$ is irrelevant for maximizing the Bell value, as long as they are equal for each Bob. Therefore, we set $\varphi_0^{(j)} = \varphi_1^{(j)} = 0$ for all $j \in [n]$ and $\varphi_{A_1} = 0$. Furthermore, the polar angles $\theta_0^{(j)}, \theta_1^{(j)}$ can be chosen the same for every Bob, without compromising the possibility to achieve the maximum Bell value. We therefore set

$\theta_0^{(j)} = \theta$ and $\theta_1^{(j)} = \pi - \theta$ for all $j \in [n]$. In total, the maximum Bell value $\mathcal{B}^{(n)}$ given an n-GHZ state is measured, can be achieved with

$$A_0 = \sigma_z, \quad A_1 = \sigma_x, \quad B_0^{(j)} = \sin(\theta)\,\sigma_x + \cos(\theta)\,\sigma_z, \quad B_1^{(j)} = \sin(\theta)\,\sigma_x - \cos(\theta)\,\sigma_z \quad \forall\, j \in [n], \tag{40}$$

where the optimal value of the polar angle θ depends on the number of parties n. This choice allows a straightforward calculation of the Bell value with the n-GHZ state

$$g_{\mathrm{GHZ}}^{(n)} = \left[\sin(\theta)^{n-1} - \delta_{\lfloor \frac{n}{2} \rfloor, \frac{n}{2}} \cos(\theta)^{n-1}\right] - \sum_{k=1}^{\lfloor \frac{n-1}{2} \rfloor} \cos(\theta)^{2k-1} \left[\binom{n-1}{2k-1} + \cos(\theta) \binom{n-1}{2k}\right], \tag{41}$$

which can be simplified to

$$g_{\mathrm{GHZ}}^{(n)} = 1 - (1 + \cos(\theta))^{n-1} + \sin(\theta)^{n-1} \qquad \text{for } n \text{ odd}, \tag{42a}$$

$$g_{\mathrm{GHZ}}^{(n)} = 1 - (1 + \cos(\theta))^{n-1} + \frac{\cot(\theta/2)\sin(\theta)^n}{1 + \cos(\theta)} \qquad \text{for } n \text{ even}. \tag{42b}$$

For given n, the corresponding relation (42) can be numerically optimized for θ and the limits become

$$\lim_{n\to\infty} g_{\mathrm{GHZ}}^{(n)} = 2 \qquad \text{and} \qquad \lim_{n\to\infty} \theta^{(n)} = \frac{\pi}{2}. \tag{43a}$$

Multipartite DIQKD Protocol

Finally, we want to state the DIQKD protocol. Alice has two measurement inputs $x \in \{0, 1\}$ implementing the measurement of a dichotomic observable A_x. Each Bob$^{(j)}$ has three inputs $y^{(j)} \in \{0, 1, 2\}$, with dichotomic observables $B_{y^{(j)}}^{(j)}$. The protocol includes the following steps, see also [4, 34]:

(i) In every round of the protocol, the parties do:
State preparation - Alice produces and distributes a multipartite state $\rho_{\boldsymbol{AB}}$. Since we assume an i.i.d. implementation, the source generates the same state in every round.
Measurement - There are two types of measurement rounds, key generation (type-0) and parameter estimation (type-1) measurement rounds. For type 0, the parties choose the inputs $(x, \boldsymbol{y}) = (0, 2, \ldots, 2)$, and for type 1 they choose their inputs $x, y^{(j)} \in \{0, 1\}$ uniformly at random. The parties use a preshared random key to agree on the type of measurement round.

(ii) *Parameter estimation* - The parties publicly communicate the list of bases and outcomes for type-1 rounds and an equal amount of measurement outputs for type-0 rounds. The publicly announced data from type 1 is used to estimate the Bell value $g_{\mathrm{obs}}^{(n)}$ of inequality (16), whereas the announced type-0 data is used to estimate the quantum bit error rate Q, which quantifies the asymptotic error-correction information.

(iii) *Classical postprocessing* - Similar to the device-dependent multipartite QKD protocol [4], an error-correction and privacy-amplification protocol is performed.

If the parties verify, that their data violates our Bell inequality (16), they commence the error correction. The solution of the SDP in the article then upper bounds Eve's guessing probability. If $g_{\mathrm{obs}}^{(n)} \leqslant g_{\mathrm{cl}}^{(n)\downarrow}$ they abort the protocol.

* holzt@uni-duesseldorf.de

[1] M. F. Riedel, D. Binosi, R. Thew, and T. Calarco, Quantum Sci. Technol. **2**, 030501 (2017).

[2] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, *et al.*, New J. Phys. **20**, 080201 (2018).

[3] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, eaam9288 (2018).

[4] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, New J. Phys. **19**, 093012 (2017).

[5] C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984) pp. 175–179.

[6] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[7] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[8] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, 1998) pp. 503–509.

[9] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[10] R. Colbeck, arXiv:0911.3814 (2009).

[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[12] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[13] L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[14] C. A. Miller and Y. Shi, SIAM J. Comp. **46**, 1304 (2017).

[15] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[16] R. Arnon-Friedman, R. Renner, and T. Vidick, SIAM J. Comp. **48**, 181 (2019).

[17] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).

[18] J. Ribeiro, G. Murta, and S. Wehner, Phys. Rev. A **100**, 026302 (2019).

[19] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[20] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's theorem, quantum theory and conceptions of the universe* (Springer, 1989) pp. 69–72.

[21] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

[22] M. Ardehali, Phys. Rev. A **46**, 5375 (1992).

[23] A. V. Belinskiĭ and D. N. Klyshko, Phys. Usp. **36**, 653 (1993).

[24] R. Augusiak, A. Salavrakos, J. Tura, and A. Acín, arXiv:1907.10116 (2019).

[25] T. Holz, D. Miller, H. Kampermann, and D. Bruß, Phys. Rev. A **100**, 026301 (2019).

[26] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007).

[27] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).

[28] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).

[29] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Phys. Rev. Lett. **119**, 040402 (2017).

[30] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).

[31] P. Wittek, ACM Trans. Math. Softw. **41**, 21 (2015).

[32] R. Konig, R. Renner, and C. Schaffner, IEEE Transactions on Information Theory **55**, 4337 (2009).

[33] E. Y.-Z. Tan, R. Schwonnek, K. T. Goh, I. W. Primaatmaja, and C. C.-W. Lim, arXiv:1908.11372 (2019).

[34] J. Ribeiro, G. Murta, and S. Wehner, Phys. Rev. A **97**, 022307 (2018).

[35] J. Briët and P. Harremoës, Phys. Rev. A **79**, 052311 (2009).

[36] R. F. Werner and M. M. Wolf, Phys. Rev. A **61**, 062102 (2000).

[37] R. F. Werner and M. M. Wolf, Phys. Rev. A **64**, 032112 (2001).

[38] D. Gottesman, arxiv:quant-ph/9705052 (1997).

[39] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel, *Entanglement in graph states and its applications*, Proc. Internat. School Phys. Enrico Fermi Vol. 162 (IOS Press, Amsterdam, Netherlands, 2005) pp. 115–218.

[40] I. Pitowsky, *Quantum Probability – Quantum Logic*, Lect. Notes Phys. Vol. 321 (Springer-Verlag, Berlin Heidelberg, 1989) p. 12.

[41] J.-D. Bancal, N. Gisin, and S. Pironio, J. Phys. A: Math. Theor. **43**, 385303 (2010).