Quantum communication: Security analysis and long-distance implementations

Inaugural-Dissertation

zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Sylvia Marta Bratzik

aus Schwientochlowitz, Polen

Düsseldorf, März 2014

Aus dem Institut für Theoretische Physik III
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit der Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Referentin: Prof. Dr. Dagmar Bruß
Koreferent: Prof. Dr. Reinhold Egger

Tag der mündlichen Prüfung: 26. März 2014

„Wir können davon ausgehen, dass die Welt tatsächlich so verrückt ist, wie Einstein hoffte, dass sie es nicht ist.“

[Zeilinger, 2005]

Danksagung

Zu allererst möchte ich Prof. Dr. Dagmar Bruß für die Möglichkeit danken, bei ihr die Doktorarbeit anzufertigen. Auch wenn der Weg nicht immer einfach war, hat sie stets ein offenes Ohr für jegliche Probleme gehabt und zusammen haben immer wir eine Lösung gefunden. Ich schätze sie sehr als Betreuerin. Die Zeit, die ich an ihrem Lehrstuhl verbracht habe, war eine sehr schöne, spannende und inspirierende Zeit.

Dr. Hermann Kampermann danke ich für seine Ratschläge nicht nur von wissenschaftlicher Seite, sondern auch für die Tipps in allen Lebenslagen und die Durchsicht meiner Doktorarbeit. Meinen Bürokollegen Silvestre Abruzzo habe ich als einen sehr kooperativen und stets offenen Mitarbeiter geschätzt. Ihm danke ich für seine konstruktive Kritik und den stetigen wissenschaftlichen Diskurs. Meinen Kollegen Dr. Markus Mertz, Dr. Zahra Shadman, Dr. Alexander Streltsov, Michael Epping, Junyi Wu und Jochen Szangolies danke ich für die wunderbaren Diskussionen und die tolle Atmosphäre am Institut. Michael Epping danke ich vor allem für die Durchsicht meiner Arbeit. Ich werde euch alle vermissen! Auch danke ich besonders Jens Bremer, der sich mit seiner Expertise um unsere Rechner kümmert und uns dadurch für die Forschung den Rücken freihält. Dr. Roland Hützen danke ich für unsere interdisziplinären Diskussionen, die Durchsicht der Doktorarbeit und für seine wertvollen Tipps.

Besonderer Dank geht an Jens, Nils, Angelika und Rainer Pfennig für ihre langjährige Unterstützung. Ich habe euch viel zu verdanken. Vor allem danke ich Jens, der mir in allen Lebenslagen beratend zur Seite stand. Auch danke ich meinen Freunden Sonja, Monica und Henning für lustige Stunden und ihre Unterstützung vor allem in schwierigen Lebenslagen und in der Endphase der Doktorarbeit. Scott Adams danke ich für das Abdrucken des Comics. Auch danke ich allen, deren Lebenswege sich mit den Meinigen gekreuzt haben und mich positiv beeinflusst haben, die ich aber vergessen habe zu erwähnen.

Dem Bundesministerium für Bildung und Forschung danke ich für die finanzielle Unterstützung im Rahmen des Projekts „Quanten-Repeater-Plattform mit Methoden der Quantenoptik“.

Großer Dank gebührt auch meinen Eltern und meiner Familie für ihren Beistand während meiner Promotionszeit.

List of included publications

Bratzik, S., Kampermann, H., and Bruß, D. "Secret key rates for an encoded quantum repeater." `arXiv:1401.6859v1`, *to be published in Physical Review A*, 2014.

Bratzik, S., Abruzzo, S., Kampermann, H., and Bruß, D. "Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate." *Physical Review A* **87**, 062335, 2013.

Abruzzo, S., Bratzik, S., Bernardes, N.K., Kampermann, H., van Loock, P., and Bruß, D. "Quantum repeaters and quantum key distribution: Analysis of secret-key rates." *Physical Review A* **87**, 052315, 2013.

Mertz, M., Kampermann, H., Bratzik, S., and Bruß, D. "Secret key rates for coherent attacks." *Physical Review A* **87**, 012315, 2013.

Summary

Quantum key distribution (QKD) allows to exchange secret keys using the laws of quantum mechanics. These keys are utilized to encrypt messages with the Vernam cipher. Under the assumption that the theory of quantum mechanics is correct and the setup is implemented correctly, this cryptographic system is unconditionally secure meaning that its security does not depend on the computational power and strategy of a potential eavesdropper. The required qubits for QKD are distributed as photons through optical fibers and thus current QKD systems are limited to a few hundred of kilometers due to losses in the fiber. To overcome this problem, quantum repeaters were introduced. In classical telecommunication technology, repeaters enhance the available signal; but in quantum theory simply copying an unknown quantum state is prohibited by the *no-cloning theorem*. Quantum repeaters, however, establish entanglement between qubits which are several hundreds to thousands kilometers apart by relying on fundamental concepts from quantum information theory like entanglement swapping and entanglement distillation.

This thesis covers two topics from quantum communication: Long-distance quantum key distribution via quantum repeaters and security analysis for keys in the regime of a finite number of signals.

On the one hand, secret key rates using quantum repeaters for infinitely many signals are investigated. For this purpose, we present error models for the components of a quantum repeater. We perform a quantitative analysis of the optimal secret key rates in terms of relevant experimental parameters for different implementations of the repeater. Among them are the original quantum repeater, the hybrid quantum repeater, the quantum repeater with atomic ensembles, and the quantum repeater using quantum error-correcting codes. We find that the original quantum repeater can tolerate more gate errors than the hybrid quantum repeater and that the repeater with atomic ensembles is robust against realistic imperfections. We also investigate the influence of different distillation strategies (i.e., distillation protocols and different number of distillation rounds in each nesting level) on the original quantum repeater scheme resulting in quantitative statements about the strategies for obtaining the maximal secret key rate. We derive the rate for generating entangled pairs considering the classical communication times required for entanglement swapping and entanglement distillation. Furthermore, we analyze if different entanglement distillation techniques or the use of quantum error-correcting codes is advantageous in terms of the secret key rate as the quantum repeater using error-correcting codes needs less classical communication time. We find that the former is advantageous for the parameter region studied here.

On the other hand, this thesis is devoted to QKD without repeaters. We derive a bound for the secret key rate for a finite number of signals under the most general form of eavesdropping attacks, namely coherent attacks. So far, not much is known about the difference in secret key rates for collective and coherent attacks if the number of signals is finite but in the limit

they become equivalent. Our results indicate that this does not hold in the finite case.

Zusammenfassung

Quantenschlüsselverteilung erlaubt den Austausch von sicheren Schlüsseln basierend auf den Gesetzen der Quantenmechanik. Diese Schlüssel werden verwendet, um Nachrichten mithilfe der Vernamchiffre zu kodieren. Unter der Annahme, dass die Theorie der Quantenmechanik korrekt ist und dass der Aufbau korrekt implementiert wird, sind diese kryptografischen Systeme bedingungslos sicher. Bedingungslose Sicherheit bedeutet, dass die Sicherheit nicht von der Rechenleistung und der Angriffsstrategie eines potenziellen Lauschers abhängt. Da die benötigten Qubits als Photonen durch die Glasfaberkabel gesendet werden, ist die Quantenschlüsselverteilung aufgrund der Verluste im Kabel leider auf wenige Hundert Kilometer beschränkt. Um dieses Problem zu beheben, wurden Quanten-Repeater eingeführt. In der klassischen Telekommunikationstechnik verstärken Repeater das vorhandene Signal; in der Quantentheorie ist jedoch jegliches Kopieren von unbekannten Quantenzuständen durch das *no-cloning* Theorem verboten. Quanten-Repeater hingegen können Verschränkung zwischen Qubits erzeugen, die Hunderte bis Tausende Kilometern entfernt sind. Dabei basieren sie auf fundamentalen Konzepten aus der Quanteninformationstheorie wie Verschränkungstausch und Verschränkungsdestillierung.

Diese Arbeit befasst sich mit zwei Themen aus der Quantenkommunikation: Quantenschlüsselverteilung über weite Strecken mithilfe von Quanten-Repeatern und die Sicherheitsanalyse für Schlüssel im Bereich von endlich vielen Signalen.

Einerseits werden sichere Schlüsselraten mithilfe von Quanten-Repeatern für unendlich viele Signale untersucht. Zu diesem Zweck präsentieren wir Fehlermodelle für die Komponenten eines Quanten-Repeaters. Wir führen eine quantitative Analyse der optimalen sicheren Schlüsselraten für relevante experimentelle Parameter von verschiedenen Implementierungen des Repeaters durch. Unter diesen Implementierungen sind der ursprüngliche Quanten-Repeater, der hybride Quanten-Repeater, der Quanten-Repeater bestehend aus atomaren Ensembles und ein Quanten-Repeater basierend auf Fehlerkorrektur-Codes. Wir finden heraus, dass der ursprüngliche Quanten-Repeater mehr Gatterfehler als der hybride Quanten-Repeater tolerieren kann und dass der Quanten-Repeater bestehend aus atomaren Ensembles robust gegen realistische Fehler ist. Wir untersuchen auch den Einfluss von unterschiedlichen Destillierungsstrategien (Destillierungsprotokolle und Anzahl der Destillierungsrunden in jedem Zwischenschritt des Quanten-Repeaters) auf den ursprünglichen Quanten-Repeater und können quantitative Aussagen über die Strategien machen, die zu einer maximalen sicheren Schlüsselrate führen. Wir leiten die Erzeugungsrate für verschränkte Paare unter Berücksichtigung der klassischen Kommunikationszeit, die für den Verschränkungstausch und die Verschränkungsdestillierung benötigt wird, her. Des Weiteren analysieren wir, ob verschiedene Destillierungstechniken oder Fehlerkorrektur-Codes von Vorteil bezüglich der sicheren Schlüsselrate sind, da der Quanten-Repeater mithilfe von Fehlerkorrektur-Codes weniger klassische Kommunikation braucht. Wir kommen zu dem Ergebnis, dass ersterer Repeater von

Vorteil ist für die hier betrachtete Parameterregion.

Andererseits ist diese Arbeit der Quantenschlüsselverteilung ohne Repeater gewidmet. Wir leiten eine Grenze für die sichere Schlüsselrate für endlich viele Signale unter der Annahme der allgemeinsten Form von Lauschangriffen (kohärente Attacke) her. Bisher ist nicht viel über den Unterschied von sicheren Schlüsselraten unter kollektiven und kohärenten Lauschangriffen für eine endliche Anzahl von Signalen bekannt; aber im Limes von unendlich vielen Signalen existiert eine Äquivalenz. Unsere Resultate deuten allerdings darauf hin, dass das für endlich viele Signale nicht stimmt.

Contents

1 Introduction

In the history of mankind, inventions for guaranteeing the secrecy of a message are numerous. They range from the Caesar cipher, which is a substitution cipher (i.e, each letter is substituted by another), to modern cryptographic systems relying on prime factorization (for an introduction to the history of cryptography, see [Singh, 1999]). Most of the cryptographic schemes have in common that their safety depends on the computational power available to an adversary, making these protocols *computationally secure*. Prime factorization, for example, has a subexponential[1] running time depending on the size of the integer (see, e.g., [Hoffstein *et al.*, 2008]). But by building a quantum computer [Deutsch, 1985; DiVincenzo, 1996], the running time can be decreased to polynomial scaling by an appropriate algorithm [Shor, 1994], thus compromising the security of these schemes.

The security of *quantum key distribution* [Bennett and Brassard, 1984] or quantum cryptography is not conditioned on the computational power and strategy of a potential eavesdropper, hence this cryptographic system is called *unconditionally secure*. The term quantum cryptography might be misleading as it consists of two parts: distributing the key between the two communicating parties by sending and measuring, e.g., photons and encrypting the message with this key using the *Vernam cipher* [Vernam, 1926] (also called *one-time pad*). The encryption of the bit-message (plaintext) using this cipher consists in adding modulo 2 the preshared key to the plaintext, leading to the so-called ciphertext. The ciphertext is decrypted by reversing the encryption procedure: the same key is added modulo 2 to the ciphertext. This method is called one-time pad, as the key is only used once for every message. It was later shown in [Shannon, 1949] that a multiple use of the key compromises the security. Furthermore, the key has to have the same length as the message. The security of quantum key distribution relies on the fact that incompatible measurement results reveal possible eavesdropping attempts on the established key. The Vernam cipher itself is unconditionally secure as long as the key is equally distributed and completely uncorrelated with the eavesdropper.

Quantum key distribution is developing very fast since its invention almost thirty years ago: commercial quantum key distribution systems are now available on the market [Scarani *et al.*, 2009]. But still these systems are limited to distances of a few hundred kilometers [Stucki *et al.*, 2009] due to the losses in optical fibers. For long-distance quantum key distribution we require so-called *quantum repeaters* [Briegel *et al.*, 1998] to distribute entanglement over large distances. They are based on principles like entanglement swapping and entanglement distillation which are established concepts in quantum information theory. The main purpose of this thesis is to investigate quantum key distribution in the context of quantum repeaters.

[1] Note that subexponential scaling is between exponential and polynomial growth, for further details see [Hoffstein *et al.*, 2008].

Several examinations in this field were performed, but either only on quantum relays (quantum repeaters without distillation) [Collins *et al.*, 2005; Waks *et al.*, 2002; Scherer *et al.*, 2011] or for specific experimental implementations [Razavi *et al.*, 2010; Amirloo *et al.*, 2010].

This thesis is structured as follows: in Chapter 2 we present the theoretical background of classical and quantum information theory. Chapter 3 is devoted to quantum key distribution; we explain the basic concepts and introduce the secret key fraction which is the ratio of the secret key length and the measured bits. The main purpose of Chapter 4 is to introduce the theory of quantum repeaters. We describe the procedures of entanglement swapping and entanglement distillation. Furthermore, we introduce the repeater rate as the production rate of entangled pairs per second and motivate the error models used for the repeater. We explain the strategies how to handle gate errors in the repeater by introducing new distillation protocols and present the concept of quantum repeaters using quantum error-correcting codes. In Chapter 5, we summarize the results of our papers, which are given in the appendix, and in Chapter 6, we discuss possible continuations of our investigations. We finish the thesis by giving a list of the main results in Chapter 7.

2 Theoretical background

In this chapter we develop the necessary mathematical background of quantum information theory [Nielsen and Chuang, 2000].

2.1 Quantum states

The state of a physical system is described by the state vector $|\psi\rangle$ which is an element of the Hilbert space $\mathcal{H}$. A prominent example of a quantum state is the quantum bit (*qubit*):

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

with $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$ and the orthonormal basis states $\{|0\rangle\,, |1\rangle\}$. The qubit is an element of the two-dimensional Hilbert space and the states $|0\rangle$ and $|1\rangle$ can denote, e.g., the energy levels of an atom, the polarization of a photon or the spin of an electron. A qubit can be in a superposition of two states $|0\rangle$ and $|1\rangle$; a phenomenon not known for classical bits.

During the thesis, we will encounter quantum states that are elements of the tensor product of Hilbert spaces. If one party named Alice possesses a quantum state $|\psi_A\rangle \in \mathcal{H}^A$ and the other party (Bob) holds a state $|\psi_B\rangle \in \mathcal{H}^B$, then the total state of both parties together is an element of the Hilbert space $\mathcal{H}^{AB} := \mathcal{H}^A \otimes \mathcal{H}^B$. Any state $|\psi\rangle \in \mathcal{H}^{AB}$ can be written in the Schmidt decomposition as:

$$|\psi\rangle = \sum_{j=1}^{r} a_j\,|e_j\rangle_A\,|f_j\rangle_B\,, \tag{2.2}$$

where $a_j \in \mathbb{R}^{>0}$, $\sum_j a_j^2 = 1$, and $|e_j\rangle_A$ ($|f_j\rangle_B$) are orthonormal states in $\mathcal{H}^A$ ($\mathcal{H}^B$). The number r denotes the Schmidt rank. States for which the Schmidt rank r is greater than one are called *entangled*, otherwise they are called *product states*. Important two-qubit entangled states are the *Bell states*:

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \text{ and } \left|\psi^{\pm}\right\rangle := \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \tag{2.3}$$

Bell states are important for quantum key distribution as explained in Chapter 3.

Quantum systems which are in different quantum states $|\psi_i\rangle$ with probabilities p_i are described by *density matrices*:

$$\rho = \sum_j p_j\,|\psi_j\rangle\,\langle\psi_j|\,, \tag{2.4}$$

with $\sum_i p_i = 1$ and $p_i > 0$. They fulfill the following properties:

- $\mathrm{tr}\,(\rho) = 1$,

- ρ is a positive operator, i.e., $\langle\phi|\rho|\phi\rangle \geq 0 \; \forall \, |\phi\rangle$,
- ρ is hermitean, i.e., $\rho = \rho^\dagger$.

In order to measure the quality of a density operator ρ with respect to a pure state $|\psi\rangle$, we introduce the *fidelity* as

$$F(\rho) = \langle\psi|\rho|\psi\rangle. \tag{2.5}$$

2.2 Quantum computation

The manipulation of quantum states is the topic of this section.

2.2.1 Quantum gates

Quantum gates are unitary[2] matrices, as they follow the rules of quantum mechanics, which require reversible operations. For a single qubit important operations (quantum gates) are the *Pauli operators*, given by the matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.6}$$

By convention, the vector $\binom{1}{0}$ represents the state $|0\rangle$ and the vector $\binom{0}{1}$ the state $|1\rangle$ (often referred to as the *computational basis*). The action of the X-gate on the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ results into a bit-flip: $X\,|\psi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle$. The application of the Z-gate causes a phase-flip: $Z\,|\psi\rangle = \alpha\,|0\rangle - \beta\,|1\rangle$, i.e., the relative phase between the two states is changed. The Y-gate causes a bit- and a phase-flip. Another important qubit gate is the Hadamard-gate, which causes a rotation of the vectors from the computational basis by $\frac{\pi}{4}$:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.7}$$

The basis resulting from the rotation of the computational basis $\{|0\rangle, |1\rangle\}$ is usually called rotated basis: $\{|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. The two bases (the computational and the rotated bases) are essential for quantum key distribution, as we will see in Sec. 2.2.3.

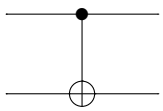
So far, we have treated quantum gates that act on single qubits. An important gate acting on two qubits is the controlled-NOT (CNOT) gate. It consists of one control and one target qubit. A bit-flip (NOT) operation is applied to the target qubit if the control qubit is in the

[2] A matrix U is unitary, when $U^\dagger U = \mathbb{1}$ holds.

state $|1\rangle$. Thus the gate can be written as the unitary operation:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0|^c \otimes \mathbb{1}^t + |1\rangle\langle 1|^c \otimes X^t. \tag{2.8}$$

In the notation of quantum circuits, where each line represents a qubit, the CNOT gate is given by



One important property of the CNOT gate is that it is entangling, thus it is able to produce the Bell states [see Eq. (2.3)] from product states. The circuit given in Fig. 2.1 produces the Bell states.

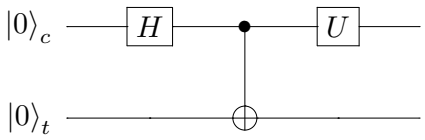


Figure 2.1: Circuit for producing the Bell states, where U is given by $\{\mathbb{1}, X, Y, Z\}$ producing the Bell states $\{|\phi^+\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^-\rangle\}$ up to some global phase.

2.2.2 Quantum operations

A general quantum operation $\mathcal{E}$ maps any density operator ρ into a valid density operator ρ', i.e., $\mathcal{E}(\rho) = \rho'$, where the following axioms must be fulfilled:

- $\rho, \rho' \geq 0$, and $\text{tr}(\rho) = \text{tr}(\rho') = 1$,
- the map $\mathcal{E}$ is a convex-linear map, i.e., it holds that $\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i)$,
- complete positivity is required for the map $\mathcal{E}$. Positivity means that the output of the map $\mathcal{E}(\rho)$ must be a positive operator for any ρ. A map is called completely positive when the output state is positive if the map is only acting on one subsystem of the input state, i.e., it holds that $(\mathbb{1}_A \otimes \mathcal{E}_B)(\rho)$ is positive for any bipartite ρ.

An equivalent representation for the map $\mathcal{E}$ satisfying the axioms above is the Kraus-operator representation [Kraus, 1983]:

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger, \tag{2.9}$$

where $\sum_i E_i^\dagger E_i = \mathbb{1}$ holds for the Kraus operators $\{E_i\}$.

An important map is the so-called *depolarizing map*, as this map simulates the behavior of quantum states in a noisy quantum channel. With probability $1-p$ the state is replaced by the completely mixed state and with probability p it is left unchanged:

$$\mathcal{E}_{\text{dep}}(\rho) = p\rho + (1-p)\frac{\mathbb{1}_2}{2}, \tag{2.10}$$

with $\mathbb{1}_d$ being the $d \times d$ identity matrix.

In the operator-sum representation the map for one qubit looks as follows (with the parametrization $p = \frac{4F-1}{3}$):

$$\mathcal{E}_{\text{dep}}(\rho) = F\rho + \frac{1-F}{3}\left(X\rho X + Y\rho Y + Z\rho Z\right). \tag{2.11}$$

This map is important as it generates the class of *depolarized states*. The action of a depolarizing channel [Eq. (2.11)] on the Bell state $|\phi^+\rangle$ gives

$$\rho_{\text{dep}}(F) := (\mathbb{1} \otimes \mathcal{E}_{\text{dep}}) \left|\phi^+\right\rangle \left\langle\phi^+\right| = F \left|\phi^+\right\rangle \left\langle\phi^+\right| + \frac{1-F}{3}\left(\mathbb{1}_4 - \left|\phi^+\right\rangle \left\langle\phi^+\right|\right), \tag{2.12}$$

Another map is the *partial trace* which results in *reduced density operators*. The partial trace over subsystem B, denoted by $\text{tr}_B(\rho) : \mathcal{H}^A \otimes \mathcal{H}^B \to \mathcal{H}^A$, is given by

$$\text{tr}_B(\rho) = \sum_i E_i \rho E_i^\dagger, \text{ with } E_i = \sum_j |a_j\rangle \langle a_j| \langle b_i|, \tag{2.13}$$

and with the orthonormal states $|a_i\rangle$ ($|b_i\rangle$) of system A (B). The completeness relation $\sum_i E_i^\dagger E_i = \mathbb{1}_{AB}$ is also fulfilled. The partial trace guarantees that the measurement statistics of the remaining subsystem is not changed.

So far, we have defined depolarizing maps for qubits. We can generalize this concept for general maps for n qubits in the sense that with probability p_G an ideal map $\mathcal{E}_{i,j}^{ideal}$ is applied and with probability $(1-p_G)$ we replace this subsystem by the identity matrix:

$$\mathcal{E}_{i,j}^{\text{real}}(\rho) = p_G \mathcal{E}_{i,j}^{\text{ideal}}(\rho) + (1-p_G)\text{tr}_{i,j}(\rho) \otimes \frac{\mathbb{1}_4^{i,j}}{4}, \tag{2.14}$$

where $\text{tr}_{i,j}(\rho)$ is the partial trace on the subsystems i, j and $\mathbb{1}_4^{i,j}$ is the 4×4 identity matrix on the subsystems i and j. This is the error model used for quantum gates throughout the thesis.

2.2.3 Quantum measurements

Quantum measurements are performed via a set of measurement operators $\{E_i\}$, where E_i is the measurement operator associated to the measurement outcome i. These operators have to fulfill the completeness relation, i.e., $\sum_i E_i^\dagger E_i = \mathbb{1}$. The probability of obtaining outcome i is given by $p(i) = \text{tr}\left(E_i^\dagger E_i \rho\right)$. The resulting state after the measurement is given

by $\rho_i = \frac{E_i \rho E_i^\dagger}{p(i)}$.

An example of quantum measurements are projective measurements, i.e., where $E_i^2 = E_i$ holds. In the following we explain how a measurement can alter a state. For this purpose we introduce the measurement operators for the computational basis (mentioned in Sec. 2.2.1 above) which are $E_0 = |0\rangle\langle 0|$ and $E_1 = |1\rangle\langle 1|$ and for the rotated basis $E_+ = |+\rangle\langle +|$ and $E_- = |-\rangle\langle -|$. The probability of obtaining the measurement outcome 0 or 1 when the state $|0\rangle$ is measured is $p(0) = 1$ and $p(1) = 0$. But if we measure the state in the rotated basis, the probabilities of obtaining measurement $+$ or $-$ are equal, i.e., $p(+) = p(-) = \frac{1}{2}$. It means that measuring in the rotated basis, the state vector is projected into this basis, i.e., it is either $|+\rangle$ or $|-\rangle$ after the measurement. If we then once again measure in the computational basis, the probabilities of obtaining outcomes 0 or 1 have drastically changed: $p(0) = p(1) = \frac{1}{2}$. Although we had the state $|0\rangle$ in the beginning, we can have the state $|1\rangle$ in the end. The basic idea of quantum key distribution is to exploit this behavior for detecting an eavesdropper.

2.3 Classical and quantum entropies

The classical (quantum) entropy quantifies the uncertainty about a random variable (quantum state) and is thus related to the security in quantum key distribution as it will be shown in Sec. 3.2.

The concept of entropies in information theory were developed in [Shannon, 1948a,b]. Assume that the random variable X takes the value x with probability $p(x)$, then the *Shannon entropy* related to the probability distribution of this random variable is defined to be

$$H(X) = \sum_x p(x) \log_2 p(x), \tag{2.15}$$

with the convention that $0 \log_2 0 = 0$ holds. The logarithm is taken to be in base two, as the entropy is conventionally measured in bits. In the case where the random variable takes two values, one with probability p and the other with $1 - p$, the Shannon entropy is given by

$$h(p) := -p \log_2 p - (1-p) \log_2 (1-p), \tag{2.16}$$

which is also called the *binary Shannon entropy*. For two random variables X and Y, the *joint entropy* measures the total uncertainty of the pair (X, Y):

$$H(X,Y) = \sum_{x,y} p(x,y) \log_2 p(x,y), \tag{2.17}$$

where $p(x, y)$ is the probability that the random variable $X\,(Y)$ takes value $x\,(y)$. When knowing the random variable Y, we can define the *entropy of X conditioned on the knowledge*

of Y (conditional entropy):

$$H(X|Y) = H(X,Y) - H(Y). \tag{2.18}$$

The *mutual information* of the random variables X and Y represents the information we can learn about X by knowing Y:

$$I(X,Y) = H(X) + H(Y) - H(X,Y). \tag{2.19}$$

For quantifying information of quantum states we use the eigenvalues of the density operators instead of probability distributions. The *von Neumann entropy* [von Neumann, 1927] for a quantum state ρ is defined as

$$S(\rho) := -\mathrm{tr}\,(\rho \log \rho) = -\sum_i \lambda_i \log \lambda_i, \tag{2.20}$$

where $\{\lambda_i\}_i$ are the eigenvalues of ρ. The conditional entropy of a composite system ρ_{AB} is given by

$$S(A|B) = S(A,B) - S(B) = S(\rho_{AB}) - S(\rho_B), \tag{2.21}$$

where ρ_B is defined as the partial trace [see Eq. (2.13)] over the system A of the state ρ_{AB}, i.e., $\rho_B = \mathrm{tr}_A(\rho_{AB})$.

Another important entropy which we will encounter in the chapter about quantum key distribution for finite keys is the *min-entropy*. The min-entropy in classical information theory defines the uncertainty of correctly guessing the value of the random variable in one single trial: $H_{\min}(X) = -\log \max_x p(x)$ (see, e.g., [Renner and König, 2005]). R. Renner developed a formalism for the quantum min-entropy in his PhD thesis [Renner, 2008]. For two density operators ρ_{AB} and σ_B the conditional min-entropy is defined as [Renner, 2008]:

$$H_{\min}(\rho_{AB}|\sigma_B) := -\log\left(\min_{\lambda\in\mathbb{R}} \lambda \cdot \mathbb{1}_A \otimes \sigma_B - \rho_{AB} \geq 0\right), \tag{2.22}$$

where $\sigma - \rho \geq 0$ means that the eigenvalues of the operator $\sigma - \rho$ are non-negative. When we take the supremum over all arbitrary states σ_B, we write

$$H_{\min}(\rho_{AB}|B) := \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B). \tag{2.23}$$

The operational meaning of the min-entropy becomes clear by using the result from [König *et al.*, 2009]: First, let ρ_{XE} be a *classical-quantum state*, i.e.,

$$\rho_{XE} = \sum_x p_x \left|x\right\rangle\left\langle x\right| \otimes \rho_E^x. \tag{2.24}$$

The classical-quantum state describes the system when party A has measured her system (resulting in her classical system X) but the quantum party E is possessing information

about the outcome of this measurement encoded in her state ρ_E^x. Second, let the set $\{M^x\}_x$ be the elements of a positive operator valued measure (POVM)[3] for system E, then

$$H_{\min}(\rho_{XE}|E) = -\log p_{\text{guess}}, \tag{2.25}$$

where the guessing probability p_{guess} is given by

$$p_{\text{guess}} := \max_{\{M^x\}_x} \sum_x p_x \text{tr}(M^x \rho_E^x). \tag{2.26}$$

The min-entropy is thus related to the maximal probability p_{guess} of correctly guessing the outcome of a random variable X when we only possess system E.

We introduce the *ε-smooth min-entropy* by taking the supremum of all states with trace distance ε to the original state, i.e.,

$$H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) := \sup_{\bar{\rho}^{AB}} H_{\min}(\bar{\rho}_{AB}|\sigma_B), \tag{2.27}$$

with $||\rho^{AB} - \bar{\rho}^{AB}||_1 \leq \varepsilon$. The trace-norm $||\rho||_1$ of a state ρ is defined as $||\rho||_1 := \text{tr}\left(|\rho|\right) = \text{tr}\left(\sqrt{\rho^\dagger \rho}\right)$. The smoothing is essential as small modifications of the state have a large impact on the entropy (see [Renner, 2008] for examples). The relation between the von Neumann and the min-entropy is [Renner, 2008]

$$\frac{1}{n} H_{\min}^{\varepsilon}(\rho_{XE}^{\otimes n}|\rho_E^{\otimes n}) \geq S(X|E) - \delta, \tag{2.28}$$

where $\delta := (2\log \text{rank}(\rho_X) + 3)\sqrt{\log(2/\varepsilon)/n}$ and ρ_{XE} is a classical-quantum state [see Eq. (2.24)]. In [Tomamichel *et al.*, 2009] it was shown that the ε-smooth min-entropy converges to the von Neumann entropy:

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\varepsilon}(\rho_{XE}^{\otimes n}|\rho_E^{\otimes n}) = S(X|E). \tag{2.29}$$

This result it also known as the quantum asymptotic equipartition property (AEP). The classical AEP states that the outcome of a random experiment is given by a sequence of independent and identically distributed (i.i.d.) random variables $(X_1, ..., X_n)$ with probability close to $2^{-nH(X)}$ [Cover and Thomas, 2006]. Thus all events are equally likely. It is a consequence of the weak law of large numbers, where the value of $\frac{1}{n}\sum_i X_i$ approaches the expectation value of the random variable X for large n. The quantum AEP is a generalization for a classical random variable X with quantum side information E.

[3] The operators of this measurement are positive and fulfill the completeness relation, see Sec. 2.2.3.

3 Quantum key distribution

3.1 Introduction

The aim of quantum key distribution is to generate a correlated string of symbols, e.g., bits between two parties, which are usually called Alice and Bob. Alice and Bob use the laws of quantum mechanics in their favor to distribute a secret key, hence the name *quantum key distribution* (a review on quantum key distribution can be found in [Scarani *et al.*, 2009]). In order to start with the secret transmission of the keys, both parties should *authenticate* each other's identity. For authentication the parties need a preshared key, thus the procedure is sometimes referred to as *quantum key growing* (see, e.g., discussion in [Alleaume *et al.*, 2007]). The first known quantum key distribution protocol is the *BB84-protocol* [Bennett and Brassard, 1984] named after their inventors C. H. Bennett and G. Brassard[4] and it contains the following steps:

(1) **State distribution:** Alice randomly prepares states in the computational basis $\mathcal{B}_0 = \{|0\rangle, |1\rangle\}$ (encoding each the classical bits '0' and '1') or in the rotated basis $\mathcal{B}_+ = \{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ (encoding '0' and '1') and sends them to Bob. The sequence of bits is noted as it later serves for the key.

(2) **Measurement:** Bob randomly measures the qubits in the bases $\mathcal{B}_0$ or $\mathcal{B}_+$ and records the measurement basis and the measurement outcome.

(3) **Sifting:** Alice and Bob compare their choices of bases over an authenticated channel and keep only those measurement outcomes where their measurement bases coincided. It is important to note that no information about the outcome of the measurements is revealed.

(4) **Classical postprocessing:** Alice and Bob reveal a fraction of their keys in order to estimate the error (which could have been introduced either by the channel or an eavesdropper), apply an error correction algorithm to the remaining bits and decrease the eavesdropper's (possible) knowledge by procedures known as privacy amplification (see [Scarani *et al.*, 2009] for a review).

As Alice prepares the quantum states and sends them to Bob, this scheme is called *prepare-and-measure* scheme. An equivalent description with a source of entangled Bell pairs (see Eq. (2.3) in Sec. 2.1) placed in the middle between Alice and Bob[5] is provided in [Ekert,

[4] S. Wiesner should also be acknowledged as he had the idea of quantum money in the early seventies, but his idea was only published in 1983 [Wiesner, 1983].

[5] The source can also be equivalently placed in Alice's lab.

1991; Bennett *et al.*, 1992]. The source could also belong to a potential eavesdropper who pretends to send entanglement states, but in reality only sends classically correlated states. Alice and Bob can discover the fraud as their results would not be correlated anymore and the measurement results would not violate the CHSH-inequality [Clauser *et al.*, 1969] which can only be violated by entangled quantum states. It was shown in [Curty *et al.*, 2004] that entanglement is a necessary prerequisite for QKD. The reader might then think that the eavesdropper could also produce entangled states which are tripartite entangled like the so-called GHZ-state [Greenberger *et al.*, 1990] $\frac{1}{\sqrt{2}}(|000\rangle_{ABE} + |111\rangle_{ABE})$, but entanglement is monogamous [Koashi and Winter, 2004] thus Alice and Bob are not fully entangled anymore as in the case of Bell states and this can also be detected.

3.2 Security of quantum key distribution

The security of a cryptographic setting can be either *computationally* or *unconditionally secure* (see, e.g., [Maurer, 1999]). As already mentioned in the introduction, classical cryptographic protocols are only computationally secure; the development of quantum computers presents, e.g., a serious threat for the security. The advantage of quantum key distribution is that it is *unconditionally secure* thus technological advances would not compromise its security.

In the following we will describe the possible eavesdropping attacks relevant for our work and then introduce the notion of secret key rates, which gives the amount of extractable secret bits divided by the initially sent quantum states. The secret key rate is the product of the secret fraction and the raw key rate, which is the key rate before the classical postprocessing ([Scarani *et al.*, 2009], see also Eq. (5.3) in Sec. 5.2).

3.2.1 Eavesdropping attacks

We divide the attacks by an eavesdropper into individual, collective, and coherent attacks (see, e.g., [Scarani *et al.*, 2009]). For the individual attacks we assume the following: Eve attacks the states sent from Alice to Bob independently and with the same strategy; she measures her ancillas (the auxiliary system that she appended to Alice's states) before the classical post-processing. In the collective attack scenario Eve has more power: she is allowed to keep her ancillas in a quantum memory, but is still restricted to attack each of the states independently. The most general attack is the coherent attack. In this case Eve is not restricted at all.

3.2.2 Asymptotic secret fraction

We are now interested how to measure the amount of secrecy between Alice and Bob. We know that the mutual information $I(X, Y)$ of two random variables X and Y quantifies their common knowledge (see Sec. 2.3). In order to determine Alice's and Bob's unique knowledge about X and Y, we have to subtract Eve's knowledge about their random variables from

the mutual information. The fraction of secret bits over sent signals (*secret fraction*, in the asymptotic limit and for one-way classical postprocessing [Scarani *et al.*, 2009]) is given by

$$r_\infty = \lim_{N\to\infty} \frac{\ell}{N} = I(X,Y) - \max(I_{XE}, I_{YE}), \tag{3.1}$$

where I_{XE} and I_{YE} depend on the eavesdropping strategy. In the case of individual attacks the quantities I_{XE} and I_{YE} are given by the mutual information maximized over all eavesdropping strategies, i.e., $I_{XE} = \max_E I(X,E)$ or $I_{YE} = \max_E I(Y,E)$ (Csiszár-Körner bound [Csiszár and Körner, 1978]). In the case of collective attacks $I_{XE} = \max_E \chi(X,E)$ [Devetak and Winter, 2005], where $\chi(X,E)$ is the Holevo quantity [Holevo, 1973]:

$$\chi(X,E) = S(E) - \sum_x p_x S(\rho_E^x), \tag{3.2}$$

with $\rho_{XE} = \sum_x p_x |x\rangle\langle x| \otimes \rho_E^x$ being a classical-quantum state. In this case Eq. (3.1) is called *Devetak-Winter bound* [Devetak and Winter, 2005] and can be rewritten as

$$\begin{aligned} r_\infty &= I(X,Y) - \chi(X,E) = H(X) - H(X|Y) - S(E) + \sum_x p_x S(\rho_E^x) && (3.3)\\ &= S(X|E) - H(X|Y), && (3.4) \end{aligned}$$

where we used that $S(X|E) = S(X,E) - S(E)$ and $S(X,E) = H(X) + \sum_x p_x S(\rho_E^x)$ (joint-entropy theorem, see [Nielsen and Chuang, 2000]).

If the initial state between Alice and Bob is of Bell-diagonal form, i.e.,

$$\rho_{AB} = A\left|\phi^+\right\rangle\left\langle\phi^+\right| + B\left|\phi^-\right\rangle\left\langle\phi^-\right| + C\left|\psi^+\right\rangle\left\langle\psi^+\right| + D\left|\psi^-\right\rangle\left\langle\psi^-\right|, \tag{3.5}$$

the secret fraction for the *BB84*-protocol is given by [Scarani *et al.*, 2009]:

$$r_\infty^{\mathrm{BB84}} = 1 - h(e_Z) - h(e_X), \tag{3.6}$$

where $h(p)$ is the binary entropy given in Eq. (2.16), and

$$e_Z = C + D \text{ and } e_X = B + D \tag{3.7}$$

are the error rates in the Z-basis ($\mathcal{B}_0$) and in the X-basis ($\mathcal{B}_+$). The error rate in basis i is defined to be the fraction of discordant bits, i.e., $e_i := \frac{1}{2}\left(\langle 01|\rho|01\rangle_i + \langle 10|\rho|10\rangle_i\right)$. The description of a qubit using only measurements in the X- and Z-basis is not complete; as the qubit is represented in the Bloch sphere (see, e.g., [Nielsen and Chuang, 2000]), an additional basis is required, the Y-basis. Its basis states $\left\{\frac{1}{\sqrt{2}}\left(|0\rangle + i\,|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - i\,|1\rangle\right)\right\}$ are the eigenstates of the Pauli Y-matrix [see Eq. (2.6)] and can also be used for quantum key distribution. This is the idea of the *six-state* protocol [Bruß, 1998; Bechmann-Pasquinucci and Gisin, 1999]. It results in a higher secret fraction than the *BB84-protocol*, because we can determine all parameters of the quantum state. The secret fraction for the *six-state* protocol

is [Scarani *et al.*, 2009; Renner, 2008]:

$$r_{\infty}^{\text{six-state}} := 1 - e_Z h\left(\frac{1+(e_X-e_Y)/e_Z}{2}\right) - (1-e_Z)h\left(\frac{1-(e_X+e_Y+e_Z)/2}{1-e_Z}\right) - h(e_Z), \tag{3.8}$$

with

$$e_Y = B + C. \tag{3.9}$$

It was shown in [Kraus *et al.*, 2005; Renner *et al.*, 2005] that collective and coherent attacks are equivalent under certain restrictions and under the assumption of infinitely many signals. An equivalence has not yet been proved for a finite number of signals. We showed in our publication [Mertz *et al.*, 2013] that they might be inequivalent in the finite regime.

3.2.3 Finite-key analysis

Finite-key analysis is the study of secret key rates under the assumption of a finite number of signals. We have already introduced in Sec. 2.3 the notion of the ε-smooth min-entropy [Eq. (2.27)] and its connection to the von Neumann entropy [Eq. (2.28)]. It was shown in [Renner, 2008; Scarani and Renner, 2008] that the secret key rate of an ε-secure key for a finite number of signals is given by

$$r = \frac{1}{N}\inf_{\rho_{AB}\in\Gamma_\xi}\left(H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n}|E^n\right) - \text{leak}_{\text{EC}}\right) + \frac{2}{N}\log_2\left(2\varepsilon_{PA}\right). \tag{3.10}$$

The probability $\varepsilon := \varepsilon_{\text{PE}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} + \bar{\varepsilon}$ describes the probability that the key is not secure[6] and any of the classical postprocessing procedures failed. The abbreviation PE stands for *parameter estimation* (Alice and Bob estimate the error in the channel), EC stands for *error correction* and PA for *privacy amplification* (see [Scarani *et al.*, 2009] for an introduction). Different to other approaches for deriving finite-key rates (see, e.g., [Scarani and Renner, 2008]), the secret key rate presented here is composably secure. Composability means that the secret key generated by these procedures remains secure if used for other application like one-time pad encryption (see Chapter 1) [Renner, 2008]. The set Γ_ξ contains all the states that are compatible with the measurement statistics for parameter estimation, where ξ is the deviation of the measured to the real parameter (see below). In parameter estimation we estimate the statistics of the data by using a small subset of the sample. Assume that we have sent $m+n$ quantum states, and we perform measurements on m signals to estimate the error Q_m in the channel. We are now interested in the deviation of Q_m to the error Q_n which we would obtain if we would measure the remaining n signals. We cannot measure these signals as we want to use them for our secret key. It holds except with probability ε_{PE} that $\frac{1}{2}||Q_m - Q_n||_1 \leq \xi$. The last term in Eq. (3.10) is the leakage term for error correction

[6] We define a key to be ε-secure, if the trace distance to the uniformly distributed and completely uncorrelated key is given by ε (see, e.g., [Renner, 2008]).

leak_{EC}. It is defined by

$$\text{leak}_{\text{EC}} := nfH(X|Y) + \log_2(2/\varepsilon_{\text{EC}}), \tag{3.11}$$

where n is the number of signals on which we perform error correction and f is the efficiency of the error correction protocol. The efficiency of the error correction protocol is given by the length of the conversation (measured in the number of exchanged symbols) divided by the optimal conversation length, which is given by the *Shannon limit* (see, e.g., [Elkouss *et al.*, 2011]). For infinitely many signals the efficiency f is assumed to be 1. Recent error correction protocols can approach the Shannon limit by achieving good efficiencies of $f = 1.05 - 1.1$ [Elkouss *et al.*, 2011]. Recently, it was found [Tomamichel *et al.*, 2014] that the estimate of the leakage term given in Eq. (3.11) is too optimistic using $f = 1.1$ for the finite-key regime. In their paper they propose a two-parameter estimation that is more suited to the finite-key effects.

4 Quantum repeaters

4.1 Introduction

The concept of quantum repeaters was introduced in [Briegel *et al.*, 1998] and aims at distributing entanglement over distances greater than several hundreds of kilometers. The necessity for the development of quantum repeaters is that the photon transmission probability decays exponentially with the length of the optical fiber (Beer-Lambert's law, see, e.g., [Demtröder, 2005]):

$$P_t = e^{-L/L_{\text{att}}} = 10^{-\alpha L/10}, \tag{4.1}$$

where L_{att} is the attenuation length, i.e., the length where the probability of transmission drops to e^{-1} and α is called the attenuation coefficient and is measured in dB/km. For wavelengths used in telecommunication the attenuation coefficient is 0.35 dB/km at 1310 nm and 0.2 dB/km at 1550 nm [Gisin *et al.*, 2002]. If we send one photon at 1550 nm to a receiver at 100 km, the probability of transmission is $P_t = 0.01$, at 600 km it is $P_t = 10^{-12}$ and at 1000 km it is already $P_t = 10^{-20}$. Even for a single-photon repetition rate of 10 GHz (repetition rates of 50 MHz are available nowadays [Lee *et al.*, 2011]), on average one photon arrives every 318 years at a distance of 1000 km. Obviously, this is not feasible.

The quantum repeater uses techniques of *entanglement swapping* and *entanglement distillation* to extend the entanglement over a long distance. The basic principle is shown in Fig. 4.1: the distance between Alice and Bob is L. To distribute an entangled pair over

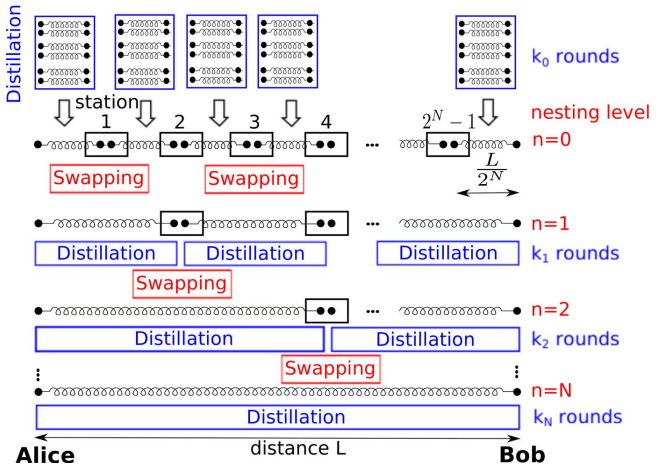


Figure 4.1: Quantum repeater, figure taken from [Bratzik *et al.*, 2013].

this distance, they divide the distance L in equidistant parts with length $L_0 = L/2^N$ and

place a repeater station at every division point. Using entanglement distillation they increase the quality of the quantum state and by entanglement swapping two repeater stations are entangled that did not shared any entanglement before. These concepts will be described in the following.

4.1.1 Entanglement swapping

For entanglement swapping [Żukowski *et al.*, 1993] two distant parties want to share entanglement that never interacted before. In Fig. 4.2, Alice and Bob each share entanglement with Charlie, but not with one another. Charlie performs a Bell measurement and sends the result to Bob, who depending on the measurement result applies an unitary operation on his qubit[7]. Then Alice and Bob are entangled with each other. This scenario works perfectly

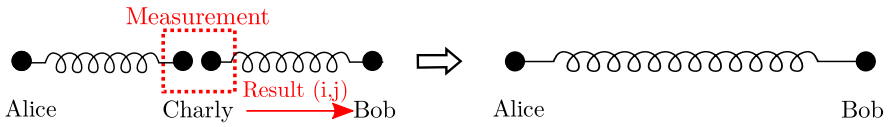


Figure 4.2: Principle of entanglement swapping.

as long as the devices and the states are perfect. For mixed states of depolarized form [see Eq. (2.12)], i.e.,

$$\rho_{\text{dep}}(F) = F\left|\phi^+\right\rangle\left\langle\phi^+\right| + \frac{1-F}{3}\left(\mathbb{1}_4 - \left|\phi^+\right\rangle\left\langle\phi^+\right|\right), \tag{4.2}$$

the fidelity [Eq. (2.5)] after swapping N pairs is given by [Briegel *et al.*, 1998]

$$F_N = \frac{1}{4}\left[1 + 3\left(\frac{4F-1}{3}\right)^N\right], \tag{4.3}$$

thus decreases exponentially in the number of swappings N.

4.1.2 Entanglement distillation

The concept of entanglement distillation was presented in [Bennett *et al.*, 1996a]. There, the initial states used for distillation are depolarized states [Eq. (2.12)]. By applying appropriate bilateral rotations (this operation is called *twirl*), any two-qubit state can be transformed to a depolarized state [Bennett *et al.*, 1996a]. Assume that we distributed two of these pairs to Alice and Bob, i.e., they hold the total state:

$$\rho_{\text{tot}} = \rho_{\text{dep}}(F_0)_{a1,b1} \otimes \rho_{\text{dep}}(F_0)_{a2,b2}, \tag{4.4}$$

where Alice (Bob) holds particles $a1$ ($b1$) and $a2$ ($b2$) (see Fig. 4.3). We want to generate a pair $\rho_{\text{dep}}(F_1)_{a1,b1}$ with $F_1 > F_0$. This is achieved by local operations and classical communication: Alice and Bob each perform a CNOT operation [see Eq. (2.8)] on their qubits with $a1$

[7] This information is needed in order to know which of the four Bell states [see Eq. (2.3)] Alice and Bob share.

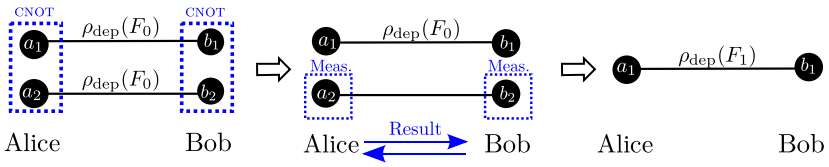


Figure 4.3: Entanglement distillation.

$(b1)$ as control and $a2$ $(b2)$ as target qubits. Then they both perform a measurement in the computational basis on their qubits a_2 and b_2 and communicate the result of the measurement to each other. If their measurement results coincide they have successfully generated $\rho_{\text{dep}}(F_1)_{a1,b1}$. If their results do not match, they throw away the pairs, as the fidelity F_1 of the resulting pairs is lower than F_0 (it is even $F_1 = 0.25$, thus they have a completely mixed state). Note that the process of entanglement distillation is probabilistic and requires two-way classical communication. For protocols with one-way classical communication see [Bennett *et al.*, 1996b]. The procedure is successful as the bilateral CNOT operation and the measurements increase the probability of the appearance of the state $|\phi^+\rangle$ in the resulting mixed state [see Eq. (2.4)] and thus the fidelity. In the case of the described distillation protocol, the fidelity after one round of entanglement distillation is [Bennett *et al.*, 1996b]:

$$F_D = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}. \tag{4.5}$$

The probability that this entanglement distillation procedure is successful is given by the denominator of Eq. (4.5).

Other distillation protocols are presented in Sec. 4.3.

4.1.3 Quantum repeater strategies

In this section we explain why entanglement swapping and entanglement distillation is in principle needed for the quantum repeater. In Fig. 4.4 the procedure is explained. If we start with a fidelity of around $F = 0.95$ it decreases due to swapping as shown in the picture. In order to achieve the same fidelity as in the beginning, we have to perform several rounds of distillation. For quantum key distribution, it is not always advantageous to have the setup for the repeater as depicted in Fig. 4.1 with entanglement distillation after each swapping. Additionally, it is also not necessary to distill to the same fidelity before swapping as shown in Fig. 4.4. As entanglement distillation is probabilistic, multiple rounds of distillation, have an impact on the rate of generating entangled pairs (see Sec. 4.1.4 and our publications [Abruzzo *et al.*, 2013; Bratzik *et al.*, 2013]). In our publication [Bratzik *et al.*, 2013], we focus on the best *distillation strategy* for obtaining the optimal secret key rate. By distillation strategy we mean the number of rounds in each nesting level (see Sec. 5.2.2).

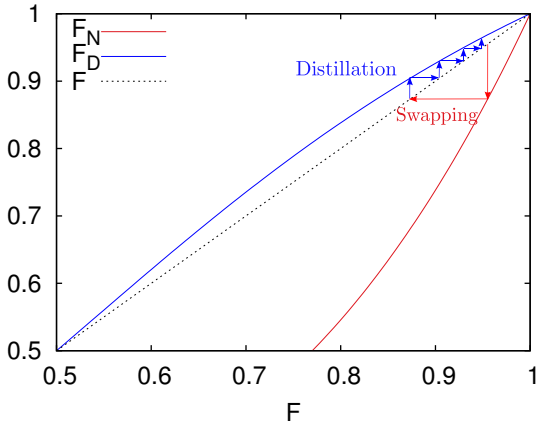


Figure 4.4: The purification loop. Figure adapted from [Briegel *et al.*, 1998]. The function F_N [Eq. (4.3)] denotes the swapping of $N = 3$ pairs and F_D [Eq. (4.5)] gives the resulting fidelity after one round of distillation.

4.1.4 Repeater rate

We are now interested in the rate of the quantum repeater, i.e., the production rate of entangled pairs per second. This quantity is called *repeater rate* which is important in our publications [Abruzzo *et al.*, 2013; Bratzik *et al.*, 2013, 2014], where these rates are derived for different quantum repeater schemes.

For this purpose, we think about the following game: consider that we have N coins which we toss in parallel at certain discrete time steps T. The probability of obtaining head is given by P and for tail $1 - P$. If we obtain head, the corresponding coin is kept and not flipped anymore. We stop the game, when all coins are flipped to head (assuming that the initial value for all coins is neither head or tail in the beginning). The average waiting time τ_N of this game is given by the expectation value of the random variable with probability distribution $p_N(m)$ times T. The distribution $p_N(m)$ gives the success after m time steps for N coins. For one single coin it is $p_1(m) = (1 - P)^{m-1}P$. The average waiting time for one coin is [Sangouard *et al.*, 2011]

$$\tau_1 = T \sum_{m=1}^{\infty} m\, p_1(m) = \frac{T}{P}. \tag{4.6}$$

For two coins the probability distribution is given by the maximum waiting time for each of the coins [Sangouard *et al.*, 2011]:

$$p_2(m) = p_1(m)^2 + 2p_1(m) \sum_{j=1}^{m-1} p_1(j). \tag{4.7}$$

It can be explained as follows: either both coins are successful (i.e., show head) after m time steps (first term) or one succeeds after m steps whereas the other coins already succeeded

after $j < m$ steps (second term). The expected waiting time is given by [Sangouard *et al.*, 2011]

$$\tau_2 = \frac{3-2P}{(2-P)P}T \approx \frac{3T}{2P}, \tag{4.8}$$

for small P. In [Bernardes *et al.*, 2011], the general formula for the average waiting time in units of T was developed:

$$\tau_N = TZ_N(P), \tag{4.9}$$

where

$$Z_N(P) := \sum_{j=1}^{N} \binom{N}{j} \frac{(-1)^{j+1}}{1-(1-P)^j}. \tag{4.10}$$

The connection to the repeater rates is the following: assume that we have $2^N - 1$ repeater stations (see Fig. 4.1) and swapping is deterministic, i.e., the probability of swapping is $P_{ES} = 1$, then the repeater rate, which is the reciprocal value of the average waiting time, is given by:

$$R_{\text{Rep}}^{\text{det}} = \frac{1}{T_0 Z_{2^N}(P_t)}, \tag{4.11}$$

where $T_0 = \frac{L_0}{c}$ is the time a photon travels over the distance $L_0 = L/2^N$ and P_t is the probability that the photon arrives at the repeater station [see Eq. (4.1)]. Thus, the generation of entanglement in the quantum repeater procedure corresponds to the coin tossing problem described above. In our publication [Abruzzo *et al.*, 2013] we derive the repeater rates for different scenarios, i.e., when entanglement swapping is probabilistic and when distillation is included.

4.2 Imperfections in quantum repeater components

The quantum repeater consists of many components, such as the source of entanglement, the detectors, the gates and the quantum memories. Each of these components can be subjected to imperfections that will be described in the following.

The source of entanglement in general depends on the following parameters: the probability of generating entangled pairs, the efficiency, the repetition rate and the fidelity of these pairs. In the ideal case, the source produces entangled Bell pairs with an infinite repetition rate and on demand. For realistic sources, the error model of the resulting pairs is the depolarizing map as introduced in Sec. 2.2.2, Eq. (2.11). For the detectors, we assume them to be photon-number resolving. They are described by the POVM elements [Kok and Lovett, 2010]

$$\Pi^{(n)} := \eta_{\text{d}}^n \sum_{m=0}^{\infty} \binom{n+m}{n} (1-\eta_{\text{d}})^m \left|n+m\right\rangle \left\langle n+m\right|, \tag{4.12}$$

where the element $\Pi^{(n)}$ corresponds to the detection of n photons and η_{d} is the detector efficiency (the probability that the detector clicks upon arrival of a photon). The notation $|n+m\rangle$ denotes here a state of $(n+m)$ photons. Usually, commercial photon detectors are

also subjected to dark counts, i.e., the detector counts a non-existing photon. We showed in our publication [Abruzzo *et al.*, 2013] that dark counts on the order of 10^{-5} are negligible. Available detectors can reach this threshold (see, e.g., [Scarani *et al.*, 2009]). For the gate errors, we assume the depolarizing model [see Sec. 2.2.2, Eq. (2.14)], i.e., with probability p_G the perfect operation is performed, whereas with probability $1-p_G$ the affected subsystem is replaced by a completely mixed state. This is the worst estimate of a gate error as the completely mixed states contains no useful information about the initial state anymore. Quantum memories are an essential part of the quantum repeater. For a recent review on quantum memories, see [Simon *et al.*, 2010]. Throughout our publications, we assume our memories to be perfect, except for the quantum repeater with atomic ensembles in Sec. 5.2.1.3, where we employ the memory efficiency η_{m}. It gives the probability that the photon is undisturbed after it was stored in the memory. There are other imperfections that we did not consider here such as the photon conversion efficiency, fiber coupling losses, and so on (see [Sangouard *et al.*, 2011] for further details); but they can be easily implemented into our analysis. The losses in the fiber are modeled by the transmission probability given in Eq. (4.1).

4.3 Entanglement distillation strategies

In this section we will describe how to improve the distillation protocol introduced in Sec. 4.1.2. In the following we present two distillation protocols: the *Deutsch et al.* and the *Dür et al.* distillation protocol. The latter was introduced in [Briegel *et al.*, 1998; Dür *et al.*, 1999], where the quantum repeater was analyzed regarding the gate errors; this distillation protocol is more robust against gate errors.

In [Deutsch *et al.*, 1996] the *Deutsch et al.* protocol which is more efficient than the protocol described in Sec. 4.1.2 was introduced. The efficiency refers to the final fidelity, as the *Deutsch et al.* protocol converges faster to unity. The only difference to the protocol given in Sec. 4.1.2 (which will now be called *Bennett et al.* protocol) is that after the application of the CNOT Alice employs the following transformation to her qubits

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle - i\,|1\rangle\right) \tag{4.13}$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|1\rangle - i\,|0\rangle\right), \tag{4.14}$$

and Bob's transformation is:

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + i\,|1\rangle\right) \tag{4.15}$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|1\rangle + i\,|0\rangle\right). \tag{4.16}$$

For the reader familiar with the Bloch vector representation of a qubit (see, e.g., [Nielsen and Chuang, 2000]), Alice's (Bob's) transformation corresponds to a $\frac{\pi}{2}$ ($\frac{-\pi}{2}$)-rotation about the

X-axis.

Under the influence of gate errors as given in Sec. 2.2.2, an analysis of the error resistance of both distillation protocols was performed in [Dür *et al.*, 1999]. The result was that the *Deutsch et al.* protocol is more resistant to errors than the *Bennett et al.* protocol. In [Dür *et al.*, 1999], another protocol, which is more efficient than the *Deutsch et al.* protocol under gate errors, was invented. It works as follows: compared to the *Deutsch et al.* protocol that distills pairs with the help of pairs with the same fidelity (see Fig. 4.5), the *Dür et al.* protocol (see Fig. 4.6), distills pairs using pairs with different fidelities. The advantage of this protocol is that it uses less gates than the *Deutsch et al.* protocol and thus can tolerate higher gate errors. But when using perfect gates, this protocol is not efficient as it will never result in a fidelity of 1. Another difference is the number of resources, i.e., qubits, used in

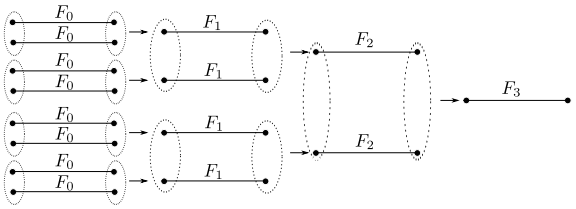


Figure 4.5: The *Deutsch et al.* protocol. The fidelity in the k-th distillation round is denoted by F_k. Figure adapted from [Dür *et al.*, 1999].

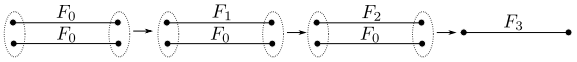


Figure 4.6: The *Dür et al.* protocol. Figure adapted from [Dür *et al.*, 1999].

these procedures. As it can be seen on Figs. 4.5 and 4.6, the number qubits needed for the *Deutsch et al.* protocol grows exponentially with the number of distillation rounds, whereas for the *Dür et al.* protocol, it grows linearly. When considering several nesting levels and $\vec{k} = (k_0, ..., k_N)$ being the distillation vector (k_i is the number of distillation rounds in the i-th nesting level), the number of memories needed per half repeater node is given by [Bratzik *et al.*, 2013]

$$M^{\mathrm{D}} = 2^{\sum_n k_n} \tag{4.17}$$

for the *Deutsch et al.* protocol and

$$M^{\mathrm{Dür}} = N + 2 + |\{k_i : k_i = 0\}| \tag{4.18}$$

for the *Dür et al.* protocol, where N is the total number of nesting levels and the set $|\{k_i : k_i = 0\}|$ is the number of elements in $\vec{k}$ that are zero.

In our publication [Bratzik *et al.*, 2013] we investigate the relation of obtaining the optimal secret key rate and the required resources by evaluating the optimal secret key rate per memory per second. The results are described in Sec. 5.2.2.

4.4 Quantum repeaters with encoding

In order to correct and detect errors on a quantum state, quantum error correction was developed (see, e.g., [Nielsen and Chuang, 2000] for an introduction). As in the classical case, an encoding and decoding procedure is applied. We encode k logical qubits in n physical qubits. The logical qubits for $|0\rangle$ and $|1\rangle$, denoted by $|0_L\rangle$ and $|1_L\rangle$, span a two-dimensional subspace. When errors occur on the qubits[8], the error operators map this subspace to other subspaces. The errors are distinguishable (and thus correctable), if the subspaces are pairwise orthogonal. If we measure the state which was subjected to errors with appropriate projectors (see Sec. 2.2.3), we can determine the subspace and thus apply the corresponding error correcting procedure. The important difference to classical codes is that quantum codes must preserve the coherence such as given in Eq. (2.1). A simple example is the three-qubit repetition code (see, e.g, [Nielsen and Chuang, 2000]), where $|0\rangle$ is encoded as $|000\rangle$ and $|1\rangle$ as $|111\rangle$. This code can correct single bit-flip errors. We have four orthogonal subspaces telling us if there was no error, an error on the first qubit and so on.

In [Jiang *et al.*, 2009] the idea of using quantum repeaters with quantum error-correcting codes appeared. To encode the sent quantum states has an advantage over the distillation protocols described above because they only require one-way classical communication. Classical communication can be a bottleneck in long-distance quantum key distribution, as it might limit the speed of the entanglement generation process (see, e.g., [Jiang *et al.*, 2009]). There is a connection between entanglement distillation and quantum error correction: it was shown in [Bennett *et al.*, 1996b] that one-way distillation protocols are equivalent to quantum error-correcting codes. The main principle of the quantum repeater using quantum

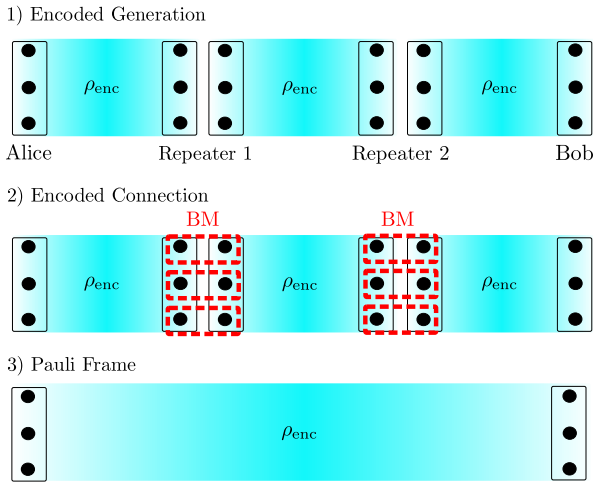


Figure 4.7: Setup of the encoded quantum repeater for the three-qubit repetition code, BM stands for Bell measurement. Figure taken from [Bratzik *et al.*, 2014], adapted from [Jiang *et al.*, 2009].

[8] An arbitrary error on a qubit can be completely described by the operators from the discrete set $\{\mathbb{1}, X, Y, Z\}$ with X, Y, Z being the Pauli matrices given in Eq. (2.6), see [Nielsen and Chuang, 2000].

error-correcting codes works as follows (see Fig. 4.7 for the three-qubit repetition code): In the first step encoded Bell pairs ρ_{enc} are distributed among the repeater stations R_i and R_{i+1}, where in the ideal case $\rho_{\text{enc}} = \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|$ is given by (for the three-qubit repetition code described above)

$$\left|\tilde{\phi}^+\right\rangle = \frac{1}{\sqrt{2}} |000\rangle_{R_i} |000\rangle_{R_{i+1}} + |111\rangle_{R_i} |111\rangle_{R_{i+1}} . \tag{4.19}$$

In the second step three Bell measurements (see Sec. 4.1.1) are performed in the repeater station leading to three measurement outcomes and thus leading to encoded entanglement swapping. The measurement outcomes identify the resulting encoded Bell state, i.e., the classical information in order to perform the correct rotation in the end (step 3), see Sec. 4.1.1. Error correction is performed in the sense that a majority vote between the measurement results is employed. No quantum operations are performed, as errors at the repeater stations do not affect the final state. In Sec. 5.2.3 we present the results of our publication [Bratzik *et al.*, 2014] where we calculate the secret key rates for the encoded quantum repeater.

5 Summary of the results

5.1 Finite secret key rates for coherent attacks

We have introduced in Sec. 3.2.1 possible attacks of an eavesdropper on the quantum states sent from Alice to Bob. These are individual, collective and coherent attacks. The latter is the most general attack. It was shown in [Kraus *et al.*, 2005; Renner *et al.*, 2005] that under the assumption of certain quantum key distribution protocols the asymptotic secret key rates (see Sec. 3.2.2) are equivalent for collective and coherent attacks. These protocols are permutationally invariant, i.e., the output of the protocol remains the same if we change the order of the input pairs. It holds for these protocols that the resulting state of Alice and Bob after the distribution of N qubit pairs (after sifting and parameter estimation n signals remain) is given by [Kraus *et al.*, 2005; Renner *et al.*, 2005]

$$\rho_{AB}^n = \mathcal{P}_n \left(\sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \sigma_1^{\otimes n_1} \otimes \sigma_2^{\otimes n_2} \otimes \sigma_3^{\otimes n_3} \otimes \sigma_4^{\otimes n_4} \right), \tag{5.1}$$

where $\mathcal{P}_n$ is a permutation map, σ_i are the projectors onto the four Bell states [Eq. (2.3)], $\mu_{\mathbf{n}}$ is the probability of one particular realization and $\Lambda^n := \{\mathbf{n} = (n_1, n_2, n_3, n_4) : \sum_{i=1}^4 n_i = n\}$ is the set of all possible realizations. In the context of finite-key analysis (see Sec. 3.2.3) the equivalence of collective and coherent attacks was not proven yet. In our publication [Mertz *et al.*, 2013] we provide a possible evidence of an inequivalence. The main result of our paper is bounding the min-entropy (see Sec. 2.3) for states subjected to coherent attacks with the min-entropy for product states which are the result of collective attacks:

$$H_{\min}^{\bar{\varepsilon}} \left(\rho_{XE}^n | E\right) \geq \inf_{\sigma_{AB}\in\Gamma_{\xi_{\mathrm{coh}}}} H_{\min}^{\bar{\varepsilon}/(2n)^2} \left(\sigma_{XE}^{\otimes n} \left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n} \right] | E \right) - 1. \tag{5.2}$$

The state ρ_{XE}^n describes Alice's (X) and Eve's (E) system after Alice's measurement and Eve's collective attack. This state is a classical-quantum state as presented in Sec. 2.3. The set $\Gamma_{\xi_{\mathrm{coh}}}$ contains all the states that comply with the statistics for parameter estimation with deviation parameter ξ_{coh} (see Sec. 3.2.3), $\bar{\varepsilon}$ is the smoothing parameter for the min-entropy [see Sec. 2.3, Eq. (2.27)], and $\sigma_{AB}[\boldsymbol{\lambda}] = \sum_{i=1}^4 \lambda_i \sigma_i$ are Bell-diagonal states with $\boldsymbol{\lambda} := (\lambda_1, \lambda_2, \lambda_3, \lambda_4) = \left(\frac{n_1}{n}, \frac{n_2}{n}, \frac{n_3}{n}, \frac{n_4}{n}\right)$. We use for this bound that permutation-invariant states are a convex combination of tensor products of Bell states [Kraus *et al.*, 2005; Renner *et al.*, 2005]. For evaluating Eq. (5.2), we use the bound of the min-entropy via the von Neumann entropy given in Eq. (2.28) in Sec. 2.3 and the results about the secret key rate for a finite number of signals given in Eq. (3.10) in Sec. 3.2.3.

Figure 5.1 shows the secret key rate for the six-state protocol in terms of the total number of signals N using the estimate given in Eq. (5.2), r_{coh}, compared to the secret key rate using collective attacks r_{coll} [Eq. (3.10)] for different values of the quantum bit error rate (QBER)[9]. Additionally, the secret key rates using the post-selection technique r_{post} [Christandl *et al.*, 2009] are depicted. We see that in the asymptotic limit the secret key rates converge to the asymptotic value, but for a small number of signals our estimate for coherent attacks (r_{coh}) shows an increase of the secret key rate of 51% (for QBER $= 0.01$, $N = 10^6$) and 45% (QBER $= 0.1$, $N = 10^8$) compared to r_{post}. It means for the same number of signals the secret key rate using our estimate is higher. As the approaches do not coincide in this region, it hints that collective and coherent attacks are not equivalent for a small number of signals ($N < 10^{10}$).

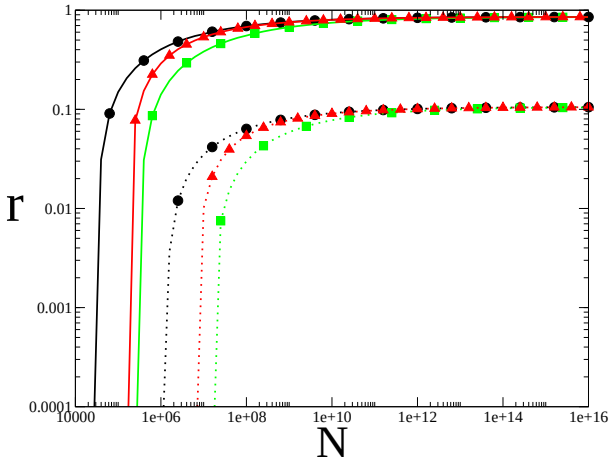


Figure 5.1: Comparison of the secret key rates r_{coll} [Eq. (3.10) using Eq. (2.28)] (black circles), r_{post} (green squares) and r_{coh} [Eq. (5.2) using Eq. (2.28)] (red triangles) versus the number N of initial signals for different quantum bit error rates (QBER) with security parameter $\varepsilon = 10^{-9}$ for the six-state protocol in logarithmic scale; QBER $= 0.01$ (straight lines) and QBER $= 0.1$ (dotted lines). Caption and figure taken from [Mertz *et al.*, 2013].

5.2 Asymptotic secret key rates using quantum repeaters

5.2.1 Analysis for different experimental scenarios

In our publication [Abruzzo *et al.*, 2013] we start our analysis by modeling the building blocks (see Sec. 4.2) of a repeater and its imperfections. The main purpose of the paper is to introduce a general analysis in such a way that it could be used for different experimental setups. We have already identified the main problems in Chapter 4, which can be summarized as the losses in the quantum channel, the error in the entanglement source (which was modeled as a depolarizing error with parameter F), the depolarizing error (parameter p_G) in the gates,

[9] The quantum bit error rate is the ratio of wrong bits to received bits [Gisin *et al.*, 2002], see also Eq. (3.7).

the detector efficiency η_{d} and the memory efficiency η_{m}. These errors also influence the processes of entanglement swapping and entanglement distillation.

In our work we characterize quantum key distribution using different quantum repeater schemes. The secret key rate using quantum repeaters is defined by the product of the secret fraction (see Sec. 3.2.2) and the repeater rate (see Sec. 4.1.4):

$$R_{\mathrm{QKD}} := R_{\mathrm{Rep}} r_{\infty}. \tag{5.3}$$

In [Abruzzo *et al.*, 2013], we develop the repeater rate for specific situations, such as probabilistic entanglement distillation and probabilistic entanglement swapping. Before, only the repeater rate for deterministic swapping (see Sec. 4.1.4) was known. Deterministic means that the probability of success is one. Usually, another factor that accounts for the sifting (see Sec. 3.1) appears in the formula for the secret key rate. But throughout the paper we assume a specific protocol, the so-called asymmetric protocol [Lo *et al.*, 2005], where the probability of choosing the measurement basis (see Sec. 3.1) is biased; thus the sifting factor is one.

In the following we will briefly describe the experimental quantum repeater schemes and the main results. As our analysis is quite extensive, we focus on the outstanding aspects of the different repeater schemes.

5.2.1.1 The original quantum repeater

We denote the scheme from [Briegel *et al.*, 1998] (see Chap. 4) by the *original quantum repeater scheme*. For simplicity, we assume that we distill only in the beginning (the restriction will be released in Sec. 5.2.2). In Table 5.1, we identify the minimal parameters for the initial fidelity F_0 and gate quality p_G to establish a nonzero secret key for different QKD-protocols (see Sec. 3.2.2). We find that increasing the number of distillation rounds, the input pairs for

N \ k	0		1		2		3	
	BB84	6S	BB84	6S	BB84	6S	BB84	6S
0	0.835	0.810	0.733	0.728	0.671	0.669	0.620	0.614
1	0.912	0.898	0.821	0.818	0.742	0.740	0.669	0.664
2	0.955	0.947	0.885	0.884	0.801	0.800	0.713	0.709
3	0.977	0.973	0.929	0.928	0.849	0.848	0.752	0.749
4	0.988	0.987	0.957	0.957	0.887	0.887	0.788	0.785
5	0.994	0.993	0.975	0.975	0.917	0.917	0.819	0.818
6	0.997	0.997	0.985	0.985	0.939	0.939	0.847	0.846
7	0.999	0.998	0.992	0.992	0.956	0.956	0.872	0.870

Table 5.1: Minimal initial fidelity F_0 (p_G is fixed to one) for extracting a secret key with maximal nesting level N and number of distillation rounds k for the BB84- and six-state protocols, from [Abruzzo *et al.*, 2013].

the repeater can have low fidelity. In Fig. 5.2, the number of distillation rounds that maximize the secret key rate in terms of the gate quality p_G and initial F_0 is depicted. Introducing more distillation rounds, increases the fidelity (see Sec. 4.1.2) and thus the secret fraction, but at the same time the repeater rate, which is a function of the success probability of distillation, decreases. For example for fairly good gates ($p_G \geq 0.97$) and fidelities ($F_0 \geq 0.97$), the optimal distillation strategies is to not distill. Thus, the effect of distillation is not dominant here. In regions for low fidelities ($F_0 \geq 0.7$) and low gate quality ($p_G \leq 0.98$), distillation is a necessary tool for having a nonzero secret key.

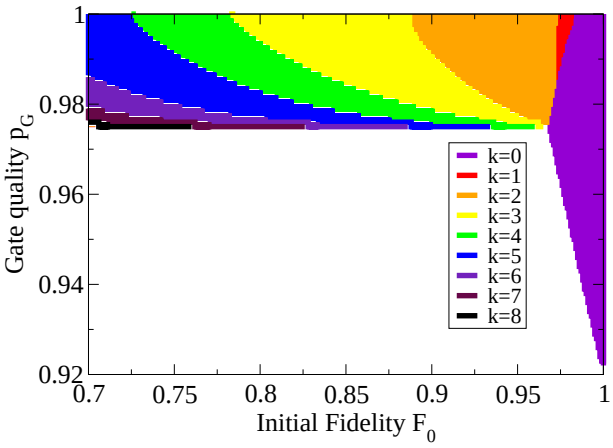


Figure 5.2: Original quantum repeater and the BB84-protocol: Number of distillation rounds k that maximizes the secret key rate as a function of gate quality p_G and initial fidelity F_0. In the white area, it is no longer possible to extract a secret key. (Parameters: $N = 2$, $L = 600$ km), figure and caption taken from [Abruzzo *et al.*, 2013].

5.2.1.2 The hybrid quantum repeater

In the hybrid quantum repeater (HQR) [van Loock *et al.*, 2006; Ladd *et al.*, 2006] the entanglement is transmitted via a coherent-laser pulse, which has previously interacted with a qubit in a cavity (for details we refer to our publication [Abruzzo *et al.*, 2013]). The main difference to the protocol given in Sec. 5.2.1.1 is that the entanglement swapping operations are not probabilistic and that the probability of successful entanglement generation P_0 depends on the initial fidelity F_0 of the state and the detector efficiency η_d (compared to $P_0 = P_t$ for the original quantum repeater protocol):

$$P_0 = 1 - (2F_0 - 1)^{\frac{P_t \eta_\mathrm{d}}{1 + P_t(1-2\eta_\mathrm{d})}}, \tag{5.4}$$

with P_t the transmission probability in a channel defined in Eq. (4.1). Different to the original quantum repeater, the produced state is of the form

$$\rho_0 := F_0 \left|\phi^+\right\rangle \left\langle\phi^+\right| + (1 - F_0) \left|\phi^-\right\rangle \left\langle\phi^-\right|, \tag{5.5}$$

which is also called a *binary* state. Due to the dependence of the generation probability P_0 [Eq. (5.4)] on the fidelity, interesting effects for the secret key rate can be observed (see Fig. 5.3): the secret key rate exhibits a nonmonotonic behavior in the fidelity. The reason is that the generation probability P_0 decreases with increasing fidelity, thus the repeater rate decreases, but at the same time the secret fraction increases. This implies that at some point a higher fidelity does not necessary lead to higher secret key rates. We examined also whether the optimal fidelity changes with the total distance, and we found that for distances $L > 100$ km, the optimal fidelities are almost constant.

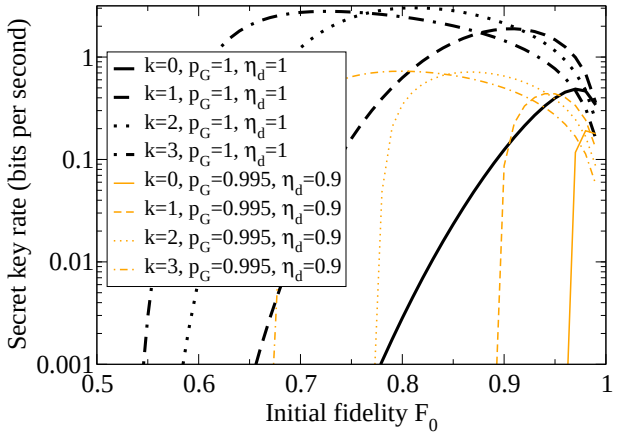


Figure 5.3: Hybrid quantum repeater with perfect quantum operations ($p_G = 1$) and perfect detectors ($\eta_\mathrm{d} = 1$) (black lines) compared to imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_\mathrm{d} = 0.9$) (orange lines): Secret key rate per second as a function of the initial fidelity for 2^3 segments ($N = 3$) and various rounds of distillation k. The distance between Alice and Bob is 600 km. Figure and caption taken from [Abruzzo *et al.*, 2013].

5.2.1.3 The atomic ensemble quantum repeater

Another experimental protocol uses atomic ensembles which is called the *DLCZ-protocol* [Duan *et al.*, 2001] named after Duan, Lukin, Cirac and Zoller. Entanglement between two remote parties is established by interfering and detecting Stokes photons emitted from two distant atomic ensembles at a beamsplitter (see, e.g, [Sangouard *et al.*, 2011]). The entanglement is thus created in the atomic excitation, as it is unknown which atomic ensemble emitted the photon.

The protocol [Minář *et al.*, 2012] investigated in our publication [Abruzzo *et al.*, 2013] is an improvement of the *DLCZ-protocol* in the sense that the states produced in the end do not contain any vacuum components. This protocol uses heralded qubit amplifiers in order to produce entanglement on demand, different to the experimental setup described in Sec. 5.2.1.2, which is probabilistic. Figure 5.4 shows the resulting secret key rates for the quantum repeater scheme with atomic ensembles optimized over the pump parameter p of the spontaneous parametric downconversion source and R the reflectivity of the beam splitter

(see our publication [Abruzzo *et al.*, 2013] for details). The figure shows that even with realistic parameters, the secret key rate is only one order of magnitude smaller compared to ideal parameters thus providing a high error tolerance.

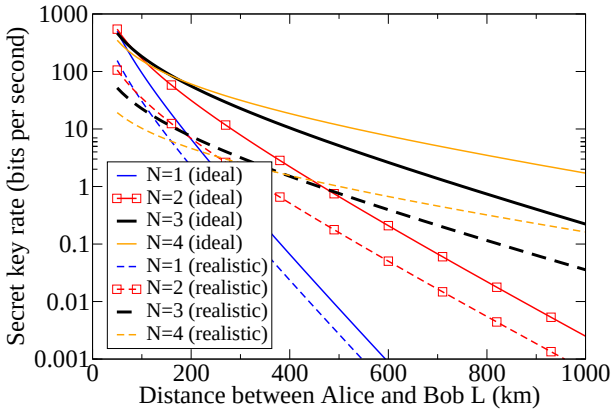


Figure 5.4: Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the distance between Alice and Bob. The secret key rate has been obtained by maximizing over p and R. Ideal setup (solid line) with parameters $\eta_{\mathrm{m}} = \eta_{\mathrm{d}} = q = 1, \gamma_{rep} = \infty$. More realistic setup (dashed line) with parameters $\eta_{\mathrm{m}} = 1$, $\eta_{\mathrm{d}} = 0.9$, $q = 0.96$, $\gamma_{rep} = 50$ MHz. The parameter q is the efficiency of the single-photon source and γ_{rep} is the repetition rate. Figure and caption taken from [Abruzzo *et al.*, 2013].

5.2.2 Improving the distillation strategies

So far, we focused in our analysis on distillation only in the beginning and only on one specific distillation protocol. In our publication [Bratzik *et al.*, 2013], we performed a generalized analysis for the original quantum repeater investigating the effects on the secret key rate regarding the distillation protocols and *distillation strategies* (see Secs. 4.1.2 and 4.3). By distillation strategies, we mean different numbers of distillation rounds in each nesting level, described by the distillation vector

$$\vec{k} = (k_0, ..., k_N)\,, \tag{5.6}$$

where k_i gives the number of distillation rounds in the i-th nesting level (see also Fig. 4.1).

In order to start with the analysis, we developed the repeater rate (see Sec. 4.1.4) for the *Deutsch et al.* and *Dür et al. protocol* (see Sec. 4.3) considering the classical communication time for entanglement distillation and entanglement swapping. In the following, the figure of merit will be the *secret key rate per memory per second* defined as:

$$K^i = R^i_{\mathrm{Rep}}(\vec{k}, N, L)\frac{r^i_\infty(F_0, p_G, \vec{k}, N)}{M^i(\vec{k}, N)}, \tag{5.7}$$

where the parameter i gives the different distillation protocols (*Deutsch et al.* or *Dür et al.*),

the memories M^i are presented in Sec. 4.3, the repeater rate R_{Rep} is explained in Sec. 4.1.4, and the asymptotic secret fraction is described in Sec. 3.2.2. For a fixed distance $L = 600$ km, we optimize the secret key rate per memory per second [see Fig. 5.5(a)] and give the resulting parameters for the optimization [Figs. 5.5(b)-(f)]. For simplicity, we focus on two distillation strategies:

- strategy α, where $\vec{k} = (k, ..., k)$, i.e., the same number of distillation rounds in each nesting level,
- strategy β, where $\vec{k} = (k, 0, ..., 0)$, i.e., distillation is only performed in the beginning.

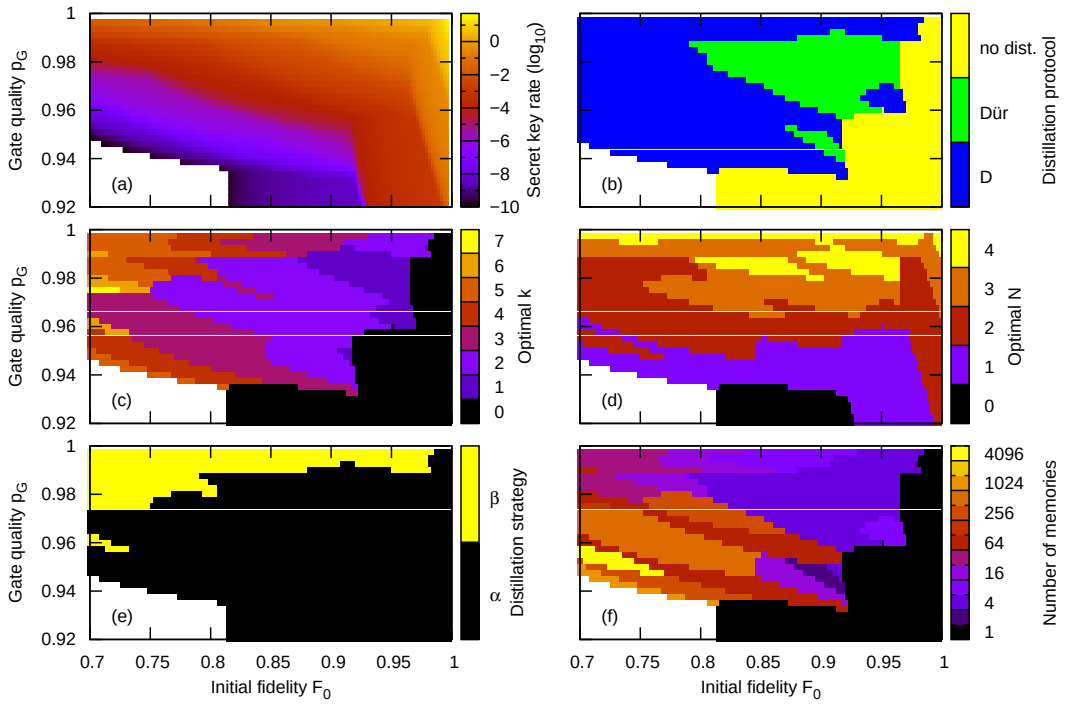


Figure 5.5: (a) Optimal secret key rate per memory per second (bits per second) [Eq. (5.7)] for the distance $L = 600$ km. The smallest secret key rate still depicted is chosen to be 10^{-10} secret bits per second per memory. In the white region an extraction of a non-zero secret key rate is not possible. The parameters for the optimal secret key rate per memory per second are: (b) Distillation protocols: *Deutsch et al.* protocol (blue), *Dür et al.* protocol (green), and no distillation (yellow). (c) Number of rounds of distillation k (for the optimal distillation strategy). (d) Number of nesting levels N. (e) Distillation strategies: Strategy α (nested distillation) and strategy β (distillation only before the first entanglement swapping). (f) Number of used memories per repeater node. Figure and caption taken from [Bratzik *et al.*, 2013].

We find that regarding the distillation protocols [Fig. 5.5(b)], we can divide the optimal protocols roughly in three regions: First, for good fidelities ($F_0 > 0.97$) and all gate parameters it is always optimal to not distill. Second, for gate qualities $0.94 \leq p_G \leq 0.99$ and fidelities

$F_0 \geq 0.8$, the *Dür et al.* protocol performs best and third, the *Deutsch et al.* protocol for the remaining regions. It is not obvious, why the *Dür et al.* protocol is optimal in the aforementioned region. There are many competing terms in the secret key rate [Eq. 5.7] such as the repeater rate, the number of memories and the resulting state. As mentioned above, during our analysis we only restricted to either distillation strategy α or β. In Fig. 5.5(e), we show that for relatively good gate qualities $p_G \geq 0.98$ it is optimal to distill only in the beginning.

For specific values of the initial fidelity F_0 and the gate quality p_G, we optimized the distillation strategy without any restriction and we have seen that the secret key rate can be improved by almost one order of magnitude than to use strategy α or β. Furthermore, allowing more general distillation strategies lead to different results regarding the optimal distillation protocols, see Table 5.2. For specific examples of F_0 and p_G, we have seen that changing the distillation strategy leads to an improvement of the secret key rate by a factor of 3.

	Dür et al. protocol		*Deutsch et al.* protocol	
N	K	$\vec{k}$	K	$\vec{k}$
0	$3.92 \cdot 10^{-9}$	(0)	$3.92 \cdot 10^{-9}$	(0)
1	$2.11 \cdot 10^{-5}$	$(0,2)$	$2.63 \cdot 10^{-5}$	$(0,1)$
2	$1.09 \cdot 10^{-4}$	$(2,3,2)$	$3.03 \cdot 10^{-4}$	$(0,3,1)$
3	$2.66 \cdot 10^{-6}$	$(3,4,5,5)$	$1.51 \cdot 10^{-4}$	$(0,3,3,1)$
4	0	0	$1.37 \cdot 10^{-5}$	$(0,3,3,3,1)$

Table 5.2: Optimal secret key rate per memory per second [Eq. (5.7)] and corresponding distillation vector $\vec{k}$ [Eq. (5.6)] for the different distillation protocols, $F_0 = 0.9$, and $p_G = 0.96$. From [Bratzik *et al.*, 2013].

Instead of varying the distillation strategies, i.e., the distillation vector, one can also think of parallel repeater setups. For parallel setups, the secret key rate resulting from each repeater is added. By fixing the total number of memories used per half node of a repeater station, we analyzed the optimal configuration and found that using parallel setups allows to improve the secret key rate by a factor of 3. Furthermore, for our choice of parameters, parallel setups may also be optimal for a different distillation protocol.

In our paper, we investigated the impact of the classical communication time on the secret key rate. We compared the secret key rate using the repeater rate that we developed to the repeater rate without any classical communication time and have found, different to the statement in [Jiang *et al.*, 2009], that the communication time has a small impact on the secret key rate for a given distance and protocol considered here. We analyzed also the influence of the form of input states onto the secret key rate. Usually we assumed the input states to be depolarized states, see Eq. (2.12). The hybrid quantum repeater [van Loock *et al.*, 2006; Ladd *et al.*, 2006] produces binary states [see Eq. (5.5)]. We have found that here we can have a nonzero secret key for a larger range of parameters, i.e., $0.7 \leq F_0 \leq 1$ and $0.92 \leq p_G \leq 1$.

5.2.3 Encoded quantum repeater

In Sec. 4.4 we described the quantum repeater using quantum error-correcting codes [Jiang *et al.*, 2009] (in the following called *encoded quantum repeater*). The idea of our publication [Bratzik *et al.*, 2014] is to compare the secret key rates for the quantum repeater using distillation (the *original quantum repeater*, see Sec. 5.2.1.1) to the encoded quantum repeater. The motivation behind it is that the encoded quantum repeater does not require classical communication time except for entanglement generation and the announcement of the results for entanglement swapping in the end. In the case of the original quantum repeater, depending on the rounds of distillation, much time is lost by communicating the measurement results needed for entanglement distillation. There exist concepts of running the repeater scheme blindly (i.e., without any communication, see, e.g., [Hartmann *et al.*, 2007]) but at the expense of exponentially decreasing the success probability.

For starting the analysis, we first developed an error model for the encoded quantum repeater. Different to the original paper [Jiang *et al.*, 2009], our idea was to initialize the states without fault-tolerance in order to save resources. Additionally, our analysis allows the employment of initial Bell states (needed for the generation of the encoded Bell pair, see Eq. (4.19) in Sec. 4.4) that have fidelity smaller than 1. Our model is as follows: We use the depolarizing gate error model given in Eq. (2.14). If we have n quantum gates, we only consider terms with gate error $\beta = 1 - p_G$, i.e., the linear terms and set all remaining states to be the identity:

$$\Lambda_{\text{conc}}(\rho) \;:=\; (1-\beta)^n \left(\prod_{a=1}^{n} U^a\right) \rho \left(\prod_{a=1}^{n} U^a\right)^{\dagger} + n\beta(1-\beta)^{n-1}\tilde{\rho} + p\frac{\mathbb{1}_d}{d}, \tag{5.8}$$

where $d = \dim(\rho)$ and $p = 1 - (1-\beta)^n - n\beta(1-\beta)^{n-1}$. The state $\tilde{\rho}$ is given by the map $\Lambda_{1-\text{faulty}}(\rho)$

$$\tilde{\rho} =: \Lambda_{1-\text{faulty}}(\rho) = \frac{1}{n}\sum_{a=1}^{n} \left(\prod_{b=a+1}^{n} U^b\right) f\left[(i_a, j_a), \rho, \prod_{c=1}^{a-1} U^c\right] \left(\prod_{b=a+1}^{n} U^b\right)^{\dagger}, \tag{5.9}$$

with $f[(i,j),\rho,A] := \text{tr}_{i,j}\left(A\rho A^{\dagger}\right) \otimes \frac{\mathbb{1}_{i,j}}{4}$. The operator U^a defines the two-qubit operation U on the qubits (i_a, j_a) and the vector $\vec{U} := \{U^1, ..., U^n\}$ gives the sequence of the unitary maps. Expanding the probability p for small β gives: $p \approx \frac{n(n-1)}{2}\beta^2 - n\binom{n-1}{2}\beta^3$. Thus, p is on the order of β^2 for appropriate n. The reason for introducing this map lies in the complexity of the computations as already for the simple three-qubit repetition code (see Sec. 4.4) we perform the computations in a 2^{12}-dimensional Hilbert space. Additional to this error model, we also investigated the errors that can be corrected during the encoded connection step and we have found a remarkable improvement if all correctable errors are used in comparison to [Jiang *et al.*, 2009]. Considering these additional errors in our analysis increases the error-tolerance of the secret key rate [Bratzik *et al.*, 2014]. Additionally, we explicitly accounted for

the effect of the decoding scheme. Our advances also involved the derivation of the repeater rate for the encoded quantum repeater scheme using the methods described in Sec. 4.1.4.

Table 5.3 shows the minimal parameters for establishing a nonzero secret key for the encoded quantum repeater. If we compare this results with Table 5.1 in the preceding section, we see that the encoded quantum repeater does not have any advantage here.

r	N	$p_{G,\min}$	$F_{0,\min}$
1	1	0.984	0.943
3	2	0.992	0.972
7	3	0.994	0.981
15	4	0.996	0.986
31	5	0.997	0.989
63	6	0.997	0.991
127	7	0.998	0.992

Table 5.3: Minimal p_G (F_0 is fixed to one) and minimal fidelity F_0 (p_G is fixed to one) for extracting a secret key for the six-state protocol with $r = 2^N - 1$ repeaters with N being the nesting level for entanglement swapping. From [Bratzik *et al.*, 2014].

Calculating the secret key rates, we find that it is always optimal to use original quantum repeaters with the *Deutsch et al.* distillation protocol (see Sec. 4.3) for the whole range of error parameters. The reason is that in the region where the encoded quantum repeater produces a nonzero secret key rate (see Table 5.3), it is not optimal to perform any distillation (see Fig. 5.5). When no distillation is performed, fewer classical communication is exchanged, and less resources are needed, whereas in the encoded quantum repeater we constantly need three Bell pairs.

During the preparation of the manuscript we became aware of a paper which treated a quantum repeater scheme with one-way classical communication using teleportation-based error correction [Muralidharan *et al.*, 2013]. There, as a figure of merit the cost function was defined as the minimal number of total qubits per secret bit:

$$C = \min_{i,N} \frac{2^{N+1}}{K^i}, \tag{5.10}$$

where K is the secret key rate as defined in Eq. (5.7), N is the nesting level and i are the different repeater protocols, i.e, either the encoded or the original quantum repeater. Figure 5.6 shows the cost coefficient which is the cost function [Eq. (5.10)] divided by the total distance. Compared to the rather complicated protocol given in [Muralidharan *et al.*, 2013], the encoded and the original quantum repeater are one order of magnitude better up to distances of 5000 km. Additionally, using the rather simple three-qubit repetition code, the optimal distance of the repeater stations is between $30 - 100$ km compared to $1 - 2$ km given in [Muralidharan *et al.*, 2013]. This means that the total number of required repeater stations is roughly $1 - 2$ orders of magnitude smaller for the original quantum repeater scheme.

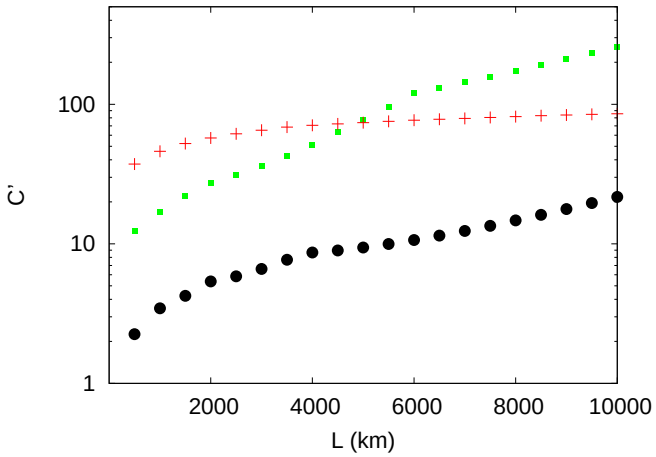


Figure 5.6: The cost coefficient ($C' = C/L$) [Eq. (5.10)] for the encoded (green squares), the generic quantum repeater (black circles) and the quantum repeater protocol presented in [Muralidharan *et al.*, 2013] (red crosses, with the effective qubit error $\varepsilon = 10^{-4}$, for an explanation see [Muralidharan *et al.*, 2013]) as a function of the total distance L (Parameters: $F_0 = 0.99995$, $p_G = 0.9999$, and $T_0 = 1$ as in [Muralidharan *et al.*, 2013]). Figure and caption from [Bratzik *et al.*, 2014].

6 Outlook

We investigated asymptotic secret key rates in the context of quantum repeaters. For our analysis, some assumptions regarding the components of the repeater have been made. We considered, e.g., the quantum memories to be perfect (except for the quantum repeater with atomic ensembles, we assumed a memory efficiency). Our findings could be extended using the results given in [Hartmann *et al.*, 2007] where the role of memory errors in quantum repeaters was analyzed. Furthermore, advances had been made regarding the repeater rate and imperfect memories [Praxmeyer, 2013], which could also be implemented in our analysis. The repeater rate and thus the secret key rate can be improved by strategies like multiplexing [Abruzzo *et al.*, 2014].

So far, we only treated quantum repeater for secret keys in the asymptotic limit. An analysis of the secret key rate for quantum repeaters in the finite-key formalism remains open. In this context new advances for calculating secret keys in the finite regime appeared by employing uncertainty relations [Tomamichel and Renner, 2011; Tomamichel *et al.*, 2012]. This approach gives tighter bounds on the finite secret key rate. Recently, new discoveries regarding the information leakage term for error correction appeared [Tomamichel *et al.*, 2014]. It was found that the existing results were too optimistic and an approach using a two-parameter approximation was given. This advance can be easily adapted to our finite-key analysis. Still, the problem of the equivalence of collective and coherent eavesdropping attacks for keys in the regime of a finite number of signals remains open.

7 List of main results

- We developed a bound for coherent eavesdropping attacks in the context of finite-key analysis. This bound is better for a small number of signals compared to the existing techniques and gives evidence of an inequivalence of collective and coherent attacks in the finite regime.

- We quantified and modeled the building blocks of a quantum repeater in order to perform a general analysis for different experimental repeater schemes. These schemes include the original quantum repeater, the hybrid quantum repeater, a quantum repeater scheme based on atomic ensembles and the encoded quantum repeater. We performed a quantitative analysis of the optimal secret key rates for each repeater scheme under different realistic parameters and identified the particularities of each scheme. Regarding the original quantum repeater, we determined the minimally required parameters (such as the gate quality and the initial fidelity) for obtaining a nonzero secret key. The requirements on the initial fidelity are not so strong, if distillation is allowed. The quantum gates however, should not exceed errors of 1%. For the hybrid quantum repeater, we found that the secret key rate is not a monotonic function in the initial fidelity, thus there exists for each nesting level and number of distillation rounds a fidelity that optimizes the secret key rate. This repeater scheme only tolerates gate errors in the order of 0.1%. The analysis of the repeater scheme with atomic ensembles showed that it is robust against most imperfections. Additionally, we derived the repeater rate for probabilistic entanglement swapping and entanglement distillation.

- For given gate errors and initial fidelities, we investigated the repeater configuration (i.e., the distillation protocol, the distillation strategy, the number of distillation rounds, number of nesting levels, and the number of memories) to obtain the optimal secret key rate. Regarding the distillation protocols we optimized either between the *Deutsch et al.* protocol and the *Dür et al.* protocol. The former works in a recursive way and is efficient in achieving the fidelity in few steps; the latter pumps the entanglement but is more noise-tolerant than the former protocol. We found that for the parameters $p_G \leq 0.99$ and $F_0 \geq 0.8$ the *Dür et al.* protocol performs best; considering lower fidelities the *Deutsch et al.* protocol is better. For extremely good fidelities $F_0 \geq 0.97$ employing no distillation is favorable. Additionally, we derived the repeater rate for different distillation protocols including the classical communication time needed for entanglement swapping and entanglement distillation and showed the communication time has a small impact on the secret key rate for the parameters considered here.

- We derived the repeater rate for an encoded quantum repeater and investigated un-

der which circumstances it can be better than other repeater schemes like the original quantum repeater using distillation. The encoded quantum repeater does not need as much communication time as the original repeater scheme, but requires more resources. For our analysis, we introduced a concatenated error model which allows the analysis of Bell pairs with a fidelity smaller than one. We identified the errors that can be corrected during entanglement connection for the three-qubit repetition code and additionally analyzed a decoding procedure. For the encoded quantum repeater using the three-qubit repetition code, no advantage over the original repeater scheme was found. Furthermore, we investigated the cost function which is the ratio of required resources over the secret key rate and we have seen that our approaches lead to a significant improvement of roughly $1-2$ orders of magnitude compared to a recent repeater proposal using one-way classical communication working on a scheme called teleportation-based error correction.

Bibliography

Abruzzo, S., Bratzik, S., Bernardes, N.K., Kampermann, H., van Loock, P., and Bruß, D. "Quantum repeaters and quantum key distribution: Analysis of secret-key rates." *Physical Review A* **87**, 052315, 2013.

Abruzzo, S., Kampermann, H., and Bruß, D. "Finite-range multiplexing enhances quantum key distribution via quantum repeaters." *Physical Review A* **89**, 012303, 2014.

Alleaume, R., Bouda, J., Branciard, C., Debuisschert, T., *et al.* "SECOQC White Paper on Quantum Key Distribution and Cryptography." 2007. `arXiv:quant-ph/0701168v1`.

Amirloo, J., Razavi, M., and Majedi, A.H. "Quantum key distribution over probabilistic quantum repeaters." *Physical Review A* **82**, 032304, 2010.

Bechmann-Pasquinucci, H. and Gisin, N. "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." *Physical Review A* **59**, 4238, 1999.

Bennett, C.H. and Brassard, G. "Quantum cryptography: Public key distribution and coin tossing." In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, page 175. IEEE, New York, 1984.

Bennett, C.H., Brassard, G., and Mermin, N. "Quantum cryptography without Bell's theorem." *Physical Review Letters* **68**, 557, 1992.

Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., and Wootters, W.K. "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels." *Physical Review Letters* **76**, 722, 1996a.

Bennett, C.H., DiVincenzo, D., Smolin, J.A., and Wootters, W.K. "Mixed-state entanglement and quantum error correction." *Physical Review A* **54**, 3824, 1996b.

Bernardes, N.K., Praxmeyer, L., and van Loock, P. "Rate analysis for a hybrid quantum repeater." *Physical Review A* **83**, 012323, 2011.

Bratzik, S., Abruzzo, S., Kampermann, H., and Bruß, D. "Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate." *Physical Review A* **87**, 062335, 2013.

Bratzik, S., Kampermann, H., and Bruß, D. "Secret key rates for an encoded quantum repeater." *to be published in Physical Review A,* 2014. `arXiv:1401.6859v1`.

Briegel, H.J., Dür, W., Cirac, J.I., and Zoller, P. "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication." *Physical Review Letters* **81**, 5932, 1998.

Bruß, D. "Optimal Eavesdropping in Quantum Cryptography with Six States." *Physical Review Letters* **81**, 3018, 1998.

Christandl, M., König, R., and Renner, R. "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography." *Physical Review Letters* **102**, 020504, 2009.

Clauser, J., Horne, M., Shimony, A., and Holt, R. "Proposed Experiment to Test Local Hidden-Variable Theories." *Physical Review Letters* **23**, 880, 1969.

Collins, D., Gisin, N., and De Riedmatten, H. "Quantum relays for long distance quantum cryptography." *Journal of Modern Optics* **52**, 735, 2005.

Cover, T.M. and Thomas, J.A. *Elements of Information Theory.* Wiley-Interscience, Hoboken, New Jersey, second edition, 2006.

Csiszár, I. and Körner, J. "Broadcast channels with confidential messages." *IEEE Transactions on Information Theory* **24**, 339, 1978.

Curty, M., Lewenstein, M., and Lütkenhaus, N. "Entanglement as a Precondition for Secure Quantum Key Distribution." *Physical Review Letters* **92**, 217903, 2004.

Demtröder, W. *Experimentalphysik 3. Atome, Moleküle und Festkörper.* Springer Berlin Heidelberg New York, third edition, 2005.

Deutsch, D. "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer." *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **400**, 97, 1985.

Deutsch, D., Ekert, A.K., Jozsa, R., Macchiavello, C., Popescu, S., and Sanpera, A. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels." *Physical Review Letters* **77**, 2818, 1996.

Devetak, I. and Winter, A. "Distillation of secret key and entanglement from quantum states." *Proc. R. Soc. A* **461**, 207, 2005.

DiVincenzo, D. "Topics in Quantum Computers." 1996. `arXiv:cond-mat/9612126v2`.

Duan, L.M., Lukin, M.D., Cirac, J.I., and Zoller, P. "Long-distance quantum communication with atomic ensembles and linear optics." *Nature* **414**, 413, 2001.

Dür, W., Briegel, H.J., Cirac, J.I., and Zoller, P. "Quantum repeaters based on entanglement purification." *Physical Review A* **59**, 169, 1999.

Ekert, A.K. "Quantum cryptography based on Bell's theorem." *Physical Review Letters* **67**, 661, 1991.

Elkouss, D., Martinez-Mateo, J., and Martin, V. "Information Reconciliation for Quantum Key Distribution." *Quantum Info. Comput.* **11**, 226, 2011.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. "Quantum cryptography." *Reviews of Modern Physics* **74**, 145, 2002.

Greenberger, D.M., Horne, M., Shimony, A., and Zeilinger, A. "Bell's theorem without inequalities." *American Journal of Physics* **58**, 1131, 1990.

Hartmann, L., Kraus, B., Briegel, H.J., and Dür, W. "Role of memory errors in quantum repeaters." *Physical Review A* **75**, 032310, 2007.

Hoffstein, J., Pipher, J.C., and Silverman, J.H. *An Introduction to Mathematical Cryptography.* Undergraduate Texts in Mathematics. Springer, New York, 2008.

Holevo, A. "Statistical problems in quantum physics." In G. Maruyama and Y.V. Prokhorov, editors, *Procedings of the Second Japan-USSR Symposium on Probability Theory*, volume 330 of *Lecture Notes in Mathematics*, page 104. Springer Berlin Heidelberg, 1973.

Jiang, L., Taylor, J.M., Nemoto, K., Munro, W.J., Van Meter, R., and Lukin, M.D. "Quantum repeater with encoding." *Physical Review A* **79**, 032325, 2009.

Koashi, M. and Winter, A. "Monogamy of quantum entanglement and other correlations." *Physical Review A* **69**, 022309, 2004.

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

König, R., Renner, R., and Schaffner, C. "The Operational Meaning of Min- and Max-Entropy." *IEEE Transactions on Information Theory* **55**, 4337, 2009.

Kraus, B., Gisin, N., and Renner, R. "Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication." *Physical Review Letters* **95**, 080501, 2005.

Kraus, K. *States, Effects, and Operations. Fundamental Notions of Quantum Theory*, volume 190 of *Lecture Notes in Physics.* Springer-Verlag, Berlin, 1983.

Ladd, T.D., Loock, P.V., Nemoto, K., Munro, W.J., and Yamamoto, Y. "Hybrid quantum repeater based on dispersive CQED interactions between matter qubits and bright coherent light." *New Journal of Physics* **8**, 184, 2006.

Lee, K.G., Chen, X.W., Eghlidi, H., Kukura, P., Lettow, R., Renn, A., Sandoghdar, V., and Götzinger, S. "A planar dielectric antenna for directional single-photon emission and near-unity collection efficiency." *Nature Photonics* **5**, 166, 2011.

Lo, H.K., Chau, H.F., and Ardehali, M. "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security." *Journal of Cryptology* **18**, 133, 2005.

Maurer, U. "Information-Theoretic Cryptography." In *Advances in Cryptology - CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, page 47. Springer-Verlag, Berlin, 1999.

Mertz, M., Kampermann, H., Bratzik, S., and Bruß, D. "Secret key rates for coherent attacks." *Physical Review A* **87**, 012315, 2013.

Minář, J., de Riedmatten, H., and Sangouard, N. "Quantum repeaters based on heralded qubit amplifiers." *Physical Review A* **85**, 032313, 2012.

Muralidharan, S., Kim, J., Lütkenhaus, N., Lukin, M.D., and Jiang, L. "Ultrafast and Fault-Tolerant Quantum Communication across Long Distances." 2013. `arXiv:1310.5291v1`.

Nielsen, M. and Chuang, I. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

Praxmeyer, L. "Reposition time in probabilistic imperfect memories." 2013. `arXiv:1309.3407v1`.

Razavi, M., Amirloo, J., and Majedi, A.H. "Quantum key distribution over atomic-ensemble quantum repeaters." In *Optical Fiber Communication (OFC), collocated National Fiber Optic Engineers Conference, 2010 Conference on (OFC/NFOEC)*, pages 1–3. IEEE, New York, 2010.

Renner, R. "Security of quantum key distribution." *International Journal of Quantum Information* **6**, 1, 2008.

Renner, R., Gisin, N., and Kraus, B. "Information-theoretic security proof for quantum-key-distribution protocols." *Physical Review A* **72**, 12332, 2005.

Renner, R. and König, R. "Universally composable privacy amplification against quantum adversaries." *Theory of Cryptography* **3378**, 407, 2005.

Sangouard, N., Simon, C., de Riedmatten, H., and Gisin, N. "Quantum repeaters based on atomic ensembles and linear optics." *Review of Modern Physics* **83**, 33, 2011.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., and Peev, M. "The security of practical quantum key distribution." *Reviews of Modern Physics* **81**, 1301, 2009.

Scarani, V. and Renner, R. "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing." *Physical review letters* **100**, 200501, 2008.

Scherer, A., Sanders, B.C., and Tittel, W. "Long-distance practical quantum key distribution by entanglement swapping." *Optics Express* **19**, 3004, 2011.

Shannon, C.E. "A Mathematical Theory of Communication." *Bell System Technical Journal* **27**, 379, 1948a.

Shannon, C.E. "A Mathematical Theory of Communication." *Bell System Technical Journal* **27**, 623, 1948b.

Shannon, C.E. "Communication theory of secrecy systems." *Bell System Technical Journal* **28**, 656, 1949.

Shor, P. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Comput. Soc., Los Alamitos, CA, 1994.

Simon, C., Afzelius, M., Appel, J., Boyer de la Giroday, a., *et al.* "Quantum memories." *The European Physical Journal D* **58**, 1, 2010.

Singh, S. *The code book: The secret history of codes and code-breaking.* Fourth Estate, London, 1999.

Stucki, D., Walenta, N., Vannel, F., Thew, R.T., *et al.* "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres." *New Journal of Physics* **11**, 075003, 2009.

Tomamichel, M., Colbeck, R., and Renner, R. "A Fully Quantum Asymptotic Equipartition Property." *IEEE Transactions on Information Theory* **55**, 5840, 2009.

Tomamichel, M., Lim, C.C.W., Gisin, N., and Renner, R. "Tight Finite-Key Analysis for Quantum Cryptography." *Nature Communication* **3**, 634, 2012.

Tomamichel, M., Martinez-Mateo, J., Pacher, C., and Elkouss, D. "Fundamental Finite Key Limits for Information Reconciliation in Quantum Key Distribution." 2014. `arXiv:1401.5194v1`.

Tomamichel, M. and Renner, R. "Uncertainty Relation for Smooth Entropies." *Physical Review Letters* **106**, 1, 2011.

van Loock, P., Ladd, T.D., Sanaka, K., Yamaguchi, F., Nemoto, K., Munro, W.J., and Yamamoto, Y. "Hybrid Quantum Repeater Using Bright Coherent Light." *Physical Review Letters* **96**, 240501, 2006.

Vernam, G.S. "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications." *Transactions of the American Institute of Electrical Engineers* **XLV**, 295, 1926.

von Neumann, J. "Mathematische Begründung der Quantenmechanik." *Nachrichten von der Gesellschaft der Wissenschaft zu Göttingen, Mathematisch-Physikalische Klasse* **1927**, 1, 1927.

Waks, E., Zeevi, A., and Yamamoto, Y. "Security of quantum key distribution with entangled photons against individual attacks." *Physical Review A* **65**, 052310, 2002.

Wiesner, S. "Conjugate coding." *ACM SIGACT News* **15**, 78, 1983.

Zeilinger, A. "Vortrag an der Uni Wien." 2005. `www.dieuniversitaet-online.at/personalia/beitrag/news/60-geburtstag-von-anton-zeilinger/301/neste/3.html`, *accessed on January 29th, 2014*.

Żukowski, M., Zeilinger, A., Horne, M.A., and Ekert, A.K. ""Event-ready-detectors" Bell experiment via entanglement swapping." *Physical Review Letters* **71**, 4287, 1993.

Publications

Secret key rates for an encoded quantum repeater

Sylvia Bratzik,* Hermann Kampermann, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany.
(Dated: March 17, 2014)

We investigate secret key rates for the quantum repeater using encoding [L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009)] and compare them to the standard repeater scheme by Briegel, Dür, Cirac, and Zoller. The former scheme has the advantage of a minimal consumption of classical communication. We analyze the trade-off in the secret key rate between the communication time and the required resources. For this purpose, we introduce an error model for the repeater using encoding which allows for input Bell states with a fidelity smaller than one, in contrast to the model given in [L. Jiang *et al.*, Phys. Rev. A **79**, 032325 (2009)]. We show that one can correct additional errors in the encoded connection procedure of this repeater and develop a suitable decoding algorithm. Furthermore, we derive the rate of producing entangled pairs for the quantum repeater using encoding and give the minimal parameter values (gate quality and initial fidelity) for establishing a nonzero secret key. We find that the generic quantum repeater is optimal regarding the secret key rate per memory per second and show that the encoded quantum repeater using the simple three-qubit repetition code can even have an advantage with respect to the resources compared to other recent quantum repeater schemes with encoding.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.67.Bg

I. INTRODUCTION AND MOTIVATION

Quantum repeaters [1, 2] are a key tool for long-distance quantum communication with photons due to the attenuation in the optical fiber (see, e.g., discussion in [3]). They permit to establish entangled Bell pairs over distances of several hundreds of kilometers. A quantum repeater setup consists of segments of small distances, where entangled Bell pairs are created and then entanglement swapping [4] with the neighboring pairs is performed. In order to overcome the decrease in the fidelity due to swapping, entanglement distillation [5, 6] can be performed. There are several suggestions for experimental realizations of quantum repeaters [7, 8]. For a recent review on quantum repeaters, see [9].

Recently, we investigated the optimal quantum repeater setups with respect to the secret key rate [10, 11]. The limiting factor of these quantum repeater schemes, especially regarding the repeater rate, can be the classical communication time to acknowledge the success of entanglement distillation [12]. To overcome this bottleneck, the quantum repeater using quantum error-correcting codes [12, 13] was developed. In these protocols, classical communication is only needed between the neighboring repeater stations. The classical communication time becomes especially important when the memories are not perfect (see, e.g., [14]), as the stored states degrade with time.

In this paper we investigate the difference in the secret key rates between the quantum repeater using distillation (*generic quantum repeater*) and the quantum repeater using quantum error-correcting codes (*encoded quantum repeater*) by employing the analysis developed in [11] for the generic quantum repeater. As a representative for the encoded quantum repeater we choose [12]. We analyze the trade-off between the communication time and the needed resources. For this purpose, we modify the analysis given in [12] by using a concatenated error model for which we obtain a bound for the fidelity. Our model does not need a fault-tolerant preparation of the initial states, as it handles input pairs which are depolarized states with fidelity $F_0 < 1$. This approach saves resources, compared to [12], where multi-qubit errors are either suppressed or avoided via distillation. Furthermore, we show how to correct additional errors in the encoded connection procedure - this correction leads to higher secret key rates - and we develop a decoding algorithm suitable for quantum key distribution. We derive the rate for generating entangled pairs with the encoded quantum repeater and use it to calculate secret key rates.

The paper is organized as follows: in Sec. II we first briefly review the repeater scheme from Ref. [12]. Furthermore, the error model and its effect on the quantum states is introduced. We show which errors can be corrected during the encoded connection step and develop an appropriate decoding procedure. We then derive the repeater rate for the encoded quantum repeater scheme, i.e., the average number of entangled Bell pairs per second. In Sec. III, we review the generic quantum repeater, which uses distillation instead of quantum error-correcting codes. Then we provide the parameter thresholds for the encoded quantum repeater for obtaining a nonzero secret key rate. We continue to calculate the optimal secret key rate of these quantum repeater protocols and point out where our analysis differs from the original proposal of the encoded quantum repeater scheme [12]. We then present a short analysis of the cost function which was introduced recently in [15]. We conclude in Sec. IV.

II. ENCODED QUANTUM REPEATER SCHEME AND SECRET KEY RATES

In this section we introduce for the quantum repeater using encoding [12] (in the following called *encoded quantum re-*

* bratzik@thphy.uni-duesseldorf.de

peater) a generic error model, show its effect in the different steps of this quantum repeater model and derive the repeater rate, which is needed to calculate the secret key rate. This error model has the advantage of handling states with initial fidelity $F_0 < 1$ and thus saving resources as no fault-tolerant distillation of the states needs to be performed. Furthermore, we identify additional correctable errors during entanglement connection and show that considering these additional errors leads to an improvement of the secret key rate. Also, we develop a decoding circuit in order to quantify its effect on the states used for quantum key distribution.

A. Principles of the encoded QR

The principle of the encoded quantum repeater is depicted in Fig. 1: the first step is to distribute Bell pairs between the neighboring repeater stations, it follows the encoding operations [step 1) in Fig. 1] and an entanglement swapping scheme [step 2)] which allows to obtain error information. The error information reveals the necessary rotation in order to get a specific encoded Bell pair in the end [step 3)]. The details for entanglement swapping and classical error correction are described in [12]. The encoded quantum repeater was developed for any CSS-code [16, 17].

For simplicity, we will consider the three-qubit repetition code throughout this paper[1]. In the ideal case the encoded state ρ_{enc}, shared between the repeater stations R_i and R_{i+1} at step 1) is of the form $\rho_{\text{enc}} = \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|$ with

$$\left|\tilde{\phi}^+\right\rangle = \frac{1}{\sqrt{2}}\left|000\right\rangle_{R_i}\left|000\right\rangle_{R_{i+1}} + \left|111\right\rangle_{R_i}\left|111\right\rangle_{R_{i+1}}. \quad (1)$$

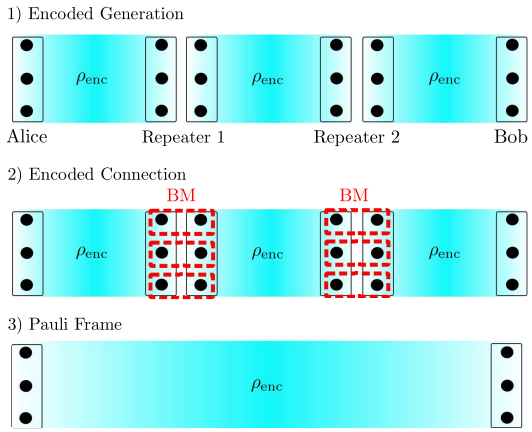


Figure 1. (Color online) Setup of the encoded quantum repeater (adapted from [12]), BM stands for Bell measurement. In the ideal case $\rho_{\text{enc}} = \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|$ with $\left|\tilde{\phi}^+\right\rangle$ defined in Eq. (1).

[1] We will see in Sec. III D that this simple code leads to a good ratio of the secret key rate and the required resources.

1. Error models

Analogously to [2, 12], we will employ the depolarizing error model for all two-qubit gates, thus the unitary operation $U_{i,j}$ acting on qubits i and j is replaced according to the following map $\Lambda(\rho)$:

$$U_{i,j}\rho U_{i,j}^\dagger \to (1-\beta)U_{i,j}\rho U_{i,j}^\dagger + \frac{\beta}{4}\text{tr}_{i,j}(\rho)\otimes \mathbb{1}_{i,j} =: \Lambda(\rho), \quad (2)$$

where β is the gate error parameter. We further assume no misalignment and errorfree one-qubit operations[2]. We define

$$U^a := \mathbb{1}_{\{1,\ldots,N\}\setminus\{i_a,j_a\}} \otimes U_{i_a,j_a}, \quad (3)$$

to be the unitary operation acting on the two qubits (i_a, j_a) and the identity on the remaining $N-2$ qubits. The vector $\vec{U} = \{U^1, \ldots, U^n\}$ defines the sequence of applications of the unitary operations: first one applies the gate U^1 on the qubits i_1, j_1, then U^2 and so on. For our analytical analysis we will approximate the concatenation of n two-qubit gates by assuming that not more than one gate acts in a faulty way (which corresponds to an expansion in β, keeping only terms in zeroth and first order). Normalization is guaranteed by adding the worst case density matrix (i.e., the identity) for the remaining probability.

Thus, the resulting map $\Lambda_{\text{conc}}(\rho)$ is:

$$\Lambda_{\text{conc}}(\rho) := (1-\beta)^n\left(\prod_{a=1}^n U^a\right)\rho\left(\prod_{a=1}^n U^a\right)^\dagger + n\beta(1-\beta)^{n-1}\tilde{\rho} + p\frac{\mathbb{1}_d}{d}, \quad (4)$$

where $d = \dim(\rho)$, $\mathbb{1}_d$ is the $d\times d$-identity matrix, and $p = 1-(1-\beta)^n - n\beta(1-\beta)^{n-1}$. For small β we can expand p in $p \approx \frac{n(n-1)}{2}\beta^2 - n\binom{n-1}{2}\beta^3$, thus p is in the order of β^2 for an appropriate n. The normalized state $\tilde{\rho}$ is given by the map $\Lambda_{1-\text{faulty}}(\rho)$

$$\tilde{\rho} = \frac{1}{n}\sum_{a=1}^n\left(\prod_{b=a+1}^n U^b\right) f\left[(i_a,j_a),\rho,\prod_{c=1}^{a-1}U^c\right]\left(\prod_{b=a+1}^n U^b\right)^\dagger =: \Lambda_{1-\text{faulty}}(\rho), \quad (5)$$

with $f[(i,j),\rho,A] := \text{tr}_{i,j}\left(A\rho A^\dagger\right)\otimes\frac{\mathbb{1}_{i,j}}{4}$. Thus, $\tilde{\rho}$ represents the convex combination of states where one gate is replaced by the identity matrix in the corresponding subspace. Instead of the first-order approximation map in Eq. (4) one could use the simpler map

$$\tilde{\Lambda}(\rho) := (1-\beta)^n\left(\prod_{a=1}^n U^a\right)\rho\left(\prod_{a=1}^n U^a\right)^\dagger + [1-(1-\beta)^n]\frac{\mathbb{1}_d}{d}. \quad (6)$$

But our analysis shows a distinct improvement in the secret key rate using the map in Eq. (4).

[2] This assumption about errorfree single-qubit rotations can be made as these rotations can be implemented in the classical postprocessing (application of bit-flips on the measurement data).

2. Encoded state generation

The first step performed in the encoded quantum repeater is to generate the encoded Bell state of Eq. (1) between all repeater stations. Thus, the encoded Bell state is denoted as (we drop the indices R_i and R_{i+1} for better readability)

$$\left|\tilde{\phi}^+\right\rangle = \frac{1}{\sqrt{2}}\left|000000\right\rangle + \left|111111\right\rangle. \tag{7}$$

To generate this state one starts with the state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ at one repeater station and with $|000\rangle$ at the other and applies a *teleportation-based controlled*-NOT (CNOT) [18–20]:

$$\begin{aligned}&\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\otimes|000\rangle\\ &\xrightarrow{\text{CNOT}}\frac{1}{\sqrt{2}}|000000\rangle + |111111\rangle.\end{aligned} \tag{8}$$

The teleportation-based CNOT consists of multiple gates and requires Bell pairs as a resources, as shown in Fig. 2. The setup

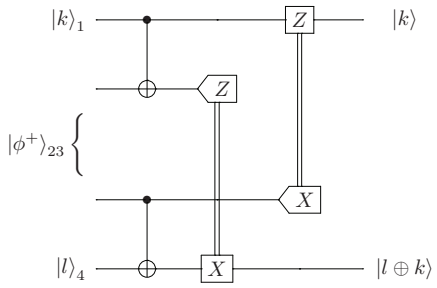


Figure 2. Teleportation-based CNOT, see [20].

in the encoded quantum repeater is shown in Fig. 3. Between the repeater stations we have a source (S) of Bell states. The teleportation-based CNOT is marked by the red dashed box, i.e., qubits 1 and 2 in Fig. 2 correspond to one black and one yellow (light grey) qubit of repeater station i and qubits 3 and 4 to the qubits of repeater station $i+1$. In total we have three teleportation based CNOTs (see Fig. 3). The total circuit in Fig. 3 consists of 6 two-qubit gates, thus we apply the concatenation of gates as described in the map of Eq. (4). The distributed Bell states are depolarized due to imperfections in the source resulting in ρ_{dep} with fidelity F_0:

$$\rho_{\text{dep}} = F_0\left|\phi^+\right\rangle\left\langle\phi^+\right| + \frac{1-F_0}{3}\left(\mathbb{1}_4 - \left|\phi^+\right\rangle\left\langle\phi^+\right|\right). \tag{9}$$

Different to the proposal in [12], we assume that the initial states do not have fidelity F_0 almost one. Due to the depolarizing error of the quantum operations, see Eq. (2), the state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ (repeater station i in Fig. 3) transforms to[3]

[3] We obtain this state by applying two faulty CNOTs ($\text{CNOT}_{1\to3}$ and $\text{CNOT}_{1\to2}$) on the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle$.

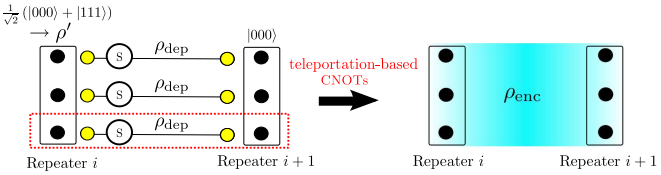


Figure 3. (Color online) Generation of the encoded state ρ_{enc} (see text).

$$\begin{aligned}\rho' = &\frac{1}{2}\left[1+\beta\left(\frac{\beta}{2}-\frac{5}{4}\right)\right](\Pi_{|000\rangle}+\Pi_{|111\rangle})\\ &+\frac{1}{2}(1-\beta)^2(|000\rangle\langle 111| + |111\rangle\langle 000|)\\ &+\frac{\beta}{4}\left(\frac{3}{2}-\beta\right)(\Pi_{|101\rangle}+\Pi_{|010\rangle})\\ &+\frac{\beta}{8}(\Pi_{|001\rangle}+\Pi_{|110\rangle}+\Pi_{|100\rangle}+\Pi_{|011\rangle}),\end{aligned} \tag{10}$$

where $\Pi_{|klm\rangle} = |klm\rangle\langle klm|$. The state ρ_{enc} after all operations is lengthy and will not be given explicitly here.

3. Encoded connection

In the second step we perform three pairwise Bell measurements (BM in Fig. 1 and Fig. 4) in the repeater station in order to connect two encoded Bell pairs. The results of the

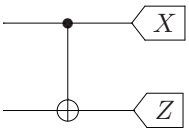


Figure 4. Circuit for a Bell measurement.

Bell measurements determine the encoded Bell state (see [12] for further explanation). As the three-qubit repetition code is used, we can correct up to one bit-flip error in the measurement results. The bit-flip error is corrected via *majority voting*. Note that the error is corrected classically in the measurement results; no quantum operation is performed on the state.

We denote the map for the total encoded connection $\mathcal{C} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H}')$, where $\mathcal{B}(\mathcal{H})$ is the space of bounded operators with $\dim\mathcal{H} = 2^{12}$ and $\dim\mathcal{H}' = 2^6$. The map consists of the following procedures: Bell measurement, correction of the measurement results and application of the corresponding Pauli matrices in order to obtain $\left|\tilde{\phi}^+\right\rangle$ in the end. Note that the action of the Pauli matrices can be replaced by applying bit-flips on the measurement data of the final state. In the following we determine all states $|\varphi_i\rangle \in \mathcal{H}$, such that an application of perfect gates would lead to the correct state, i.e.,

$$\mathcal{C}^{\text{perf}}(|\varphi_i\rangle\langle\varphi_i|) = \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|. \tag{11}$$

a. Correctable errors for ideal CNOT The three-qubit repetition code can correct single bit-flip errors. However, due to the properties of the Bell measurement given in Fig. 4 one can correct more errors, which were not considered in the analysis in [12].

If an X error on the control and the target qubit occurs before a perfect CNOT gate, the resulting error after the application of the CNOT is an X-error on the control qubit (see, e.g., [21]). As the Bell measurement is performed by applying a measurement in the X-basis (Z-basis) on the control (target) qubit, this error does not corrupt the measurement result. The same holds also for Y- and Z-errors if they appear both in the control and target qubit of one CNOT (see Fig. 5).

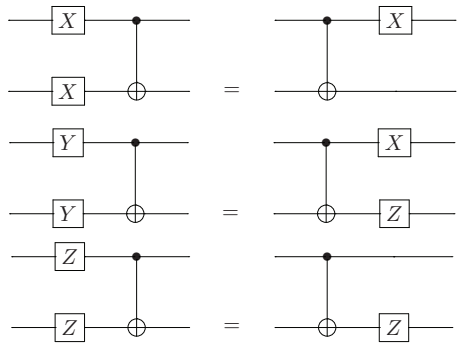


Figure 5. Commutation rules for the CNOT gates, see [21].

Our analysis shows that considering the correlated X-, Y-, and Z-errors leads to a substantially higher error tolerance for obtaining a nonzero secret key rate. As the error in the gates is only important for the secret fraction in Eq. (27), the secret fraction for different initial fidelities as a function of the gate error parameter β is displayed in Fig. 6. We find that including the correlated error makes the secret key rate more noise-tolerant, where the amount of improvement depends on the initial fidelity F_0.

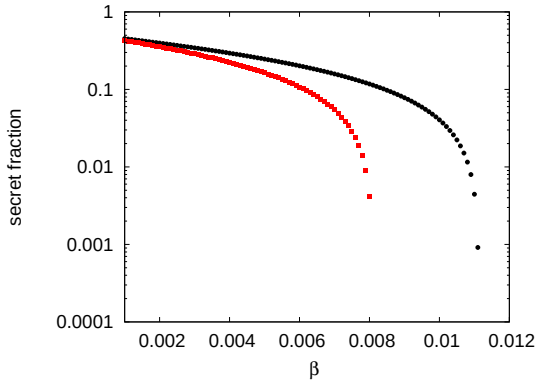


Figure 6. The secret fraction [Eq. (27)] plotted as a function of the gate error β including all errors according to Eq. (12) (black circles) and those where only single bit-flip errors were correctable (red squares), $F_0 = 0.98$, one repeater station ($r = 1$).

We denote the control (target) qubits of the i-th CNOT gate as c_i (t_i), thus we can correct errors from the set

$$E = \{X_{c_i}X_{t_i}, Y_{c_i}Y_{t_i}, Z_{c_i}Z_{t_i}, \mathbb{1}_{c_i}\mathbb{1}_{t_i}, \mathbb{1}_{c_i}X_{t_i}, X_{c_i}\mathbb{1}_{t_i}\}. \quad (12)$$

Each of the six pairs from the set of errors can happen at one of the three CNOT gates, thus we have $6^3 = 216$ combinations. But some of these combinations have to be excluded, e.g., cases like $\mathbb{1}_{c_1}X_{t_1}\mathbb{1}_{c_2}X_{t_2}\mathbb{1}_{c_3}\mathbb{1}_{t_3}$ are not allowed, as they would lead to a wrong measurement outcome for the majority voting (two X-errors cannot be corrected by the three-qubit repetition code). Excluding these cases 160 combinations remain. We count the number of permutations for three CNOT gates: Fixing, e.g., the combination $X_{c_i}X_{t_i}Y_{c_j}Y_{t_j}Z_{c_k}Z_{t_k}$ with $i \neq j \neq k \in \{1,2,3\}$ one has 6 possible permutations of $\{1,2,3\}$. In total we have $160\times6 = 960$ possible combinations of correctable errors. Let us denote these correctable error as E^i, with $i = 1,\ldots,960$, and the set that contains them as E_{corr}.

The probability of successful entanglement swappings is defined by the overlap of the states to be swapped (ρ_{enc}, see Fig. 1) with the correctable states $|\varphi_i\rangle$. These states $|\varphi_i\rangle$ are computed by the action of correctable errors E^i from the set E_{corr} onto the states $\left|\tilde{\phi}^+\right\rangle \otimes \left|\tilde{\phi}^+\right\rangle$:

$$|\varphi_i\rangle := E^i\left(\left|\tilde{\phi}^+\right\rangle \otimes \left|\tilde{\phi}^+\right\rangle\right),\ i = 1,\ldots,960. \quad (13)$$

Out of the 960 correctable states we have 64 distinct orthogonal states, denoted as $|\tilde{\varphi}_i\rangle$. The probability of successful entanglement swapping is thus:

$$p_s = \sum_{i=1}^{64} \langle\tilde{\varphi}_i|\rho_{\text{enc}} \otimes \rho_{\text{enc}}|\tilde{\varphi}_i\rangle, \quad (14)$$

where ρ_{enc} is the output state after the teleportation-based CNOT. This probability holds for one repeater station. For r repeaters we can bound the success probability by[4]

$$P_r = (p_s)^r, \quad (15)$$

because we assumed that the errors can be corrected independently. The final state after entanglement swapping is given by:

$$\rho_{\text{swap}}^{\text{ideal}}(r) = P_r\left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right| + \frac{(1-P_r)}{2^6-1}\left(\mathbb{1}_{2^6} - \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|\right), \quad (16)$$

i.e.,

$$C^{\text{perf}}(\rho_{\text{enc}} \otimes \rho_{\text{enc}}) = \rho_{\text{swap}}^{\text{ideal}}(r). \quad (17)$$

The state given in Eq. (16) is an estimate; with probability P_r we obtain the perfect state and with probability $1 - P_r$ we obtain the completely mixed state without the perfect state.

[4] Note that this estimate is a lower bound, as with more entanglement swappings we could certainly correct more errors.

b. Nonideal CNOT The nonideal CNOT operation in the Bell measurements is obtained by using the noise model of Eq. (4):

$$\Lambda_{\text{CNOT}}(\rho) = (1-\beta)^3 U\rho U^\dagger + 3\beta(1-\beta)^2\tilde{\rho} + \left[1-(1-\beta)^3 - 3\beta(1-\beta)^2\right]\frac{\mathbb{1}_{2^6}}{2^6}, \quad (18)$$

where U is the concatenation of ideal CNOTs. The state $\tilde{\rho}$, see Eq. (5), is the convex combination of states where one of the three CNOT gates is replaced by the identity matrix in the corresponding subspace [see Eq. (2)]. The map for encoded connection with imperfect CNOTs acting on the correctable states $|\tilde{\varphi}_i\rangle$ with $i = 1,\ldots,64$ is

$$\begin{aligned} C^{\text{imperf}}(|\varphi_i\rangle\langle\varphi_i|) &= (1-\beta)^3\left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right| \\ &+ 3\beta(1-\beta)^2\frac{1}{2}\left(\Pi_{|000000\rangle}+\Pi_{|111111\rangle}\right) \\ &+ \left[1-(1-\beta)^3-3\beta(1-\beta)^2\right]\frac{\mathbb{1}_{2^6}}{2^6} \\ &=: \rho_s. \end{aligned} \quad (19)$$

The resulting state for imperfect CNOTs after one round of entanglement swapping is given by:

$$\begin{aligned} &C^{\text{imperf}}(\rho_{\text{enc}}\otimes\rho_{\text{enc}}) \\ &= P_1\rho_s + \frac{1-P_1}{2^6-1}\left(\mathbb{1}_{2^6} - \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|\right). \end{aligned} \quad (20)$$

For more than one repeater station, we use the approximation

$$\begin{aligned} C^{\text{imperf}}\left(|\varphi_i\rangle\langle\varphi_i|^{\otimes r}\right) &= (1-\beta)^{3r}\left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right| \\ &+ 3^r\beta^r(1-\beta)^{2r}\frac{1}{2}\left(\Pi_{|000000\rangle}+\Pi_{|111111\rangle}\right) \\ &+ \left[1-(1-\beta)^{3r}-3^r\beta^r(1-\beta)^{2r}\right]\frac{\mathbb{1}_{2^6}}{2^6} \\ &=: \rho_s(r), \end{aligned} \quad (21)$$

which leads to a lower bound on the secret key rate; higher order terms are represented as identity, more useful states could be present.

Finally, the state with r repeater stations after swapping is given by:

$$\rho_{\text{swap}}^{\text{nonideal}}(r) = P_r\rho_s(r) + \frac{1-P_r}{2^6-1}\left(\mathbb{1}_{2^6} - \left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|\right), \quad (22)$$

with P_r given in Eq. (15).

4. Decoding and final state

In order to do quantum key distribution, one needs to decode the state $\rho_{\text{swap}}^{\text{nonideal}}(r)$ in Eq. (22).

We assume that the decoding procedure is the reverse process of the encoding procedure (see Fig. 7): Alice and Bob each measure two of their three qubits. As we employ the three-qubit repetition code, one can only correct one bit-flip error for Alice and Bob. Other errors cannot be corrected by this code. Depending on their measurement results, Alice and Bob have to correct their qubit with a bit-flip operation. If Alice's and Bob's input state was only subjected to one-qubit bit-flip errors, they only have to correct their qubit if their measurement outcome was "11", which is the case when there was a bit-flip error on the first qubit. If an error occurs in the second or the third qubit, the error does not propagate to the first qubit, thus no correction has to be performed.

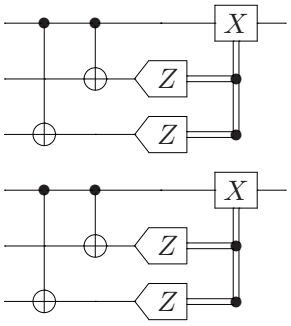


Figure 7. Decoding procedure: The upper three qubits are on Alice's and the lower are on Bob's side.

To obtain the final state which is used for quantum key distribution, we take the state after swapping in Eq. (22) and perform the decoding operation $\mathcal{D}$:

$$\rho_{\text{dec}} = \mathcal{D}\left[\rho_{\text{swap}}^{\text{nonideal}}(r)\right]. \quad (23)$$

The decoding map has the following properties:

$$\mathcal{D}\left(\left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|\right) = |\phi^+\rangle\langle\phi^+|, \quad (24a)$$

$$\mathcal{D}\left(\Pi_{|000000\rangle}+\Pi_{|111111\rangle}\right) = |00\rangle\langle 00| + |11\rangle\langle 11|, \quad (24b)$$

$$\mathcal{D}\left(\tfrac{\mathbb{1}_{2^6}}{2^6}\right) = \tfrac{1}{4}|\phi^+\rangle\langle\phi^+| + \tfrac{3}{4}\left[\tfrac{1}{3}\left(\mathbb{1}_{2^2} - |\phi^+\rangle\langle\phi^+|\right)\right] = \tfrac{\mathbb{1}_{2^2}}{4} \quad (24c)$$

The first property [Eq. (24a)] follows from the action of the CNOT gates, see Fig. 7:

$$\left|\tilde{\phi}^+\right\rangle \to |\phi\rangle^+_{1,4}\otimes|0000\rangle_{2,3,5,6}, \quad (25)$$

where the index denotes the number of qubits. The second property [Eq. (24b)] can be shown in an analogous way:

$$\begin{aligned} &\Pi_{|000000\rangle}+\Pi_{|111111\rangle} \\ &\to \left(|00\rangle\langle 00|_{1,4} + |11\rangle\langle 11|_{1,4}\right)\otimes|0000\rangle\langle 0000|_{2,3,5,6}. \end{aligned} \quad (26)$$

The last equality [Eq. (24c)] can be verified by inserting the completely mixed state into the decoding map. Using Eqs. (21) and (22) the state after perfect decoding is given by:

$$\begin{aligned} \rho_{\text{dec}} &= \left[P_r(1-\beta)^{3r} - \frac{1-P_r}{2^6-1}\right]\left|\phi^+\right\rangle\left\langle\phi^+\right| \\ &+ P_r 3^r\beta^r(1-\beta)^{2r}\frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) \\ &+ \left[P_r q_r + \frac{(1-P_r)2^6}{2^6-1}\right]\frac{\mathbb{1}_{2^2}}{4}, \end{aligned} \quad (27)$$

with $q_r = 1-(1-\beta)^{3r} - 3^r\beta^r(1-\beta)^{2r}$.

We can also include gate errors in the decoding, by again using the error model in Eq. (4), leading to the final state:

$$\begin{aligned}\rho_{\text{final}} &= (1-\beta)^4\rho_{\text{dec}} \\ &\quad +4\beta(1-\beta)^3\rho_{\text{dec}}^{\text{nonideal}} \\ &\quad +(1-(1-\beta)^4-4\beta(1-\beta)^3)\frac{\mathbb{1}_4}{4},\end{aligned} \tag{28}$$

where $\rho_{\text{dec}}^{\text{nonideal}} = \mathcal{D}^{\text{imperf}}(\rho_{\text{swap}}^{\text{nonideal}}(r))$ which is composed of $\Lambda_{1-\text{faulty}}(\rho_{\text{swap}}^{\text{nonideal}}(r))$, see Eq. (5), and applying the correcting operation (see Fig. 7) such that

$$\begin{aligned}&\mathcal{D}^{\text{imperf}}\left(\left|\tilde{\phi}^+\right\rangle\left\langle\tilde{\phi}^+\right|\right) = \mathcal{D}^{\text{imperf}}\left(\frac{1}{2}\left(\Pi_{|000000\rangle}+\Pi_{|111111\rangle}\right)\right) \\ &= \frac{1}{2}\left\{\left[\frac{3}{8}\left(|00\rangle\langle 00|+|11\rangle\langle 11|\right)+\frac{1}{8}\left(|01\rangle\langle 01|+|10\rangle\langle 10|\right)\right]\right. \\ &\quad \left.+\frac{\mathbb{1}_4}{4}\right\} \\ &=: \tilde{\rho}'.\end{aligned} \tag{29}$$

The state $\rho_{\text{dec}}^{\text{nonideal}}$ is given by

$$\begin{aligned}\rho_{\text{dec}}^{\text{nonideal}} &= P_r\left\{\left[(1-\beta)^{3r}+3^r\beta^r(1-\beta)^{2r}\right]\tilde{\rho}'\right. \\ &\quad \left.+\{1-[(1-\beta)^{3r}+3^r\beta^r(1-\beta)^{2r}]\}\frac{\mathbb{1}_4}{4}\right\} \\ &\quad +\frac{1-P_r}{2^6-1}\left(2^6\frac{\mathbb{1}_4}{4}-\tilde{\rho}'\right).\end{aligned} \tag{30}$$

We now use the final state ρ_{final} in Eq. (28) to calculate secret key rates.

B. Secret key rate

Analogously to [11], we define the secret key rate per memory per second for the repeater to be

$$K^\nu = R^\nu\frac{r_\infty}{M^\nu}, \tag{31}$$

where R^ν is the repeater rate, i.e., the average number of generated entangled Bell pairs per second for the repeater scheme[5] ν, r_∞ is the secret fraction, i.e., the ratio of secret bits and measured bits in the asymptotic limit (Devetak-Winter bound [22]) and M^ν is the number of memories used for each protocol. For the three-qubit repetition code employed here, the number of memories per half node of a repeater station is given by

$$M^{\text{QEC}} = 6, \tag{32}$$

as we need six qubits on each side to perform the teleportation-based CNOT (see Fig. 3). The formula for the secret fraction using the six-state protocol [23, 24] can be found, e.g., in Ref. [25]:

$$\begin{aligned}r_\infty &= 1-e_Z h\left(\frac{1+(e_X-e_Y)/e_Z}{2}\right) \\ &\quad -(1-e_Z)h\left(\frac{1-(e_X+e_Y+e_Z)/2}{1-e_Z}\right) \\ &\quad -h(e_Z),\end{aligned} \tag{33}$$

where the binary Shannon entropy is given by

$$h(p) = -p\log_2 p-(1-p)\log_2(1-p), \tag{34}$$

and e_X, e_Y and e_Z are the error rates in the X-, Y-, and Z-basis, respectively. The analytic form of the error rates for Bell-diagonal states can be found in [25]. It is possible to perform the analysis in an analogous way for other QKD-protocols such as the BB84-protocol [26].

The remaining term in the secret key rate is the repeater rate R^ν, which is the average number of generated entangled Bell pairs per second. For its derivation, we first estimate the average waiting time to distribute the Bell pairs needed for the teleportation-based CNOT (see Fig. 2). The probability of successful generation of one Bell pair over the distance L_0 is

$$P_0 = 10^{-\alpha L_0/10}, \tag{35}$$

with $\alpha = 0.17$ dB/km a realistic photon absorption coefficient for telecom fibers. The probability P_0 corresponds to the transmittivity of photons in an optical fiber with an attenuation length of $L_{\text{att}} = 25.5$ km. In [27] the average waiting time for generating N Bell pairs with probability P_0 is given by

$$\langle T\rangle_N = T_0 Z_N(P_0), \tag{36}$$

where $T_0 = L_0/c$ is the fundamental time (where $c = 2\times 10^5$ km/s is the speed of light in the fiber) and

$$Z_N(P_0) := \sum_{j=1}^{N}\binom{N}{j}\frac{(-1)^{j+1}}{1-(1-P_0)^j} \tag{37}$$

is the average number of attempts to connect N pairs, see [27]. For the encoded quantum repeater with r repeater stations we need to establish $3(r+1)$ Bell pairs, thus the repeater rate (the reciprocal value of the average waiting time) for the encoded quantum repeater is given by

$$R^{\text{QEC}} = \frac{1}{\langle T\rangle} = \frac{1}{2T_0 Z_{3(r+1)}(P_0)}, \tag{38}$$

under the assumption that the entanglement swapping process is deterministic, i.e., the probability of successful entanglement swapping is one. The factor 2 in front of the fundamental time T_0 accounts for the time needed to send a photon and acknowledge its arrival. Note that no further classical communication is needed in this repeater protocol. This is contrary to the generic quantum repeater, where after distillation and entanglement swapping in each step the success has to be communicated [11]. We will compare this protocol with respect to the secret key rate to the generic quantum repeater which needs much more classical communication.

[5] By the repeater scheme ν, we mean the scheme mentioned in the introduction: either the encoded quantum repeater (ν = QEC) or the generic quantum repeater (ν = QR).

III. RESULTS AND COMPARISON OF THE SECRET KEY RATES

In this section, we first investigate the minimally required parameter values for obtaining a nonzero secret key for the encoded quantum repeater. Then we find the optimal secret key rate by optimizing over the encoded quantum repeater and the generic quantum repeater model (see [11]). We further state the differences between our analysis and the analysis given in [12]. The recent development of a repeater scheme which consumes minimum classical communication time [15] is a further subject of our investigation. We calculate the cost function which is the minimum number of total memory qubits per secret bit for the aforementioned scheme and compare it to the schemes analyzed in this work.

A. Minimal parameter values

Similar to our analysis in [10], we derive for the encoded quantum repeater the minimally required parameter values, i.e., the initial fidelity F_0 [for the depolarized state given in Eq. (9)] and the gate quality $p_G = 1-\beta$ [see Eq. (4)], to obtain a nonzero secret key, see Eq. (31). Table I summarizes the results of our investigations about the minimal fidelities and gate qualities, which are needed to achieve a nonzero secret key rate.

r	N	$p_{G,\min}$	$F_{0,\min}$
1	1	0.984	0.943
3	2	0.992	0.972
7	3	0.994	0.981
15	4	0.996	0.986
31	5	0.997	0.989
63	6	0.997	0.991
127	7	0.998	0.992

Table I. Minimal gate quality $p_{G,\min}$ [see Eq. (4) with $p_G = 1-\beta$ and $F_0 = 1$] and minimal fidelity $F_{0,\min}$ with $p_G = 1$ for extracting a secret key for the six-state protocol, see Eq. (33), with $r = 2^N - 1$ repeater stations, where N is the nesting level for entanglement swapping.

Comparing these numbers to the results for the generic quantum repeater in [10], we find that the encoded quantum repeater is less tolerant against gate errors. This can be expected as many gates are needed for generating the encoded Bell pair. Regarding the initial fidelity F_0, the encoded quantum repeater also requires fairly good initial Bell states. In Fig. 8, we show the secret key rate for the encoded quantum repeater, optimized with respect to the number of repeater stations, as a function of the gate quality p_G and initial fidelity F_0, for a fixed distance. We find that a nonzero secret key rate for the encoded quantum repeater is restricted to gate errors below $\beta = 0.0165$ and fidelities above $F_0 = 0.943$.

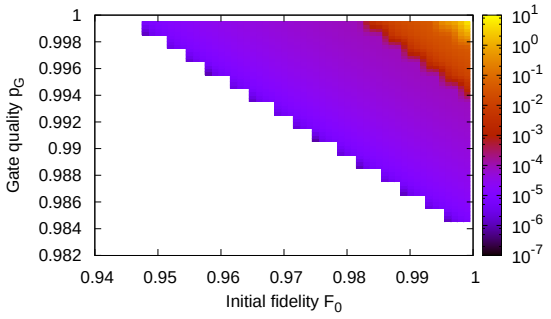


Figure 8. (Color online) The optimal secret key rate per memory per second, see Eq. (31), as a function of the initial fidelity F_0 and the gate quality p_G, optimized over the number of repeater stations for the encoded quantum repeater ($L = 600$ km). In the white region it is not possible to extract a nonzero secret key.

B. Optimal secret key rates

The purpose of this paper is to investigate whether the optimal secret key rate is reached for the encoded or the generic quantum repeater. By the generic quantum repeater, we mean the repeater scheme using distillation (either the *Deutsch et al.* [6] or the *Dür et al.* [2] distillation protocols, see [11]).

Figure 9 shows the optimal secret key rate per memory per second [Eq. (31)] for the two different repeater schemes plotted as the function of the distance for some realistic parameter values (initial fidelity $F_0 = 0.98$ and gate quality $p_G = 0.992$). We find that the generic quantum repeater leads to an optimal secret key rate that is one order of magnitude better than the encoded quantum repeater. We know from [11] that in this range of parameter values it is optimal for the generic quantum repeater to not distill, thus the number of used memories is one in this case. For the encoded quantum repeater, however, we constantly use six memories [see Eq. (32)] which reduces the secret key rate by this factor. In the case of no distillation and deterministic entanglement swapping the encoded quantum repeater is not an advantage for the chosen parameter values. Also in regimes where distillation is optimal for the generic quantum repeater (see [11]), we find that the encoded repeater is never better.

C. Comparison to the scheme in Jiang et al.

As mentioned in the introduction, Ref. [12] analyzes the errors of the encoded quantum repeater. Different to their analysis, we allow the initial Bell pairs to have a fidelity $F_0 < 1$, whereas in the original reference fault-tolerant distillation is assumed which would require additional qubits and operations. Also we do not perform fault-tolerant initialization of the codes which has the following advantages: our scheme saves resources and no additional measurements have to be realized. Our error model, see Eq. (4), is a very good estimate, especially for the β resulting from our investigations of the

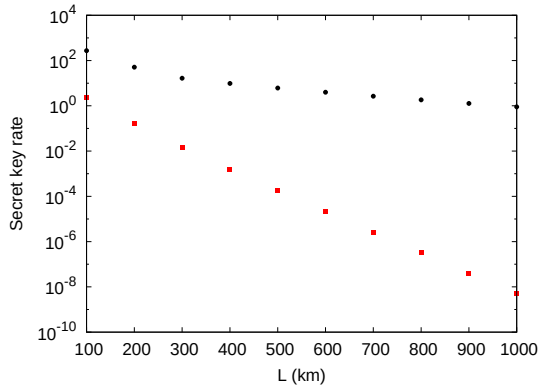


Figure 9. (Color online) The optimal secret key rate per memory per second in Eq. (31) for the encoded (red squares) and the generic quantum repeater (black circles) as a function of the total distance L (Parameters: $F_0 = 0.98$, $p_G = 0.992$).

minimal parameter values ($\beta = 10^{-2} - 10^{-3}$, see Sec. III A): the probability p for the identity is on the order of 10^{-3}. It means that the distance to a map, where the exact output state is used, is small. We verified this statement for the decoding map (Sec. II A 4) and found that the Uhlmann fidelity of the state in Eq. (28) compared to a state calculated with a map, where all gates with errors are used, is one for the range of β given above. - So far, we do not consider memory and measurement errors, but they could be implemented in a straightforward way to our analysis (see discussion in the conclusions).

Another difference in the analysis is the repeater rate. In [12] it was assumed that the generation rate for undistilled Bell pairs with m qubits[6] available at each station is given by[7]

$$R = m\frac{P_0}{L_0}, \tag{39}$$

using a perfect overall efficiency for collecting and detecting single photons. This is only an appropriate estimate in the case of infinitely many memories. We considered that exactly m Bell pairs to start the encoding process are needed and one has m memories instead of infinitely many memories available. This results in the estimate with the average waiting time as described by Eq. (37) (Sec. II B) and leads to a decrease of the repeater rate [Eq. (38)] by several orders of magnitude[8] compared to Eq. (39).

D. Cost function

Recently, in [15] a quantum repeater scheme was investigated that only uses one-way classical communication without the necessity to herald the successful generation of entangled Bell pairs between the repeater stations.

In [15], the cost function was defined to be the minimum number of total memory qubits per secret bit:

$$C = \min_{\nu,N} \frac{2^{N+1}}{K^{\nu}}, \tag{40}$$

where K is the secret key rate as defined in Eq. (31), N is the nesting level and ν is the index for the chosen protocol. The factor 2^{N+1} accounts for the total number of memories [with the number of memories M per half node of the repeater station, see Eq. (32), being implicitly contained in the secret key rate K]: $(2^N - 1)2$ is the sum of all memory qubits in the repeater stations ($r = 2^N - 1$). Adding 2 memory qubits from the two communicating parties (Alice and Bob) results in 2^{N+1} memory qubits in total.

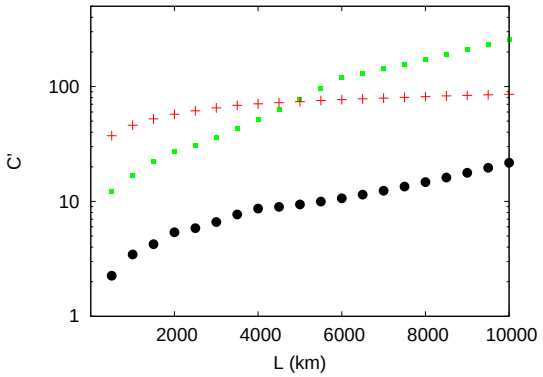


Figure 10. (Color online) The cost coefficient ($C' = C/L$) [Eq. (40)] for the encoded (green squares), the generic quantum repeater (black circles) and the quantum repeater protocol presented in [15] (red crosses, with the effective qubit error $\varepsilon = 10^{-4}$, for an explanation see [15]) as a function of the total distance L (Parameters: $F_0 = 0.99995$, $p_G = 0.9999$, and $T_0 = 1$ as in [15]).

Figure 10 shows the cost coefficient C', which is the cost function C [Eq. (40)] divided by the total length L, using the encoded quantum repeater with the three-qubit repetition code, the generic quantum repeater and the repeater protocol presented in [15]. The optimal distillation protocol for the generic quantum repeater is the *Deutsch et al.* protocol. We find that up to 5000 km both the generic quantum repeater and the encoded quantum repeater are below the cost coefficient given in [15]. The generic quantum repeater has a better resource efficiency for all distances. The generic quantum repeater needs less resources and the overhead in classical communication is compensated by fewer numbers of qubit memories used.

In Fig. 11, we show the optimal distance L_0 between the repeater stations for the encoded and the generic quantum repeater as a function of L. We point out that L_0 is in the order of 30 – 100 km, depending on L, while the optimal distance in [15] was given by 1 – 2 km. In the generic quantum repeater scheme the total number of required repeater stations is circa 1 – 2 orders of magnitude smaller than in [15].

[6] Note that $m = M/2$ with M given in Eq. (32).

[7] The probability of successful transmission P_0 [see Eq. (35)] is equivalent to the expression $\exp(-L_0/L_{\text{att}})$ given in [12].

[8] The repeater rate and thus the secret key rate can be increased by using multiplexing as shown in [28].

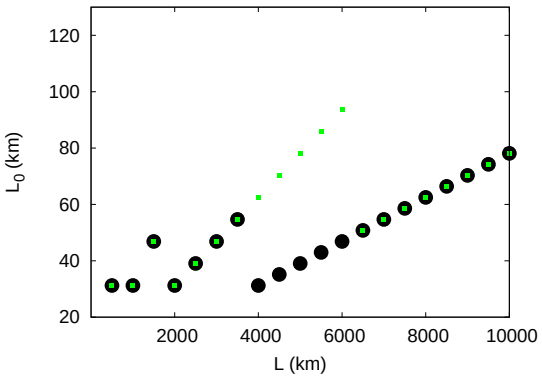


Figure 11. (Color online) The optimal distance between the repeater stations L_0 for the cost coefficient ($C' = C/L$), see Eq. (40), for the encoded (green squares) and the generic quantum repeater (black circles) (parameters $F_0 = 0.99995$ and $p_G = 0.9999$, $T_0 = 1$ as in [15]) as a function of the total distance L.

IV. CONCLUSIONS

We investigated secret key rates for the so-called *encoded quantum repeater* that utilizes quantum error-correcting codes instead of entanglement distillation as used in the *generic quantum repeater*. The advantage of the former repeater scheme is that the classical communication is minimal as it is needed only for the entanglement generation. Minimal time consumption is essential for non-perfect memories. Before starting to calculate the secret key rate, we improved the error model for the encoded quantum repeater [12] and replaced it by a concatenated one, which leads to a very good estimate of the fidelity. This model permits us to start with Bell pairs with fidelity smaller than one. We also accounted for additional correctable errors for the encoded connection of the encoded Bell states, leading to higher secret key rates, and finally developed a decoding algorithm suitable for the three-qubit repetition code using an analogous error model. We estimated the minimally required parameter values for a nonzero secret key and found that for many repeater stations the requirements for the gate quality and the initial fidelity of the Bell pairs are quite demanding. In order to calculate the secret key rate for the encoded quantum repeater, we derived the rate for generating entangled pairs. The comparison of the secret key rates for the encoded and generic quantum repeater showed that the generic scheme is advantageous for the whole considered range of parameter values for the gate quality and the initial fidelity. Finally, we calculated the cost function for the repeater schemes studied here. The cost function determines the required resources divided by the secret key rate. We found that the cost function for the schemes analyzed here is better than the scheme presented in [15], for a wide range of parameters. Furthermore, the number of repeater stations is circa $1-2$ orders of magnitude smaller than in the latter scheme.

So far, measurement errors are excluded, but can be implemented easily in our analysis in the same manner as done in [10]. The measurement error will not change the qualitative results of the paper; the secret key rate will decrease. So far, we treated perfect memories. Memory errors (see, e.g., [29]) may change the results as the lower communication time (and thus the lower degradation of the state) of the encoded quantum repeater might compensate the additional need for resources and thus increase the secret key rate. This investigation is left for future work.

The secret key rate can be improved by applying multiplexing (see, e.g., [28]). As we performed the calculations on density matrices, the quantum error-correcting codes used here for the encoded quantum repeater are limited to a small number of qubits. As an example we treated the three-qubit repetition code. We showed that even with this simple quantum error-correcting code we can have an advantage regarding the cost function over complicated schemes using more resources. We conjecture that utilizing more sophisticated codes (see, e.g., [12]) does not lead to an increase of the secret key rate, as more resources are needed especially when the encoding is performed with errors.

ACKNOWLEDGMENTS

The authors thank Michael Epping, Sreraman Muralidharan, and Liang Jiang for discussions. The authors acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, project QuOReP).

[1] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Physical Review Letters **81**, 5932 (1998).
[2] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Physical Review A **59**, 169 (1999).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **74**, 145 (2002).
[4] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Physical Review Letters **71**, 4287 (1993).
[5] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Physical Review Letters **76**, 722 (1996).
[6] D. Deutsch, A. K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Physical Review Letters **77**, 2818 (1996).
[7] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).
[8] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Physical Review Letters **96**, 240501 (2006).
[9] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Review of Modern Physics **83**, 33 (2011).
[10] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Physical Review A **87**, 052315 (2013).
[11] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß,

Physical Review A **87**, 062335 (2013).
[12] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Physical Review A **79**, 032325 (2009).
[13] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, Nature Photonics **4**, 792 (2010).
[14] L. Hartmann, B. Kraus, H. J. Briegel, and W. Dür, Physical Review A **75**, 032310 (2007).
[15] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, (2013), arXiv:arXiv:1310.5291v1.
[16] A. R. Calderbank and P. W. Shor, Physical Review A **54**, 1098 (1996).
[17] A. Steane, Proc. R. Soc. A **452**, 2551 (1996).
[18] D. Gottesman and I. Chuang, Nature **402**, 390 (1999).
[19] X. Zhou, D. W. Leung, and I. L. Chuang, Physical Review A **62**, 052316 (2000).
[20] L. Jiang, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Physical Review A **76**, 062323 (2007).
[21] M. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).
[22] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
[23] D. Bruß, Physical Review Letters **81**, 3018 (1998).
[24] H. Bechmann-Pasquinucci and N. Gisin, Physical Review A **59**, 4238 (1999).
[25] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).
[26] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984) p. 175.
[27] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Physical Review A **83**, 012323 (2011).
[28] S. Abruzzo, H. Kampermann, and D. Bruß, Physical Review A **89**, 012303 (2014).
[29] S. Abruzzo, H. Kampermann, and D. Bruß, Physical Review A **89**, 012301 (2014).

"Secret key rates for an encoded quantum repeater."
Bratzik, S., Kampermann, H. und Bruß, D.
`arXiv:1401.6859v1`, *zur Publikation angenommen bei Physical Review A*, 2014.

Journal: Physical Review A
Impact factor: 3,042
Anteil an der Arbeit: 90%, 1. Autor, Schreiben des Manuskriptes und Ausführung der Rechnungen

Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate

Sylvia Bratzik,* Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany
(Received 25 March 2013; published 26 June 2013)

We investigate quantum repeaters in the context of quantum key distribution. We optimize the secret key rate per memory per second with respect to different distillation protocols and distillation strategies. For this purpose, we also derive an analytical expression for the average number of entangled pairs created by the quantum repeater, including classical communication times for entanglement swapping and entanglement distillation. We investigate the impact of this classical communication time on the secret key rate. Finally, we study the effect of the detector efficiency on the secret key rate.

DOI: 10.1103/PhysRevA.87.062335 PACS number(s): 03.67.Hk, 03.67.Dd, 03.67.Bg

I. INTRODUCTION AND MOTIVATION

Losses in the optical fiber limit the distance for the distribution of entangled photon pairs and, hence, the range of quantum key distribution. Recent experiments cannot reach more than a few hundred kilometers (see, e.g., Ref. [1]). To overcome this problem, the concept of a quantum repeater was developed [2,3], which acts like a "distance amplifier:" It permits enhancing the probability that an entangled pair is created at a certain distance (see, e.g., calculations in Ref. [4]). For a recent review on quantum repeaters, see Ref. [5]. The main ingredients of a quantum repeater are entanglement swapping [6] and entanglement distillation [7–9]. After the distribution of entangled photon pairs between two distant parties, one can perform quantum key distribution (for reviews, see, e.g., Refs. [4,10]).

Since the original proposal of the quantum repeater, existing protocols were analyzed or were improved, *inter alia* [11–25]. Moreover, new protocols, such as, e.g., the hybrid quantum repeater [23] or quantum repeaters with atomic ensembles [26], were introduced.

Recently, the following analyses of the secret key rate in connection with a quantum repeater were performed: In Ref. [27], a quantum key distribution (QKD) setup with one repeater node and without distillation is investigated. In this case, the parameters for the optimal secret key rate are explored. In Ref. [28], the secret key rate for one node of the Duan-Lukin-Cirac-Zoller (DLCZ) repeater [26] is analyzed. Reference [29] treats a variation of the DLCZ repeater, namely, Ref. [20]. In Ref. [30], secret key rates for the original quantum repeater [2], for the hybrid quantum repeater [23], and for a variation of the DLCZ repeater [18] are investigated where distillation was considered only before the first entanglement swapping. Here, we want to lift this restriction and allow distillation in all nesting levels.

The main goal of the current paper is to analyze the achievable secret key rate under different distillation protocols and strategies. For the distillation protocols, we consider a recurrence protocol [9] and the entanglement pumping protocol [3]. The protocol [9] is more efficient regarding the final fidelity for perfect gates but at the expense of an exponentially growing number of memories. The protocol in Ref. [3] reaches a higher fidelity than the protocol in Ref. [9] in a certain regime of errors and uses less spatial resources but at the expense of a temporal overhead. As performed in Refs. [29,31], we will divide the secret key rate by the number of memories needed per node. For the distillation strategies of the quantum repeater, we consider a nested distillation scheme, i.e., where distillation after each swapping is performed. A special case will be distillation only before the first swapping, which might be experimentally more feasible. We thoroughly investigate the case where the number of distillation rounds in each nesting level is identical. Then, we lift this restriction and vary the number of distillation rounds individually after each swapping. Additionally, we account for the classical communication time needed for acknowledging the success of entanglement swapping and entanglement distillation in the quantum repeater nodes. For this purpose, we will derive a formula for the generation rate of the entangled pairs (repeater rate) including these classical communication times.

The paper is structured as follows: In Sec. II, we review the concept of quantum repeaters, the relevant distillation protocols, and the distillation strategies. In Sec. III, we present analytical formulas for the secret key rates. As the secret key rate is a product of the secret fraction and the repeater rate, we will derive the latter for the different distillation protocols. In Sec. IV, we analyze the quantum repeater in the context of quantum key distribution and present the optimal secret key rates. Here, the secret key rates are optimized with respect to the different distillation protocols and distillation strategies, the number of nesting levels, the number of distillation rounds, and the number of used memories. Furthermore, we investigate the impact of finite-efficiency detectors on the secret key rate. Then, we will fix the number of required memories and will investigate the optimal setup. In Sec. V, the influence of the classical communication time on the secret key rate is analyzed. We conclude in Sec. VI.

II. QUANTUM REPEATER AND DISTILLATION STRATEGIES

In Fig. 1, we show a quantum repeater setup, whose concept was introduced in Ref. [2]. The goal is to establish an entangled pair between the two parties Alice and Bob over distance L. For

*bratzik@thphy.uni-duesseldorf.de

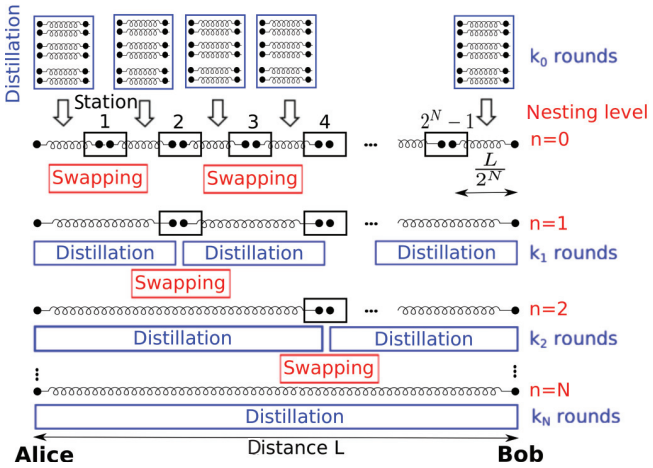


FIG. 1. (Color online) A generic quantum repeater protocol with nested distillation (see text).

this reason, one divides the distance into segments of length $L_0 = \frac{L}{2^N}$, where N is the number of *maximal nesting levels* for swapping. The segments are connected by repeater stations, which are able to perform Bell measurements and distillation. Due to entanglement swapping, the fidelity degrades, which we compensate by entanglement distillation. We define the fidelity of a state ρ as its overlap with the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, i.e.,

$$F(\rho) := \langle\phi^+|\rho|\phi^+\rangle, \tag{1}$$

where $|0\rangle$ ($|1\rangle$) is, e.g., a horizontally (vertically) polarized photon.

In the following, we will describe the distillation protocols that we want to compare. Our figure of merit is the secret key rate. Note that the influence of distillation on the fidelity was studied in Ref. [3]. The analysis of distillation protocols on the entanglement generation rate was investigated in Ref. [32]. As the secret key rate is a nontrivial function of these and other parameters, we will arrive at new results. In the following, we will assume, analogous to Ref. [3], that the quantum gates are subjected to depolarizing noise with probability $(1 - p_G)$ and with probability p_G, they are perfect.[1]

A. The distillation protocols

General distillation protocols consist of performing local operations on n-qubit pairs resulting in $m < n$ pairs with a higher fidelity than the initial pairs. Throughout this paper, we will consider protocols that operate on two-qubit pairs and lead to one-qubit pair. Usually, local operations and a CNOT gate are applied. The sequence of these operations is specific for every protocol. Finally, both parties perform a measurement and, depending on the outcome, the resulting pair has a higher fidelity or is discarded. Thus, the protocols are probabilistic.

[1]The formulas for the fidelity and the success probability considering this error parameter can also be found in Ref. [3]. Different from Ref. [3], we do not assume any misalignment, and the single-qubit operation is error free.

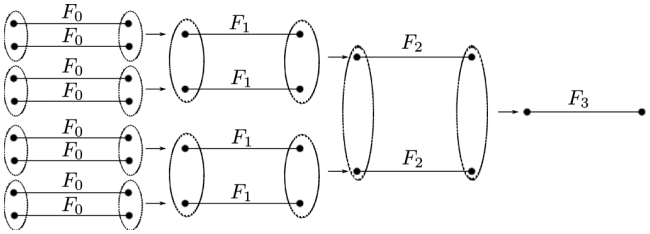


FIG. 2. Recurrence protocol: The *Deutsch et al.* protocol (figure adapted from Ref. [3]). The fidelity F_k is the fidelity in the kth distillation round.

In the following, we briefly describe the protocols considered in this paper.

1. Recurrence protocol: The Deutsch et al. protocol

The *Deutsch et al.* protocol [9], sometimes called the *Oxford protocol*, works in a similar way as the distillation protocol introduced in Refs. [7,8] but is more efficient. It can reach a higher fidelity in fewer distillation rounds and, therefore, results in higher secret key rates. In general, the protocol operates on Bell-diagonal states, i.e.,

$$\rho_{\text{Bell}} = A\Pi_{|\phi^+\rangle} + B\Pi_{|\phi^-\rangle} + C\Pi_{|\psi^+\rangle} + D\Pi_{|\psi^-\rangle}, \tag{2}$$

with $A,B,C,D \geqslant 0$, $A+B+C+D=1$, and $\Pi_{|\psi\rangle} = |\psi\rangle\langle\psi|$ being the projectors onto the four Bell states $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. For each state of the form in Eq. (2), the first qubit belongs to Alice, and the second belongs to Bob. Both share two pairs of the state given in Eq. (2). Alice (Bob) applies a $\pi/2$ $(-\pi/2)$ rotation about the X axis on her (his) two qubits, followed by a CNOT operation on both sides. After that, a bilocal measurement on one qubit in the computational basis is performed. The values of parameters A, B, C, and D as a function of the imperfections of the CNOT and the fidelity F can be found in Ref. [33]. The protocol works in a recursive way, i.e., it uses two copies of the same fidelity for the next distillation step; therefore, it is called the *recurrence protocol* (see Fig. 2).

2. Entanglement pumping: The Dür et al. protocol

This protocol, introduced in Ref. [3], sometimes also called the *Innsbruck protocol*, uses the *Deutsch et al.* protocol, but the two input states do not need to have the same fidelity. Here, distillation is performed with an auxiliary pair always having the same initial fidelity F_0, see Fig. 3, hence, the name *entanglement pumping*. We see that, different from the *Deutsch et al.* protocol, the number of required memories does not depend on the number of rounds of distillation, but it is linear in the number of nesting levels (see Sec. III C).

Throughout the paper, we will assume that we only start with entanglement swapping and entanglement distillation when both pairs are present.

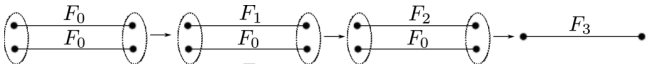


FIG. 3. Entanglement pumping: *Dür et al.* protocol (figure adapted from Ref. [3]).

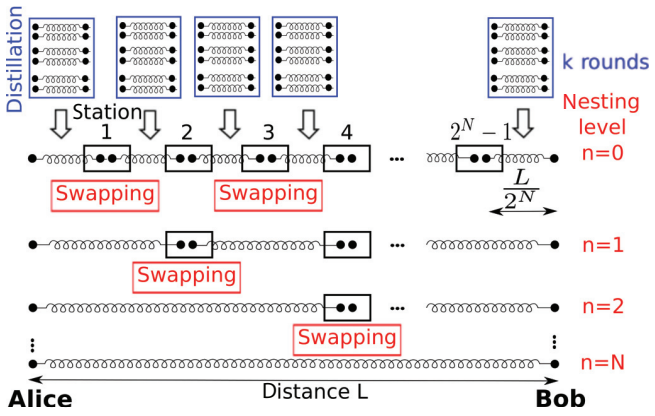


FIG. 4. (Color online) *Distillation strategy* β: distillation only in the beginning.

B. Distillation strategies for the quantum repeater

The protocols described in the previous section can be inserted into the quantum repeater protocol in different ways. In the following, we want to compare two different specific distillation strategies. For this purpose, we define the distillation vector,

$$\vec{k} = (k_0, \ldots, k_N) \tag{3}$$

for the distillation rounds where each component with index n gives the number of distillation rounds in the nth nesting level (see Fig. 1). Throughout the paper, *distillation strategy* α denotes a strategy with the same number of distillation rounds in each nesting level, hence, the distillation vector is $\vec{k}^\alpha = (k, \ldots, k)$. A strategy, which might be less demanding for experimental realizations,[2] is the *distillation strategy* β (see Fig. 4) where we only distill at the beginning. The distillation vector is, thus, $\vec{k}^\beta = (k, 0, \ldots, 0)$. In Sec. IV C 1, we will use general distillation vectors. This strategy will be called *distillation strategy* γ.

III. SECRET KEY RATES AND THE QUANTUM REPEATER

In the previous section, we have described the generation of entangled pairs over a distance L between the parties Alice and Bob using the quantum repeater protocol. For performing QKD, they measure each of their particles in some measurement basis. In this paper, we consider the six-state protocol [34,35]; the BB84 protocol [36] leads to similar secret key rates. The former works as follows: For each qubit pair, Alice and Bob each perform measurements in the X, Y, and Z directions. After the measurement, the used basis is announced (*sifting phase*). Only those measurement results where their measurement bases coincided will be utilized in the further analysis. Here, we adopt the asymmetric protocol [37], which uses different probabilities for the choice of the measurement direction. In this protocol, the sifting parameter, i.e., the fraction of sifted bits, is the one in the asymptotic limit, which we also assume here. The quantum bit error rate, i.e., the fraction of discordant bits, bounds the eavesdropping attempt: If it is above a certain threshold, the protocol is aborted. The quantity we are interested in is the *secret key rate* K per memory per second, which is the product of the *repeater rate* R_{Rep} and the *secret fraction* r_∞ (see, e.g., Ref. [4] for a review) divided by the number of memories,

$$K^i = R^i_{\mathrm{Rep}}(\vec{k}, N, L) r^i_\infty(F_0, p_G, \vec{k}, N)/M^i(\vec{k}, N), \tag{4}$$

with the superscript i being either D (the *Deutsch et al.* protocol) or Dür (the *Dür et al.* protocol).

In the following sections, we will describe or will derive each component of the secret key rate given in Eq. (4).

A. The secret fraction

The secret fraction is the ratio of secret bits and the measured bits in the asymptotic limit, thus, denoted by r_∞. It is given by the so-called Devetak-Winter bound [38] and can be expressed in terms of the error rates appearing in the six-state protocol [4], Appendix],

$$r_\infty = 1 - e_Z h\left(\frac{1 + (e_X - e_Y)/e_Z}{2}\right) - (1 - e_Z) h\left(\frac{1 - (e_X + e_Y + e_Z)/2}{1 - e_Z}\right) - h(e_Z), \tag{5}$$

with $h(p) = -p \log_2 p - (1-p)\log_2(1-p)$ being the binary Shannon entropy and e_X, e_Y, and e_Z being the error rates in the X, Y, and Z bases, respectively. These error rates depend on the components of the quantum state (see, e.g., Ref. [4], Appendix]) and, thus, are a function of the initial fidelity F_0, the gate quality p_G, the maximal nesting level N, the distillation vector $\vec{k}$, and the distillation protocol. For a detailed analysis of the topic of quantum key distribution in connection to quantum repeaters, we refer to Ref. [30].

B. The repeater rate, including classical communication times

By the repeater rate R_{Rep}, we denote the average number of long-distance entangled pairs generated by the quantum repeater per second. Considering a setup, which connects only the neighboring pairs (so-called parallelization), several formulas for different physical realizations of a quantum repeater were derived: Ref. [39] treats the repeater rate for deterministic swapping and probabilistic distillation before the first swapping, Ref. [5] deduces the rate for probabilistic swapping without distillation, and in Ref. [30], the formula from the latter reference was modified to allow distillation before the first swapping. These expressions have in common that they do not consider the classical communication times needed to acknowledge the success of entanglement swapping and entanglement distillation. In the following, we will derive a repeater rate for probabilistic swapping and probabilistic distillation including these communication times. Our derivation is inspired by the recurrence formula developed for quantum repeaters based on nitrogen-vacancy

[2]When only swapping is performed, one can collect the outcomes of the Bell measurements and later can apply bit flips on the classical data resulting from the QKD measurement on the final state (see also Ref. [30]). For the case of distillation after swapping, the single-qubit rotations have to be applied, thus, the number of quantum operations is increased.

centers in diamond [40]. In Sec. V, we show how the secret key rate changes when we omit the classical communication times needed for entanglement swapping and entanglement distillation. We will always assume that the entanglement distribution requires classical communication.

1. The Deutsch et al. protocol

We define the repeater rate to be the reciprocal value of the time $\tau^{\mathrm{D}}(\vec{k},N)$ needed to establish an entangled pair over the distance L with N being the maximal nesting level and the distillation vector $\vec{k}^{\beta} = (k,0,\ldots,0)$, i.e.,

$$R^{\mathrm{D}}_{\mathrm{Rep}} := \frac{1}{T_0\tau^{\mathrm{D}}(\vec{k},N)}. \tag{6}$$

Here, the superscript D refers to the *Deutsch et al.* protocol. Note that the time $\tau^{\mathrm{D}}(\vec{k},N)$ is given in units of the fundamental time $T_0 := \frac{L_0}{c}$ with $c = 2\times 10^5$ km/s as the speed of light in the optical fiber and $L_0 := \frac{L}{2^N}$ as the fundamental length, i.e., the distance between the repeater stations. The symbol $\tau^{\mathrm{D}}(k_N,N)$, with only one vector component k_N as the first argument, denotes the time needed in nesting level N for k_N distillation rounds. In the following, we present a recurrence formula for $\tau^{\mathrm{D}}(k_N,N)$ given by

$$\tau^{\mathrm{D}}(k_0 = 0,N = 0) = \frac{2}{P_0}, \tag{7a}$$

$$\tau^{\mathrm{D}}(k_N = 0,N > 0) = \frac{1}{P_{\mathrm{ES}}(N)}\left[\frac{3}{2}\tau^{\mathrm{D}}(k_{N-1},N-1) + 2^{N-1}\right], \tag{7b}$$

$$\tau^{\mathrm{D}}(k_N > 0,N) = \frac{1}{P^{\mathrm{D}}_D(k_N,N)}\left[\frac{3}{2}\tau^{\mathrm{D}}(k_N - 1,N) + 2^{N}\right], \tag{7c}$$

with $P_{\mathrm{ES}}(N)$ being the success probability of entanglement swapping in the Nth nesting level and $P^{\mathrm{D}}_D(i,N)$ being the probability of success for entanglement distillation using the *Deutsch et al.* protocol in the ith distillation round in the Nth nesting level. Here, P_0 is the probability to generate an entangled photon pair over a distance L_0 and is given by $P_0 = 10^{-\alpha L_0/10}$ with $\alpha = 0.17$ dB/km being the attenuation coefficient. To explain the recurrence formula in Eq. (7), we start from the first line [Eq. (7a)]. There, we assume that the source is placed at one side and the photon is distributed over the distance L_0 leading to a distribution time of T_0. The acknowledgment of the arrival of the photons at least needs the same time, so we have, in total, $2T_0$ (see Ref. [30] for further details and other schemes of entanglement distribution). We divide by the probability P_0 to generate this entangled photon pair as, on average, we have to perform this process $\frac{1}{P_0}$ times (see, e.g., Ref. [5] for an explicit calculation of this waiting time). The next line [Eq. (7b)] gives the time for the Nth nesting level before starting with distillation, i.e., it is the time directly after entanglement swapping. The formula consists of two parts: the generation time for the pairs needed to begin the swapping $[\frac{3}{2}\tau^{\mathrm{D}}(k_{N-1},N-1)T_0]$ (see, e.g., Ref. [5], Appendix] for an explanation of the factor $\frac{3}{2}$) and the time to acknowledge the success of the swapping, i.e., $2^{N-1}T_0$; both divided by the probability of successful swapping in the Nth nesting level $\frac{1}{P_{\mathrm{ES}}(N)}$. Note that the factor $\frac{3}{2}$ is an approximation for small probabilities. The first part $[\frac{3}{2}\tau^{\mathrm{D}}(k_{N-1},N-1)T_0]$ corresponds to the average time to generate two pairs after k_{N-1} rounds of distillation in the $(N-1)$th nesting level. The last line [Eq. (7c)] concludes the recurrence formula: We need the time $\frac{3}{2}\tau^{\mathrm{D}}(k_N - 1,N)T_0$ to generate two pairs for the k_Nth round of distillation. As distillation is performed over distance $\frac{L}{2^N}$, the acknowledgment time is $2^N T_0$. Both terms are divided by the probability of success for entanglement distillation $[P^{\mathrm{D}}_D(k_N,N)]$.

We present the analytic solution of the recurrence formula in Eq. (7) in Appendix Eq. (A2).

2. The Dür et al. protocol

The repeater rate for the *Dür et al.* protocol differs from the repeater rate for the *Deutsch et al.* protocol as the entanglement distillation process works in a sequential way, i.e., the auxiliary pair for each distillation round is always the same (see Fig. 3). As the swapping process is the same in both distillation protocols, Eqs. (8a) and (8b) are analogous to Eqs. (7a) and (7b),

$$\tau^{\mathrm{Dür}}(k_0 = 0,N = 0) = \frac{2}{P_0}, \tag{8a}$$

$$\tau^{\mathrm{Dür}}(k_N = 0,N > 0) = \frac{1}{P_{\mathrm{ES}}(N)}\left[\frac{3}{2}\tau^{\mathrm{Dür}}(k_{N-1},N-1) + 2^{N-1}\right], \tag{8b}$$

$$\tau^{\mathrm{Dür}}(k_N > 0,N) = \frac{1}{P^{\mathrm{Dür}}_D(k_N,N)}[\tau^{\mathrm{Dür}}(k_N - 1,N) + \tau^{\mathrm{Dür}}(0,N) + 2^{N}]. \tag{8c}$$

The third line [Eq. (8c)] differs from Eq. (7c). Equation (8c) represents the time needed to distill a pair in the k_Nth round in the Nth nesting level. In the entanglement pumping protocol, we start to produce the elementary pair $\rho(k_N = 0,N)$ for distillation when the pair to be distilled $\rho(k_N - 1,N)$ is present. Thus, we have to add the time for generating the elementary pair $\tau^{\mathrm{Dür}}(0,N)T_0$ to the time for the pair to be distilled $\tau^{\mathrm{Dür}}(k_N - 1,N)T_0$. The repeater rate for the *Dür et al.* protocol is then given by

$$R^{\mathrm{Dür}}_{\mathrm{Rep}} := \frac{1}{T_0\tau^{\mathrm{Dür}}(\vec{k},N)}. \tag{9}$$

We give an analytic solution of the recurrence formula in Appendix Eq. (A3).

C. Number of memories

In this section, we describe the needed number of memories at each half of the repeater station (see the black dots in Fig. 1). The vector $\vec{k}$ consists of the number k_n of distillation rounds in the nth nesting level, see Eq. (3). The number of memories needed at half a node for the *Deutsch et al.* protocol is

$$M^{\mathrm{D}} = 2^{\sum_n k_n}, \tag{10}$$

because, in each nesting level, the number of memories needs to be increased by a factor of 2^{k_n} as the distillation for all

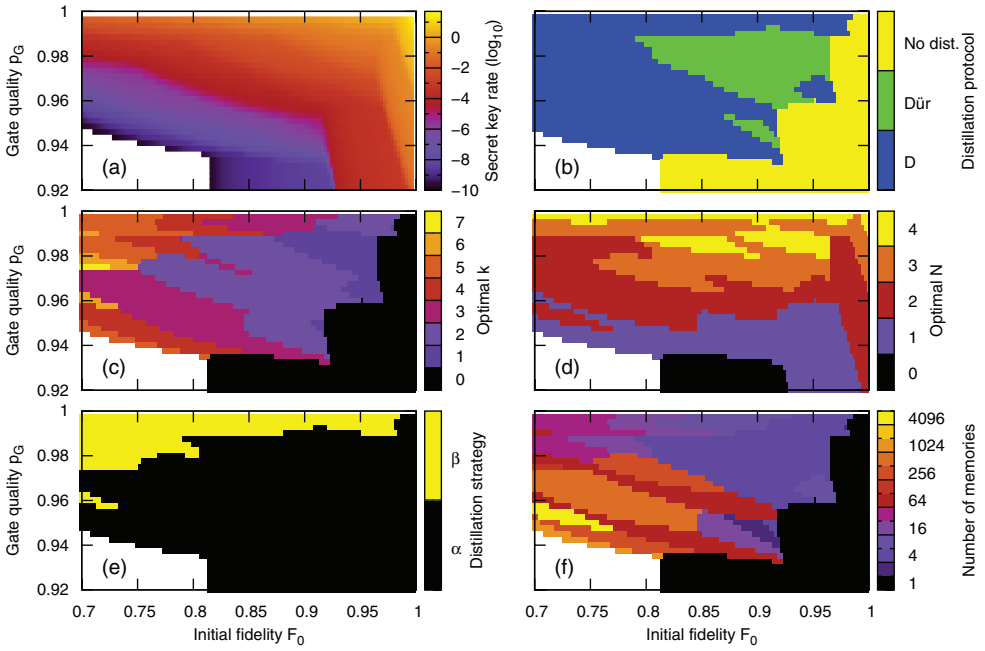


FIG. 5. (Color online) (a) Optimal secret key rate per memory per second (bits per second) [Eq. (4)] for the distance $L = 600$ km. The smallest secret key rate still depicted is chosen to be 10^{-10} secret bits per second per memory. In the white region, an extraction of a nonzero secret key rate is not possible. The parameters for the optimal secret key rate per memory per second are as follows: (b) Distillation protocols: *Deutsch et al.* protocol (blue, dark gray), *Dür et al.* protocol (green, medium gray), and no distillation (yellow, light gray). (c) Number of rounds of distillation k (for the optimal distillation strategy). (d) Number of nesting levels N. (e) Distillation strategies: strategy α (nested distillation) and strategy β (distillation only before the first entanglement swapping). (f) Number of used memories per repeater node.

nesting levels is performed in parallel. The superscript D denotes the *Deutsch et al.* protocol.

The *Dür et al.* protocol works in a sequential way, so the number of memories is

$$M^{\text{Dür}} = N + 2 - |\{k_i : k_i = 0\}|, \tag{11}$$

where the set $|\{k_i : k_i = 0\}|$ is the number of elements in $\vec{k}$ that are zero. Equation (11) for strategy α, i.e., $\vec{k} = (k, k, \ldots, k)$, can be explained as follows: For nesting level $N = 0$, at most two memories are needed for the distillation process (see Fig. 3). The resulting pair $\rho(k_0, N = 0)$ at distance L_0 after k_0 distillation rounds is stored in one memory, and the other one is emptied. After swapping two neighboring pairs, we have the pair $\rho(0, N = 1)$ at the distance $2L_0$. For starting the distillation process in this nesting level ($N = 1$), one needs another pair $\rho(0, N = 1)$, which is generated by the same procedure as above, so two additional memories are needed. In total, one needs three memories for $N = 1$. For strategy β, i.e., $\vec{k} = (k, 0, \ldots, 0)$, one just needs two memories where we store the state during the gate operation.

IV. OPTIMAL SECRET KEY RATES: COMPARING DIFFERENT DISTILLATION PROTOCOLS AND STRATEGIES

A. Comparison of key rates (strategy α vs β)

We investigate how the *Deutsch et al.* and the *Dür et al.* protocols perform under gate errors where we use the secret key rates as a figure of merit.

In the following, we calculate the secret key rate divided by the number of needed memories [see Eq. (4)]. The division by the number of memories allows for a fair comparison when considering the resources. For a fixed set of parameters F_0 (initial fidelity) and p_G (gate quality), we aim at finding the optimal distillation protocol, the optimal number of distillation rounds, the optimal number of nesting levels, the best distillation strategy, and the minimal number of memories. Note that, in the ideal case, i.e., for perfect detectors, we assume the entanglement swapping to be deterministic, i.e., $P_{\text{ES}}(N) = 1$.

We will consider two error models for the input states: on one hand, depolarized states and on the other hand, so-called binary states. The latter states are interesting as they can be produced by the hybrid quantum repeater [23,41]. Additionally, in Ref. [3], it was mentioned that the binary state given in Eq. (13) below has the optimal shape for the *Dür et al.* protocol.

1. Input states: Depolarized states

In this section, we want to investigate the optimal secret key rates [Eq. (4)] when we start with depolarized states, i.e.,

$$\rho_{\text{Dep}} = F\Pi_{|\phi^+\rangle} + \frac{1-F}{3}(\Pi_{|\phi^-\rangle} + \Pi_{|\psi^+\rangle} + \Pi_{|\psi^-\rangle}). \tag{12}$$

Optimization of the distillation protocols (*Deutsch et al.* or *Dür et al.*), the number of nesting levels N, the number of distillation rounds k, and the distillation strategy (α or β), lead to the secret key rates depicted in Fig. 5(a). We point out that we find the global maximum as we calculate K^i for all possible

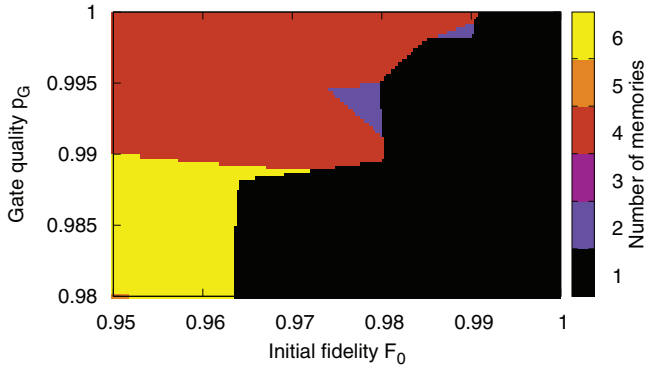


FIG. 6. (Color online) Expanded region from Fig. 5(f): Number of memories that lead to the optimal secret key rate per second per memory [see Eq. (4), $L = 600$ km].

combinations of parameters for the length L and then choose the maximal value. The parameters leading to the optimal secret key rates of Fig. 5(a) are shown in Figs. 5(b)–5(f). The optimal distillation protocol is shown in Fig. 5(b). It is difficult to find an intuitive explanation why, in certain regimes, either the *Deutsch et al.* or the *Dür et al.* protocol is optimal; there are many different effects, such as the repeater rates [see Eqs. (7) and (8)], the number of memories, and the resulting state. Figure 5(c) shows the optimal number of distillation rounds (for the optimal distillation strategy) that lead to the secret key rate per memory per second of Fig. 5(a). We find that, for a wide range of parameters, it is enough to have $k \leqslant 3$ distillation rounds. The role of the optimal number of nesting levels is treated in Fig. 5(d). We find that, with increasing gate quality and initial fidelity, more nesting levels are optimal. In Fig. 5(e), the optimal of the two distillation strategies (α) or (β) is shown: For good gates and low fidelities, it is better to only distill in the beginning, which would be experimentally less demanding. We emphasize that, in this regime of parameters, distillation in later nesting levels degrades the secret key rate. From the previous plots, in Fig. 5(f), we calculate the minimal number of memories needed to obtain the secret key rate in Fig. 5(a).

Figure 6 provides a zoom of Fig. 5(f) into the region where the secret key rate is on the order of bits per second. In the black region, no distillation is optimal, therefore, we only need one memory. For the number of memories $M = 2$ and $M = 4$, the optimal protocol is the *Deutsch et al.* protocol, whereas, for $M = 6$, the *Dür et al.* protocol becomes favorable. From Eq. (10), we see that, in a single setup, the number of memories is restricted to a power of 2 for the *Deutsch et al.* protocol. If we want to use, e.g., $M = 6$ memories and the *Deutsch et al.* protocol, we have to employ setups in parallel. We will treat this subject in Sec. IV C2.

2. *Input states: Binary states*

We will now consider binary states, i.e., states of the form

$$\rho_{\mathrm{Bin}} = F|\phi^+\rangle\langle\phi^+| + (1-F)|\phi^-\rangle\langle\phi^-|. \tag{13}$$

We performed a complete analysis of this case, in analogy to Sec. IV A1. The results of our investigation can be summarized as follows:

(1) Different from the setup where we start with depolarized states, it is possible to extract a nonzero secret key rate per memory per second for the whole range of parameters considered here, i.e., for $0.7 \leqslant F_0 \leqslant 1$ and $0.92 \leqslant p_G \leqslant 1$. The largest value of the secret key rate per memory per second using binary states is on the same order of magnitude as for depolarized states.

(2) The region where the *Dür et al.* protocol is optimal extends to lower initial fidelities, compared to Fig. 5(b), and the largest value for the optimal rounds of distillation is $k = 3$. Also, the region where no distillation is optimal increases.

(3) Due to the small optimal k, the maximal number of memories decreases.

One would recommend the use of binary states when $p_G \leqslant 0.97$ and $F_0 \leqslant 0.8$ as then, the number of used memories is smaller than for depolarized states and the secret key rate per memory per second is nonzero.

B. The influence of the detector efficiency

In this section, we want to investigate the impact of finite-efficiency detectors on the secret key rate. The detector efficiency is given by the parameter η_d with $0 \leqslant \eta_d \leqslant 1$ where $\eta_d = 1$ corresponds to perfect detectors. For implementing the detector efficiency in our formulas, we have to replace the probability of successful distillation $P_D(k,n)$ and the probability of successful swapping in the nth nesting level $P_{\mathrm{ES}}(n)$ in the equations for the repeater rate [Eqs. (6) and (9)] by

$$P_D(k,n) \to \eta_d^2 P_D(k,n) \tag{14a}$$

$$P_{\mathrm{ES}}(n) \to \eta_d^2 P_{\mathrm{ES}}(n), \tag{14b}$$

because the Bell measurement requires a twofold detector click. Additionally, we have to multiply the secret key rate [Eq. (4)] by a factor of η_d^2, which accounts for the final quantum key distribution measurement.

The only contribution of the detector efficiency in the secret key rate is in the repeater rate. For simplicity, we will consider the repeater rate without classical communication for entanglement swapping and entanglement distillation [see Eqs. (17) and (18) in Sec. V]. After replacing the probabilities in the repeater rates by Eq. (14), the repeater rate scales with $\eta_d^{2(N+\sum_n k_n)}$.

When analyzing different detector efficiencies, we made the following observations:

(1) With decreasing η_d, the region where no distillation is optimal increases such that, for $\eta_d = 0.1$, it is optimal to not perform distillation for almost all parameters,

(2) with decreasing η_d, the optimal number of nesting levels also decreases,

(3) with decreasing η_d, the region where the distillation strategy β (distillation only in the beginning) is optimal increases (see Fig. 7).

Figure 7 shows the optimal distillation strategies for the secret key rate per memory per second with a detector efficiency of $\eta_d = 0.9$. This can be compared to Fig. 5(e) where the detectors are perfect, i.e., $\eta_d = 1$. We see that, for low initial fidelities, the region where the distillation strategy β is optimal increases.

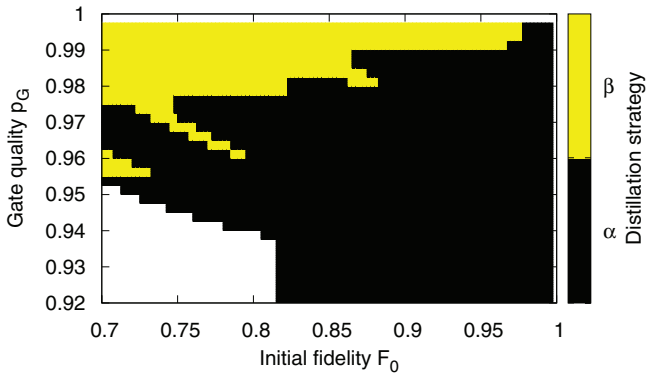


FIG. 7. (Color online) Distillation strategies with imperfect detectors: strategy α (nested distillation strategy) and strategy β (distillation only before the first entanglement swapping) that lead to the optimal secret key rate per memory per second [Eq. (4), $L = 600$ km and $\eta_d = 0.9$].

C. More general strategies

1. Distillation strategy γ

As mentioned in Sec. II B, we now lift the restriction that the number of distillation rounds in each nesting level is the same. For this purpose, we fix the parameters for the initial fidelity F_0 and the gate quality p_G and vary the number of nesting levels and the number of distillation rounds in each nesting level. A result for the parameters $F_0 = 0.9$ and $p_G = 0.96$ is shown in Table I. There, we report the optimal distillation vector $\vec{k}$, see Eq. (3), for the number of nesting levels up to $N = 4$ and the corresponding secret key rate per memory per second. We found the optimal $\vec{k}$ by calculating the key rate for all possible $\vec{k}$'s. For the given parameters, distillation only in the beginning does not help. Comparing the values that we achieved in Sec. IV A, i.e., only considering strategy α [distillation vector $\vec{k} = (k,k,\ldots,k)$] or β [$\vec{k} = (k,0,\ldots,0)$], the optimal secret key rate for the given set of parameters was 0.99×10^{-4} with $N = 2$, $\vec{k} = (2,2,2)$ for the *Dür et al.* protocol. Here, the best secret key rate is 3.03×10^{-4} for $N = 2$, $\vec{k} = (0,3,1)$ and the *Deutsch et al.* protocol. Thus, the secret key rate is on the same of order of magnitude but can be improved by a factor of 3.

Table II gives results for the parameters $F_0 = 0.97$ and $p_G = 0.99$. The parameters that lead to the optimal secret key rate per memory per second of $K = 0.32$ in Sec. IV A are for the nesting level $N = 3$, distillation strategy β, and

TABLE I. Optimal secret key rate per memory per second [Eq. (4)] and corresponding distillation vector $\vec{k}$ [Eq. (3)] for the different distillation protocols $F_0 = 0.9$ and $p_G = 0.96$.

	Dür et al. protocol		*Deutsch et al.* protocol	
N	K	$\vec{k}$	K	$\vec{k}$
0	3.92×10^{-9}	(0)	3.92×10^{-9}	(0)
1	2.11×10^{-5}	(0,2)	2.63×10^{-5}	(0,1)
2	1.09×10^{-4}	(2,3,2)	3.03×10^{-4}	(0,3,1)
3	2.66×10^{-6}	(3,4,5,5)	1.51×10^{-4}	(0,3,3,1)
4	0	0	1.37×10^{-5}	(0,3,3,3,1)

TABLE II. Optimal secret key rate per memory per second [Eq. (4)] and corresponding distillation vector $\vec{k}$ [Eq. (3)] for the different distillation protocols $F_0 = 0.97$ and $p_G = 0.99$.

	Dür et al. protocol		*Deutsch et al.* protocol	
N	K	$\vec{k}$	K	$\vec{k}$
0	7.97×10^{-9}	(0)	7.97×10^{-9}	(0)
1	9.64×10^{-4}	(0,0)	9.64×10^{-4}	(0,0)
2	0.19	(0,0,0)	0.19	(0,0,0)
3	0.57	(0,0,2,0)	0.73	(0,2,0,0)
4	0.96	(0,1,1,1,0)	0.88	(0,1,1,1,0)
5	0.62	(0,1,1,2,0,0)	0.54	(0,0,2,1,0,0)
6	0.34	(0,1,1,1,1,1,0)	0.2	(0,1,1,1,1,1,0)

$\vec{k} = (2,0,0,0)$ using the *Deutsch et al.* protocol. In this example, we see that, by allowing general distillation strategies, the optimal secret key rate can be increased by increasing the nesting level. In this example, different from above, the *Dür et al.* protocol remains optimal.

Due to the computational complexity, we only calculated the general distillation strategies for two specific set of parameters (see Tables I and II). As the quantum repeater exhibits a self-similar structure, dynamical programming was used in Ref. [42] in order to optimize the average time to create an entangled pair for a given final fidelity and distance. The results and methods of Ref. [42] cannot be used for a global optimization as we have found counterexamples where the distillation vector consists of different numbers in each nesting level (see, e.g., Table I for the *Dür et al.* protocol and Table II).

We see that it is not trivial to make general statements about the optimal number of rounds of distillation, regarding the secret key rate. For implementations, one has to determine the parameters of the experiment, i.e., F_0 and p_G, and then to optimize the secret key rate for any specific set of parameters.

2. Optimal strategies for a fixed number of memories allowing parallel setups

In Sec. III C, we have mentioned that, in the following, we want to fix the number of memories and find which setup is optimal. As the memories in the *Deutsch et al.* protocol are restricted to a power of 2 (see Sec. III C), we also allow setups working in parallel.

For calculating the optimal strategy for a fixed number of memories M, we solve the following equation to get all possible setups:

$$\sum_{m=1}^{M} s_m m = M \tag{15}$$

for $s_m \in \mathbb{N}$ and $\lfloor \frac{M}{m} \rfloor \geqslant s_m \geqslant 0$. The number s_m denotes how many setups using m memories work in parallel. For each setup, we then proceed by calculating the optimal secret key rate per second, i.e., $mK_m = r_\infty R_{\mathrm{Rep}}$. The index m for the secret key rate K means that we restrict to distillation vectors and nesting levels that solve Eqs. (10) and (11) for m memories. The optimal vector $\vec{s} = (s_1,\ldots,s_M)$, a solution of Eq. (15), is found by maximizing the value $\sum_m s_m m K_m$. The secret key

TABLE III. Secret key rate per total number of used memories [Eq. (16)] for the different distillation protocols and for a fixed number of memories M. The optimal configurations are given by the distillation vectors $\vec{k}_M = (k_0, \ldots, k_N)$ with $\vec{k}_M$ denoting the distillation strategy using M memories. The notation $(\vec{k}_m, \vec{k}_{m'})$ means parallel setups using m and m' memories. Parameters: $F_0 = 0.97$ and $p_G = 0.99$.

	Dür et al. protocol		*Deutsch et al.* protocol	
M	K	Configuration	K	Configuration
1	0.19	$\vec{k}_1 = (0,0,0)$	0.19	$\vec{k}_1 = (0,0,0)$
2	0.58	$\vec{k}_2 = (0,0,2,0)$	0.58	$\vec{k}_2 = (0,0,1,0)$
3	0.96	$\vec{k}_3 = (0,1,2,0,0)$	0.45	$(\vec{k}_1, \vec{k}_2)$
4	0.82	$\vec{k}_4 = (0,1,1,1,0)$	0.87	$\vec{k}_4 = (0,0,2,0,0)$
5	0.81	$(\vec{k}_2, \vec{k}_3)$	0.73	$(\vec{k}_1, \vec{k}_4)$
6	0.96	$(\vec{k}_3, \vec{k}_3)$	0.78	$(\vec{k}_2, \vec{k}_4)$
7	0.89	$(\vec{k}_3, \vec{k}_4)$	0.69	$(\vec{k}_1, \vec{k}_2, \vec{k}_4)$

rate of the total setup with a fixed number of memories M is, thus, given by

$$K = \frac{\sum_m s_m m K_m}{M}, \tag{16}$$

with $\sum_m s_m m = M$. We will also compare this result to a configuration of one setup with distillation vector $\vec{k}$ [see Eq. (3)], if possible. For the parameters $F_0 = 0.97$ and $p_G = 0.99$, we calculated the optimal $\vec{s}$ to see if a parallel setup was advantageous. In Sec. IV A, we showed that the optimal number of memories is 4 using the *Deutsch et al.* protocol for $N = 3$, $\vec{k} = (2,0,0,0)$ with a secret key rate per memory per second of $K = 0.32$. In Table III, we fixed the number of memories and calculated the optimal key rate by optimizing the remaining parameters. We find that, except for $M = 4$, the secret key rate per memory per second is higher (or equal) for the *Dür et al.* protocol.

V. IMPACT OF CLASSICAL COMMUNICATION ON THE SECRET KEY RATE

In this section, we investigate the impact of the classical communication time required for acknowledging the success of entanglement swapping and entanglement distillation on the secret key rate. First, we calculate the repeater rates $R_{\mathrm{Rep,NC}}$ where we only consider the classical communication for entanglement distribution. Then, we compare the optimal secret key rates using the repeater rate without ($R_{\mathrm{Rep,NC}}$) and with classical communication (R_{Rep}) [see Eqs. (6) and (9)] and discuss the differences.

The repeater rate for the *Deutsch et al.* protocol, without the classical communication time due to entanglement swapping and entanglement distillation, is given by (see, e.g., Refs. [5,30])

$$R^{\mathrm{D}}_{\mathrm{Rep,NC}} = \frac{1}{2T_0}\left(\frac{2}{3}\right)^{N+\sum_n k_n} P_0 \prod_{n=1}^{N} P_{\mathrm{ES}}(n) \prod_{i=0}^{k_n} P_D^{\mathrm{D}}(i,n), \tag{17}$$

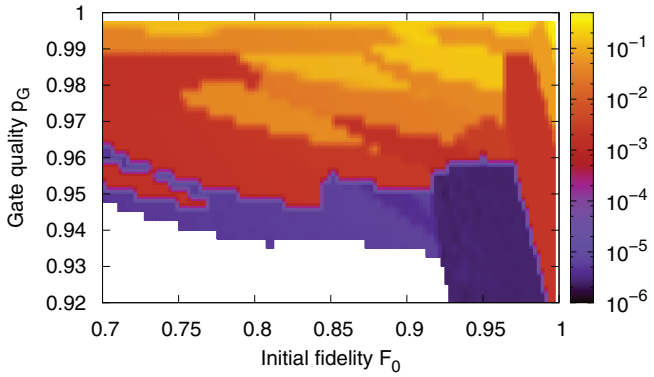


FIG. 8. (Color online) The relative change [Eq. (20)] in the optimal secret key rate per memory per second [Eq. (4)] without and with the classical communication time (see text) in terms of the initial fidelity F_0 and gate quality p_G ($L = 600$ km).

which is derived from the solution of the recurrence relation in Eq. (7) by omitting all terms acknowledging the classical communication time, i.e., the terms with 2^{N-1} and 2^N [see Appendix Eq. (A2)].

The corresponding repeater rate for the *Dür et al.* protocol can be derived analogously by omitting terms in the recurrence relation given in Eq. (8). This leads to

$$R^{\mathrm{Dür}}_{\mathrm{Rep,NC}} = \frac{P_0}{2T_0}\left(\frac{2}{3}\right)^N \prod_{i=0}^{N} \frac{P_{\mathrm{ES}}(i)}{a(i)}, \tag{18}$$

where

$$a(i) = \prod_{j=0}^{k_i-1} P_D^{\mathrm{Dür}}(k_i - j, i)^{-1} + \sum_{m=0}^{k_i-1} \prod_{j=0}^{m} P_D^{\mathrm{Dür}}(k_i - j, i)^{-1}, \tag{19}$$

and $P_{\mathrm{ES}}(0) = 1$ (see Appendix A 2b for details).

For investigating the relevance of the classical communication time, we determine the *relative change* in the optimal secret key rates with this classical communication $K(R_{\mathrm{Rep}})$ and without classical communication $K(R_{\mathrm{Rep,NC}})$, i.e.,

$$\Delta_{\mathrm{rel}}(K(R_{\mathrm{Rep,NC}}), K(R_{\mathrm{Rep}})), \tag{20}$$

with K being the optimal secret key rate per memory per second [Eq. (4)]. The relative change Δ_{rel} is defined by

$$\Delta_{\mathrm{rel}}(a,b) := (a-b)/\max\{a,b\}. \tag{21}$$

We optimize both secret key rates over the same parameter set as in Sec. IV.

Figure 8 shows the relative change in the optimal secret key rate per second per memory. Depending on the parameters, the secret key rate, without the classical communication time $K(R_{\mathrm{Rep,NC}})$, can be bigger by a factor of 2. This is the yellow region in Fig. 8. By inspecting Fig. 5(a), the secret key rate in this region is on the order of secret bits per second. Except for some regions, the parameters leading to the optimal secret key rate without and with the classical communication time are almost the same.

In a previous paper [3], it was claimed that the main contribution of the entanglement generation time (i.e., the

inverse of the repeater rate) is the classical communication time needed for acknowledging the success of entanglement swapping and entanglement distillation. Here, we have seen that this is not the case. Comparing the results given in Ref. [3], we have found that the relative change [Eq. (20)] is not more than 40% and both secret key rates are on the same order of magnitude (distance $L = 1280$ km). We discovered that the influence of nonperfect success probabilities for distillation is substantial. Here, the entanglement generation time is 1 order of magnitude larger than in Ref. [3] where the success probability of entanglement distillation was not considered (parameters: $F_0 = 0.96$ and $p_G = 0.995$).

Note that, here, we consider the memories to be perfect. Certainly, if the storage time of the memories is limited, such an analysis might lead to other results.

VI. CONCLUSION

For given imperfect initial fidelities and imperfect gates, we found the quantum repeater configurations (i.e., the distillation protocol, distillation strategy, number of distillation rounds, number of nesting levels, and number of memories) that lead to the optimal secret key rate per memory per second. For this purpose, we focused on a specific recurrence protocol (*Deutsch et al.*) and an entanglement pumping protocol (*Dür et al.*). We found that there exists a regime ($p_G \leqslant 0.99$ and $F_0 \geqslant 0.8$) of parameters where the entanglement pumping protocol performs best. However, for lower initial fidelities, typically, the recurrence protocol is favorable.

Regarding the distillation strategy [distilling with the same number of rounds in each nesting level (strategy α) or distilling only in the beginning (strategy β)], we have seen that, for some parameters, strategy β, which is experimentally more feasible, is optimal and that this region strongly depends on the detector efficiency. We found that, with decreasing detector efficiency, it is optimal to not distill. Lifting the restriction of an equal number of distillation rounds in each nesting level for some set of parameters (initial fidelity and gate quality), we have found that the improvement of the secret rate is not more than 1 order of magnitude compared to distillation strategy α. We also showed that increasing the number of repeater stations and rounds of distillation does not necessarily lead to an increase in the secret key rate.

We investigated the role of the form of the input states where we used either a depolarized or a binary state. We found that the secret key rate per memory per second for both forms is in the same order of magnitude; the binary states have the advantage that, for low fidelities and gate qualities, they provide a nonzero secret key rate compared to a depolarized input state. Binary states can be produced by the hybrid quantum repeater.

When fixing the number of memories for a specific set of parameters, we investigated which distillation protocol is optimal and found that setups working in parallel can be advantageous.

Finally, we derived formulas for the generation rate of entangled pairs per second (*repeater rate*) including the classical communication times for acknowledging the success of entanglement swapping and entanglement distillation. We calculated the secret key rate per memory per second without and with the classical communication time and found that the main contribution is the time to distribute the entangled pairs, which is contrary to the results in the literature.

Further studies could implement the formalism for the quantum repeater in the context of finite keys (see, e.g., Ref. [4] for a review) and for imperfect memories (see, e.g., Ref. [43]).

ACKNOWLEDGMENTS

The authors acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, Project QuOReP).

APPENDIX: SOLUTIONS FOR THE RECURRENCE FORMULAS

In this appendix, we give the solutions for the recurrence formulas [Eqs. (7) and (8) in Sec. III B] that are needed for calculating the repeater rate for the *Deutsch et al.* and the *Dür et al.* protocols.

1. The *Deutsch et al.* protocol

We first solve the recurrence relation for Eq. (7c) and terminate when $k_N = 0$,

$$\tau^{\mathrm{D}}(k_N,N) = \tau^{\mathrm{D}}(0,N)\underbrace{\left(\frac{3}{2}\right)^{k_N}\prod_{j=0}^{k_N-1}\frac{1}{P_D^{\mathrm{D}}(k_N-j,N)}}_{=:\alpha(N)} + \underbrace{2^N\sum_{i=0}^{k_N-1}\left(\frac{3}{2}\right)^{i}\prod_{j=0}^{i}\frac{1}{P_D^{\mathrm{D}}(k_N-j,N)}}_{=:\beta(N)}. \quad \text{(A1)}$$

Then, we replace $\tau^{\mathrm{D}}(0,N)$ by Eq. (7b), resulting in

$$\tau^{\mathrm{D}}(k_N,N) = \frac{\alpha(N)}{P_{\mathrm{ES}}(N)}\left(\frac{3}{2}\tau^{\mathrm{D}}(k_{N-1},N-1)+2^{N-1}\right)+\beta(N),$$

which is another recurrence relation depending on N. We can now solve this relation until we reach $\tau^{\mathrm{D}}(k_0,0)$,

$$\begin{aligned}\tau^{\mathrm{D}}(k_N,N) = {}& \tau^{\mathrm{D}}(k_0,0)\left(\frac{3}{2}\right)^{N}\prod_{j=0}^{N-1}\frac{\alpha(N-j)}{P_{\mathrm{ES}}(N-j)} \\ & + \sum_{i=1}^{N}\left(\frac{3}{2}\right)^{N-i}2^{i-1}\prod_{j=0}^{N-i}\frac{\alpha(N-j)}{P_{\mathrm{ES}}(N-j)} \\ & + \sum_{i=1}^{N}\left(\frac{3}{2}\right)^{N-i}\beta(i)\prod_{j=0}^{N-(i+1)}\frac{\alpha(N-j)}{P_{\mathrm{ES}}(N-j)}, \end{aligned} \quad \text{(A2)}$$

where we can replace $\tau^{\mathrm{D}}(k_0,0)$ by $\tau^{\mathrm{D}}(0,0)\alpha(0)+\beta(0)$ using Eq. (A1).

2. The *Dür et al.* protocol

a. Solution of the recurrence relation Eq. (8)

The solution of the recurrence relation in Eq. (8) is analogously given by

$$\tau^{\mathrm{Dür}}(k_N,N)=\tau^{\mathrm{Dür}}(0,N)\underbrace{\left(\prod_{j=0}^{k_N-1}P_D^{\mathrm{Dür}}(k_N-j,N)^{-1}+\sum_{i=0}^{k_N-1}\prod_{j=0}^{i}P_D^{\mathrm{Dür}}(k_N-j,N)^{-1}\right)}_{=:a(N)}+2^N\underbrace{\left(\sum_{i=0}^{k_N-1}\prod_{j=0}^{i}P_D^{\mathrm{Dür}}(k_N-j,N)^{-1}\right)}_{=:b(N)}, \tag{A3}$$

where we use the convention that $\sum_{i=0}^{-1}f(i)=0$ and $\prod_{i=0}^{-1}c(i)=1$. Now, inserting $\tau^{\mathrm{Dür}}(0,N)=\frac{3}{2}\tau^{\mathrm{Dür}}(k_{N-1},N-1)+2^{N-1}$ into $\tau^{\mathrm{Dür}}(k_N,N)=\tau^{\mathrm{Dür}}(0,N)a(N)+b(N)$ leads to the recurrence relation,

$$\tau^{\mathrm{Dür}}(k_N,N)=\frac{a(N)}{P_{\mathrm{ES}}(N)}\left(\frac{3}{2}\tau^{\mathrm{Dür}}(k_{N-1},N-1)+2^{N-1}\right)+b(N). \tag{A4}$$

The solution of this relation is

$$\begin{aligned}\tau^{\mathrm{Dür}}(k_N,N)=\tau(k_0,0)\left(\frac{3}{2}\right)^N\prod_{j=0}^{N-1}\frac{a(N-j)}{P_{\mathrm{ES}}(N-j)}\\+\sum_{i=1}^{N}\left(\frac{3}{2}\right)^{N-i}2^{i-1}\prod_{j=0}^{N-i}\frac{a(N-j)}{P_{\mathrm{ES}}(N-j)}\\+\sum_{i=1}^{N}\left(\frac{3}{2}\right)^{N-i}b(i)\prod_{j=0}^{N-(i+1)}\frac{a(N-j)}{P_{\mathrm{ES}}(N-j)}.\end{aligned} \tag{A5}$$

We get the solution for $\tau^{\mathrm{Dür}}(k_0,0)$ from Eq. (A3),

$$\tau^{\mathrm{Dür}}(k_0,0)=\tau^{\mathrm{Dür}}(0,0)a(0)+b(0). \tag{A6}$$

b. Derivation of the repeater rate without the classical communication time for entanglement distillation and entanglement swapping, Eq. (18)

For obtaining the solution for the recurrence relations without classical communication time for entanglement distillation and entanglement swapping, in Eq. (A3) we just set $b(N)=0$. What remains from the solution is just the first term of Eq. (A5), which is exactly

$$\tau_{\mathrm{NC}}^{\mathrm{Dür}}(k_N,N)=\tau_{\mathrm{NC}}^{\mathrm{Dür}}(k_0,0)\left(\frac{3}{2}\right)^N\prod_{j=0}^{N-1}\frac{a(N-j)}{P_{\mathrm{ES}}(N-j)}. \tag{A7}$$

We replace $\tau_{\mathrm{NC}}^{\mathrm{Dür}}(k_0,0)$ by $\tau^{\mathrm{Dür}}(0,0)a(0)$ [see Eq. (A6)] and get

$$\tau_{\mathrm{NC}}^{\mathrm{Dür}}(k_N,N)=\tau^{\mathrm{Dür}}(0,0)\left(\frac{3}{2}\right)^N\prod_{j=0}^{N}\frac{a(N-j)}{P_{\mathrm{ES}}(N-j)}. \tag{A8}$$

The repeater rate is given by

$$\begin{aligned}R_{\mathrm{Rep,NC}}^{\mathrm{Dür}}&=\frac{1}{T_0\tau_{\mathrm{NC}}^{\mathrm{Dür}}(k_N,N)}\\&=\frac{P_0}{2T_0}\left(\frac{2}{3}\right)^N\prod_{i=0}^{N}\frac{P_{\mathrm{ES}}(i)}{a(i)},\end{aligned} \tag{A9}$$

where we used the fact that $\tau^{\mathrm{Dür}}(0,0)=\frac{2}{P_0}$.

[1] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[2] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[3] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[5] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

[6] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[8] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[9] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[11] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).

[12] J. B. Brask, I. Rigas, E. S. Polzik, U. L. Andersen, and A. S. Sørensen, Phys. Rev. Lett. **105**, 160501 (2010).

[13] D. Aghamalyan and Y. Malakyan, Phys. Rev. A **84**, 042305 (2011).

[14] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).

[15] U. W. E. Dorner, A. Klein, and D. Jaksch, Quantum Inf. Comput. **8**, 0468 (2008).
[16] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).
[17] L. Jiang, J. M. Taylor, and M. D. Lukin, Phys. Rev. A **76**, 012301 (2007).
[18] J. Minář, H. de Riedmatten, and N. Sangouard, Phys. Rev. A **85**, 032313 (2012).
[19] W. J. Munro, R. Van Meter, S. G. R. Louis, and K. Nemoto, Phys. Rev. Lett. **101**, 040502 (2008).
[20] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, Phys. Rev. A **76**, 050301 (2007).
[21] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. de Riedmatten, J.-W. Pan, and N. Gisin, Phys. Rev. A **77**, 062301 (2008).
[22] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **98**, 190503 (2007).
[23] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).
[24] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).
[25] B. Zhao, M. Müller, K. Hammerer, and P. Zoller, Phys. Rev. A **81**, 052329 (2010).
[26] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[27] A. Scherer, B. C. Sanders, and W. Tittel, Opt. Express **19**, 3004 (2011).
[28] J. Amirloo, M. Razavi, and A. Hamed Majedi, Phys. Rev. A **82**, 032304 (2010).
[29] N. Lo Piparo and M. Razavi, arXiv:1210.8042.
[30] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).
[31] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).
[32] R. van Meter, T. Ladd, W. Munro, and K. Nemoto, IEEE/ACM Trans. Netw. **17**, 1002 (2009).
[33] W. Dür, Ph.D thesis, University of Innsbruck, 1998.
[34] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[35] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[36] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), Vol. 175.
[37] H. K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[38] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).
[39] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).
[40] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. A **72**, 052330 (2005).
[41] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. **8**, 184 (2006).
[42] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, Proc. Natl. Acad. Sci. USA **104**, 17291 (2007).
[43] L. Hartmann, B. Kraus, H. J. Briegel, and W. Dür, Phys. Rev. A **75**, 032310 (2007).

"Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate."
Bratzik, S., Abruzzo, S., Kampermann, H. und Bruß, D.
Physical Review A **87**, 062335, 2013.

Journal: Physical Review A
Impact factor: 3,042
Anteil an der Arbeit: 90%, 1. Autor, Schreiben des Manuskriptes und Ausführung der Rechnungen

Quantum repeaters and quantum key distribution: Analysis of secret-key rates

Silvestre Abruzzo,[1,*] Sylvia Bratzik,[1] Nadja K. Bernardes,[2,3] Hermann Kampermann,[1] Peter van Loock,[2,3,4] and Dagmar Bruß[1]

[1]*Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstrasse 1, 40225 Düsseldorf, Germany*

[2]*Optical Quantum Information Theory Group, Max Planck Institute for the Science of Light, Günther-Scharowsky-Strasse 1/Bau 24, 91058 Erlangen, Germany*

[3]*Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Staudtstrasse 7/B2, 91058 Erlangen, Germany*

[4]*Institute of Physics, Johannes-Gutenberg Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany*

(Received 20 November 2012; published 17 May 2013)

We analyze various prominent quantum repeater protocols in the context of long-distance quantum key distribution. These protocols are the original quantum repeater proposal by Briegel, Dür, Cirac and Zoller, the so-called hybrid quantum repeater using optical coherent states dispersively interacting with atomic spin qubits, and the Duan-Lukin-Cirac-Zoller-type repeater using atomic ensembles together with linear optics and, in its most recent extension, heralded qubit amplifiers. For our analysis, we investigate the most important experimental parameters of every repeater component and find their minimally required values for obtaining a nonzero secret key. Additionally, we examine in detail the impact of device imperfections on the final secret key rate and on the optimal number of rounds of distillation when the entangled states are purified right after their initial distribution.

DOI: 10.1103/PhysRevA.87.052315 PACS number(s): 03.67.Hk, 03.67.Dd

I. INTRODUCTION

Quantum communication is one of the most exciting and well developed areas of quantum information. Quantum key distribution (QKD) is a subfield, where two parties, usually called Alice and Bob, want to establish a secret key. For this purpose, typically, they perform some quantum operations on two-level systems, the qubits, which, for instance, can be realized by using polarized photons [1–5].

Photons naturally have a long decoherence time and hence could be transmitted over long distances. Nevertheless, recent experiments show that QKD so far is limited to about 150 km [6], due to losses in the optical-fiber channel. Hence, the concept of quantum relays and repeaters was developed [7–11]. These aim at entangling qubits over long distances by means of entanglement swapping and entanglement distillation. There exist various proposals for an experimental implementation, such as those based upon atomic ensembles and single-rail entanglement [12], the hybrid quantum repeater [13], the ion-trap quantum repeater [14], repeaters based on deterministic Rydberg gates [15,16], and repeaters based on nitrogen-vacancy (NV) centers in diamond [17].

In this paper, we analyze the performance of quantum repeaters within a QKD setup for calculating secret key rates as a function of the relevant experimental parameters. Previous investigations on long-distance QKD either consider quantum relays [9,11,18], which only employ entanglement swapping without using quantum memories or entanglement distillation, or, like the works in [19,20], they exclusively refer to the original Duan-Lukin-Cirac-Zoller (DLCZ) quantum repeater [12]. Finally, in [21] the authors analyze a variation of the DLCZ protocol [22] where they consider, at most, one repeater station. Here, our aim is to quantify the influence of characteristic experimental parameters on the secret key rate for three different repeater schemes, namely the original quantum repeater protocol [7], the hybrid quantum repeater [13], and a recent variation of the DLCZ repeater [23]. We investigate the minimally required parameters that allow a nonzero secret key rate. In order to reduce the complexity of the full repeater protocol, we consider entanglement distillation only directly after the initial entanglement distribution. Within this scenario, we investigate also the optimal number of distillation rounds for a wide range of parameters. The influence of distillation during later stages of the repeater, as well as the comparison between different distillation protocols, will be studied elsewhere [24].

This paper is organized as follows. In Sec. II we present a description of the relevant parameters of a quantum repeater, as well as the main tools for analyzing its performance for QKD. This section should also provide a general framework for analyzing other existing quantum repeater protocols and for studying the performance and the potential of new protocols. Sections III, IV, and V investigate long-distance QKD protocols for three different quantum repeater schemes; these sections can be read independently. Section III is devoted to the original proposal for a quantum repeater [7], Sec. IV analyzes the hybrid quantum repeater [13], and finally, in Sec. V, we investigate quantum repeaters with atomic ensembles [12]. The conclusion is given in Sec. VI, and more details on the calculations are presented in the Appendixes.

II. GENERAL FRAMEWORK

A. Quantum repeater

The purpose of this section is to provide a general framework that describes formally the theoretical analysis of a quantum repeater.

1. The protocol

Let L be the distance between the two parties Alice and Bob who wish to share an entangled state. A quantum repeater [7] consists of a chain of 2^N segments of fundamental length $L_0 := L/2^N$ and $2^N - 1$ repeater stations which are placed at the intersection points between two segments (see Fig. 1).

*abruzzo@thphy.uni-duesseldorf.de

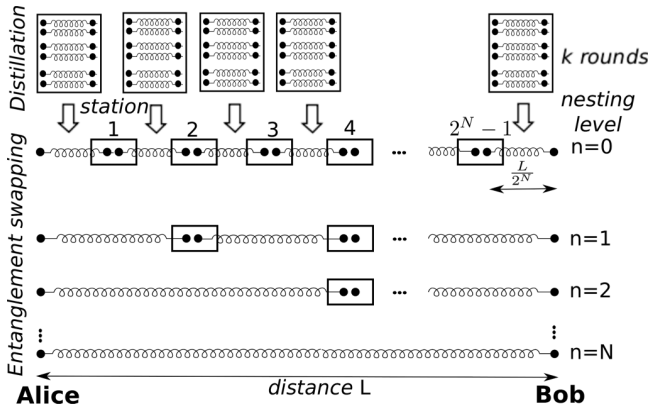


FIG. 1. Scheme of a generic quantum repeater protocol. We adopt the nested protocol proposed in [7]. The distance between Alice and Bob is L, which is divided into 2^N segments, each having the length $L_0 := L/2^N$. The parameter n describes the different nesting levels, and the value N represents the maximum nesting level. In this paper, we consider quantum repeaters where distillation is performed exclusively before the first entanglement swapping step. The number of distillation rounds is denoted by k.

Each repeater station is equipped with quantum memories and local quantum processors to perform entanglement swapping and, in general, also entanglement distillation. In consecutive *nesting levels*, the distances over which the entangled states are shared will be doubled. The parameter N is the *maximal nesting level*.

The protocol starts by creating entangled states in all segments, i.e., between two quantum memories over distance L_0. After that, if necessary, entanglement distillation is performed. This distillation is a probabilistic process which requires sufficiently many initial pairs shared over distance L_0. As a next step, entanglement swapping is performed at the corresponding repeater stations in order to connect two adjacent entangled pairs and thus gradually extend the entanglement. In those protocols where entanglement swapping is a probabilistic process, the whole quantum repeater protocol is performed in a recursive way as shown in Fig. 1. Whenever the swapping is deterministic (i.e., it never fails), then all swappings can be executed simultaneously, provided that no further probabilistic entanglement distillation steps are to be incorporated at some intermediate nesting levels for enhancing the fidelities. Recall that in the present work, we do not include such intermediate distillations in order to keep the experimental requirements as low as possible. At the same time it allows us to find analytical rate formulas with no need for numerically optimizing the distillation-versus-swapping scheduling in a fully nested quantum repeater.

2. Building blocks of the quantum repeater and their imperfections

In this section we describe a model of the imperfections for the main building blocks of a quantum repeater. In an experimental setup more imperfections than those considered in this model may affect the devices. However, most of them can be incorporated into our model. We point out that if not all possible imperfections are included, the resulting curves for the figure of merit (throughout this paper: the secret key rate) can be interpreted as an upper bound for a given repeater protocol.

(a) Quantum channel. Let us consider photons (in the form of single- or multiphoton pulses) traveling through optical fibers.

Photon losses are the main source of imperfection. Other imperfections like birefringence are negligible in our context [8,25]. Losses scale exponentially with the length ℓ; i.e., the transmittivity is given by [8]

$$\eta_t(\ell) := 10^{-\frac{\alpha_{att}\ell}{10}}, \tag{1}$$

where α_{att} is the attenuation coefficient given in dB/km. The lowest attenuation is achieved in the telecom wavelength range around 1550 nm and it corresponds to $\alpha_{att} = 0.17$ dB/km. This attenuation is also used throughout the paper. Note that other types of quantum channels, such as free space, can be treated in an equivalent way (see, e.g., [26]). Further note that besides losses, the effect of the quantum channel can be incorporated into the form of the initial state shared between the connecting repeater stations.

(b) Source of entanglement. The purpose of a source is to create entanglement between quantum memories over distance L_0. An ideal source produces maximally entangled Bell states (see below) on demand. In practice, however, the created state may not be maximally entangled and may be produced in a probabilistic way. We denote by ρ_0 a state shared between two quantum memories over the elementary distance L_0 and by P_0 the total probability to generate and distribute this state. This probability would contain any finite local state-preparation probabilities before the distribution, the effect of channel losses, and the success probabilities of other processes, such as the conditioning on a desired initial state ρ_0 after the state distribution over L_0.

For improving the scaling over the total distance L from exponential to subexponential, it is necessary to have a heralded creation and storage of ρ_0. How this heralding is implemented depends on the particular protocol and it usually involves a form of postprocessing, e.g., conditioning the state on a specific pattern of detector clicks. This can also be a finite postselection window of quadrature values in homodyne detection. However, in the present work, the measurements employed in all protocols considered here are either photon-number measurements or Pauli measurements on memory qubits.

(c) Detectors. We consider photon-number resolving detectors (PNRDs) which can be described by a positive-operator valued measure (POVM) with elements [27]

$$\Pi^{(n)} := \eta_{\mathrm{d}}^n \sum_{m=0}^{\infty} \binom{n+m}{n} (1-\eta_{\mathrm{d}})^m \, |n+m\rangle \langle n+m| \, . \tag{2}$$

Here, $\Pi^{(n)}$ is the element of the POVM related to the detection of n photons, η_{d} is the efficiency of the detector, and $|n+m\rangle$ is a state of $(n+m)$ photons. In the POVM above, we have neglected dark counts; we have shown analytically for those protocols considered in this paper that realistic dark counts of the order of 10^{-5} are negligible [see Appendix B, below Eq. (B5), for the proof]. Note that our analysis could

also be extended to threshold detectors, by replacing the corresponding POVM (see, e.g., [27]) in our formulas.

(d) Gates. Imperfections of gates also depend on the particular quantum repeater implementation. Such imperfections are described, e.g., in [28]. In our analysis, we characterize them using the gate quality, which will be denoted by p_G [see Eqs. (19) and (24)].

(e) Quantum memories. Quantum memories are a crucial part of a quantum repeater. A complete characterization of imperfections of quantum memories is beyond the purpose of this paper (see [29] for a recent review). Here we account for memory errors by using a fixed time-independent quantum memory efficiency η_m when appropriate. This is the probability that a photon is released when a reading signal is applied to the quantum memory, or, more generally, the probability that an initial qubit state is still intact after write in, storage, and readout. We discuss the role of η_m only for the quantum repeater with atomic ensembles (see Sec. V).

(f) Entanglement distillation. As mentioned before, throughout this work we only consider distillation at the beginning of each repeater protocol. Entanglement distillation is a probabilistic process requiring local multiqubit gates and classical communication. In this paper, we consider the protocol by Deutsch *et al.* [30]. This protocol performs especially well when there are different types of errors (e.g., bit flips and phase flips). However, depending on the particular form of the initial state and on the particular quantum repeater protocol, other distillation schemes may perform better (see [24] for a detailed discussion). The Deutsch *et al.* protocol starts with 2^k pairs, and after k rounds it produces one entangled pair with higher fidelity than at the beginning. Every round requires two controlled NOT (CNOT) operations, each performed on two qubits at the same repeater station, and projective measurements with postselection.

Distillation has two main sources of errors: imperfect quantum gates which no longer permit to achieve the ideal fidelity, as well as imperfections of the quantum memories and the detectors, decreasing the success probability. We denote the success probability in the ith distillation round by $P_D[i]$.

We study entanglement distillation for the original quantum repeater protocol (Sec. III) and the hybrid quantum repeater (Sec. IV). For the quantum repeater with atomic ensembles (Sec. V), we do not consider any additional distillation on two or more initial memory pairs.

(g) Entanglement swapping. In order to extend the initial distances of the shared entanglement, entanglement swapping can be achieved through a Bell measurement performed at the corresponding stations between two adjacent segments. Such a Bell measurement can be, in principle, realized using a CNOT gate and suitable projection measurements on the corresponding quantum memories [31]. An alternative implementation of the Bell measurement uses photons released from the quantum memories and linear optics [32]. The latter technique is probabilistic, but typically much less demanding from an experimental point of view.

We should emphasize that the single-qubit rotation depending on the result of the Bell measurement, as generally needed to complete the entanglement swapping step, is not necessary when the final state is used for QKD applications. In fact, it simply corresponds to suitable bit flip operations on the outcomes of the QKD measurements; i.e., the effect of that single-qubit rotation can be included into the classical postprocessing.

Imperfections of entanglement swapping are characterized by the imperfections of the gates (which introduce noise and therefore a decrease in fidelity) and by the imperfections of the measurement process, caused by imperfect quantum memories and imperfect detectors. We denote the probability that entanglement swapping is successful in the nth nesting level by $P_{\mathrm{ES}}^{(n)}$.

(h) Other imperfections. Other imperfections which are not explicitly considered in this paper but which are likely to be present in a real experiment include imperfections of the interconversion process, fluctuations of the quantum channel, fiber coupling losses, and passive losses of optical elements (see [25] and references therein for additional details). These imperfections can be accounted for by a suitable adjustment of the relevant parameters in our model.

3. Generation rate of long-distance entangled pairs

In order to evaluate the performance of a quantum repeater protocol it is necessary to assess how many entangled pairs across distance L can be generated per second.

A relevant unit of time is the *fundamental time* needed to communicate the successful distribution of an elementary entangled pair over distance L_0, which is given by

$$T_0 := \frac{\beta L_0}{c}, \tag{3}$$

where $c = 2 \times 10^5$ km/s is the speed of light in the fiber channel (see, e.g., [25]) and β is a factor depending on the type of entanglement distribution. Note that here we have neglected the additional local times needed for preparing and manipulating the physical systems at each repeater station. Figure 2 shows three different possibilities of how to model the initial entanglement distribution. The fundamental time T_0 consists of the time to distribute the photonic signals, T_{dist}, and the time of acknowledgment, T_{ack}, which all together can be different for the three cases shown.

Throughout the paper, we denote the average number of final entangled pairs produced in the repeater per second by R_{REP}. We emphasize that, regarding any figures and plots, for each protocol, we are interested in the consumption of time rather than spatial memories. Thus, if one wants to compare different setups for the same number of spatial memories, one has to rescale the rates such that the number of memories becomes equal. For example, in order to compare a protocol without distillation with another one with k rounds of distillation, one has to divide the rates for the case with distillation by 2^k (as we need two initial pairs to obtain one distilled pair in every round).

In the literature, two different upper bounds on the entanglement generation rate R_{REP} are known. In the case of deterministic entanglement swapping ($P_{ES}^{(n)} = 1$) we have [35]

$$R_{\mathrm{REP}}^{\mathrm{det}} = [T_0 Z_N(P_{L_0}[k])]^{-1}, \tag{4}$$

with $P_{L_0}[i]$ being a recursive probability depending on the rounds of distillation i as follows [35]:

$$P_{L_0}[i = 0] = P_0, \tag{5}$$

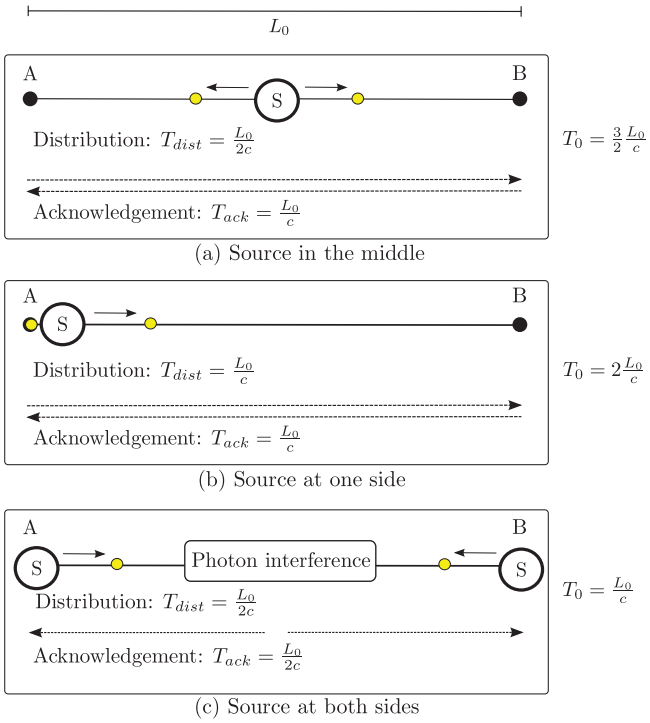


FIG. 2. (Color online) The fundamental time for different models of entanglement generation and distribution. The source (S) that produces the initial entangled states is either placed in the middle (a), at one side (b), or at both sides (c). In the latter case, photons are emitted from a source and interfere in the middle (see [33,34]).

$$P_{L_0}[i > 0] = \frac{P_D[i]}{Z_1(P_{L_0}[i-1])}. \tag{6}$$

We remind the reader that $P_D[i]$ is the success probability in the ith distillation round. Here,

$$Z_N(P_0) := \sum_{j=1}^{2^N} \binom{2^N}{j} \frac{(-1)^{j+1}}{1-(1-P_0)^j} \tag{7}$$

is the average number of attempts to connect 2^N pairs, each generated with probability P_0.

In the case of probabilistic entanglement swapping, probabilistic entanglement distillation, and $P_0 \ll 1$, we find an upper bound on the entanglement generation rate,

$$R_{\mathrm{REP}}^{\mathrm{prob}} = \frac{1}{T_0}\left(\frac{2}{3a}\right)^{N+k} P_0 P_{ES}^{(1)} P_{ES}^{(2)} \cdots P_{ES}^{(N)} \prod_{i=1}^{k} P_D[i], \tag{8}$$

with $a \leqslant \frac{2}{3} P_{L_0}[k] Z_1(P_{L_0}[k])$. Our derivation is given in Appendix A. For the plots we bound a according to the occurring parameters, typically a is close to one, which corresponds to the approximate formula given in [25] for the case when there is no distillation.

Equations (4) and (8) should be interpreted as a limiting upper bound on the repeater rate, due to the minimal time needed for communicating the quantum and classical signals. For this minimal time, we consider explicitly only those communication times for initially generating entanglement, but not those for entanglement swapping and entanglement distillation.

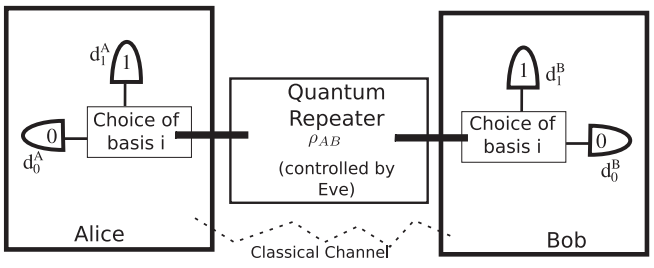


FIG. 3. Scheme of QKD. The state ρ_{AB} is produced using a quantum repeater. Alice and Bob locally rotate this state in a measurement basis and then they perform the measurement. The detectors are denoted by $d_0^A, d_1^A, d_0^B, d_1^B$ and to each detector click a classical outcome is assigned.

B. Quantum key distribution

1. The QKD protocol

In Fig. 3 a general QKD setup is shown. For long-distance QKD, Alice and Bob will generate entangled pairs using the quantum repeater protocol. For the security analysis of the whole repeater-based QKD scheme, we assume that a potential eavesdropper (Eve) has complete control of the repeater stations, the quantum channels connecting them, and the classical channels used for communicating the measurement outcomes for entanglement swapping and distillation (see Fig. 3). The QKD protocol itself starts with Alice and Bob performing measurements on their shared, long-distance entangled pairs (see Fig. 3). For this purpose, they would both independently choose a certain measurement from a given set of measurement settings. The next step is the classical postprocessing and for this an authenticated channel is necessary. First, Alice and Bob discard those measurement outcomes where their choice of the setting did not coincide (sifting), thus obtaining a raw key associated with a *raw key rate*. They proceed by comparing publicly a small subset of outcomes (parameter estimation). From this subset, they can estimate the *quantum bit error rate* (QBER), which corresponds to the fraction of uncorrelated bits. If the QBER is below a certain threshold, they apply an error correction protocol and privacy amplification in order to shrink the eavesdropper's information about the secret key (for more details, see, e.g., [36]).

Various QKD protocols exist in the literature. Besides the original QKD protocol by Bennett and Brassard from 1984, the so-called BB84 protocol [37], the first QKD protocol based upon entanglement was the Ekert protocol [1]. Shortly thereafter the relation of the Ekert protocol to the BB84 protocol was found [38]. Another protocol which can also be applied in entanglement-based QKD is the six-state protocol [39,40].

2. The quantum bit error rate

In order to evaluate the performance of a QKD protocol, it is necessary to determine the QBER. This is the fraction of discordant outcomes when Alice and Bob compare a small amount of outcomes taken from a specified measurement basis.

This measurement can be modeled by means of four detectors (two on Alice's side and two on Bob's side; see Fig. 3), where to each detector click a classical binary outcome is assigned. Particular care is necessary when multiphoton states are measured [41,42]. In the following, we give the definition of the QBER for the case of PNRDs and we refer to [20] for the definition in the case of threshold detectors. The probability that a particular detection pattern occurs is given by

$$P^{(i)}_{jklm} := \mathrm{tr}\left(\Pi^{(j)}_{d_0^A}\Pi^{(k)}_{d_1^A}\Pi^{(l)}_{d_0^B}\Pi^{(m)}_{d_1^B}\rho^{(i)}_{AB}\right), \tag{9}$$

where the POVM $\Pi^{(n)}$ has been defined in Eq. (2) with a subscript denoting the detectors given in Fig. 3. The superscript i refers to the measurement basis and $\rho^{(i)}_{AB}$ represents the state ρ_{AB} rotated in the basis i.

A valid QKD measurement event happens when one detector on Alice's side and one on Bob's side click. The probability of this event is given by [20]

$$P^{(i)}_{\mathrm{click}} := P^{(i)}_{1010} + P^{(i)}_{0101} + P^{(i)}_{0110} + P^{(i)}_{1001}. \tag{10}$$

The probability that two outcomes do not coincide is given by [20]

$$P^{(i)}_{\mathrm{err}} := P^{(i)}_{0110} + P^{(i)}_{1001}. \tag{11}$$

Thus, the fraction of discordant bits, i.e., the QBER for measurement basis i is [20]

$$e_i := \frac{P^{(i)}_{\mathrm{err}}}{P^{(i)}_{\mathrm{click}}}. \tag{12}$$

For the case that ρ_{AB} is a two-qubit state, we find that the QBER does not depend on the efficiency of the detectors, as $P^{(i)}_{\mathrm{click}} = \eta_{\mathrm{d}}^2$ and $P^{(i)}_{\mathrm{err}} \propto \eta_{\mathrm{d}}^2$.

If we assume a genuine two-qubit system[1] like in the original quantum repeater proposal (see Sec. III) or the hybrid quantum repeater (see Sec. IV), without loss of generality,[2] the entangled state ρ_{AB} can be considered diagonal in the Bell basis, i.e., $\rho_{AB} = A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|$, with the probabilities A, B, C, D, $A + B + C + D = 1$, and with the dual-rail[3] encoded Bell states[4] $|\phi^\pm\rangle = (|1010\rangle \pm |0101\rangle)/\sqrt{2}$ and $|\psi^\pm\rangle = (|1001\rangle \pm |0110\rangle)/\sqrt{2}$ (we shall use the notation $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$ for the Bell basis in any type of encoding throughout the paper). Then the QBER along the directions X, Y, and Z corresponds to [6]

$$e_X := B + D, \quad e_Z := C + D, \quad e_Y := B + C. \tag{13}$$

Throughout the whole paper X, Y, and Z denote the three Pauli operators acting on the restricted Hilbert space of qubits.

3. The secret key rate

The figure of merit representing the performance of QKD is the *secret key rate* R_{QKD}, which is the product of the *raw key rate* R_{raw} (see above) and the *secret fraction* r_∞. Throughout this paper, we use asymptotic secret key rates. The secret fraction represents the fraction of secure bits that may be extracted from the raw key. Formally, we have

$$R_{\mathrm{QKD}} := R_{\mathrm{raw}} r_\infty = R_{\mathrm{REP}} P_{\mathrm{click}} R_{\mathrm{sift}} r_\infty, \tag{14}$$

where the sifting rate R_{sift} is the fraction of measurements performed in the same basis by Alice and Bob. Throughout the paper we use $R_{\mathrm{sift}} = 1$, which represents the asymptotic bound for R_{sift} when the measurement basis are chosen with biased probability [45]. We point out that both R_{REP} and r_∞ are functions of the explicit repeater protocol and the involved experimental parameters, as we discuss in detail later. Our aim is to maximize the overall secret key rate R_{QKD}. There will be a trade-off between R_{REP} and r_∞, as the secret key fraction r_∞ is an increasing function of the final fidelity, while the repeater rate R_{REP} typically decreases with increasing final fidelity.

Note that even though for the considered protocol we find upper bounds on the secret key rate, an improved model (e.g., including distillation in later nesting levels or multiplexing [46]) could lead to improved key rates.

The secret fraction represents the fraction of secure bits over the total number of measured bits. We adopt the *composable security definition* discussed in [47–49]. Here, composable means that the secret key can be used in successive tasks without compromising its security. In the following we calculate secret key rates using the state produced by the quantum repeater protocol.

In the present work, we consider only two QKD protocols, namely the BB84 protocol and the six-state protocol, for which collective and coherent attacks are equivalent [43,44] in the limit of a large number of exchanged signals. The unique parameter entering the formula of the secret fraction is the QBER.

In the BB84 protocol only two of the three Pauli matrices are measured. We adopt the asymmetric protocol where the measurement operators are chosen with different probabilities [45], because this leads to higher key rates. We call X the basis used for extracting a key, i.e., the basis that will be chosen with a probability of almost one in the measurement process, while Z is the basis used for the estimation of the QBER. Thus, in the asymptotic limit, we have $R_{\mathrm{sift}} = 1$. The formula for the secret fraction is [6]

$$r_\infty^{\mathrm{BB84}} := 1 - h(e_Z) - h(e_X), \tag{15}$$

with $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ being the binary entropy. This formula is an upper bound on the secret fraction, which is achievable only for ideal implementations

[1]Note that the states of the DLCZ-type quantum repeaters (see Sec. V) are only effectively two-qubit states when higher-order excitations of the atom-light entangled states [12], or those of the states created through parametric down-conversion [23], are neglected.

[2]As proven in [43,44], it is possible to apply an appropriate local twirling operation that transforms an arbitrary two-qubit state into a Bell diagonal state, while the security of the protocol is not compromised.

[3]In this paper, by *dual-rail representation* we mean that a single photon can be in a superposition of two optical modes, thus representing a single qubit. By *single-rail representation* we mean that a qubit is implemented using only one single optical mode. See [27] for additional details.

[4]The ket $|abcd\rangle$ is a vector in a Hilbert space of four modes and the values of a, b, c, and d represent the number of excitations in the Fock basis.

of the protocol; any realistic, experimental imperfection will decrease this secret key rate.

In the six-state protocol we use all three Pauli matrices. We call X the basis used for extracting a key, which will be chosen with a probability of almost one, and both Y and Z are the bases used for parameter estimation. In this case, the formula for the secret fraction is given by [6,36][5]

$$r_\infty^{6S} := 1 - e_Z h\left(\frac{1+(e_X-e_Y)/e_Z}{2}\right) - (1-e_Z)h\left(\frac{1-(e_X+e_Y+e_Z)/2}{1-e_Z}\right) - h(e_Z). \tag{16}$$

C. Methods

The secret key rate represents the central figure of merit for our investigations. We study the BB84 protocol, because it is most easily implementable and can also be used for protocols, where ρ_{AB} is not a two-qubit state, with help of the squashing model [41,42]. Throughout the paper, we also report on results of the six-state protocol if applicable. We evaluate Eq. (14) exactly, except for the quantum repeater based on atomic ensembles where we truncate the states and cut off the higher excitations at some maximal number (see footnote 11 for the details). For the maximization of the secret key rate, we have used the numerical functions provided by Mathematica [50].

III. THE ORIGINAL QUANTUM REPEATER

In this section, we consider a general class of quantum repeaters in the spirit of the original proposal by Briegel *et al.* [7]. We analyze the requirements for the experimental parameters such that the quantum repeater is useful in conjunction with QKD. The model we consider in this section is applicable whenever two-qubit entanglement is distributed by using qubits encoded into single photons. This is the case, for instance, for quantum repeaters based on ion traps or Rydberg-blockade gates. We emphasize that we do not aim to capture all peculiarities of a specific setup. Instead, our intention is to present a fairly general analysis that can give an idea of the order of magnitude, which has to be achieved for the relevant experimental parameters. The error model we consider is the one used in [7].

A. The setup

1. Elementary entanglement creation

The probability that two adjacent repeater stations (separated by distance L_0) share an entangled pair is given by

$$P_0 := \eta_t(L_0), \tag{17}$$

where $\eta_t(\ell)$, as defined in Eq. (1), is the probability that a photon is not absorbed during the channel transmission. In a specific protocol, P_0 may contain an additional multiplicative factor such as the probability that entanglement is heralded or also a source efficiency. We assume that the state created over distance L_0 is a depolarized state of fidelity F_0 with respect to $|\phi^+\rangle$; i.e.,

$$\rho_0 := F_0|\phi^+\rangle\langle\phi^+| + \frac{1-F_0}{3}(|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-| + |\phi^-\rangle\langle\phi^-|). \tag{18}$$

The fidelity F_0 contains the noise due to an imperfect preparation and the noise in the quantum channel. We have chosen a depolarized state, because this corresponds to a generic noise model and, moreover, any two-qubit mixed quantum state can be brought into this form using local twirling operations [51].

2. Imperfect gates

For the local qubit operations, such as the CNOT gates, we use a generic gate model with depolarizing noise, as considered in [7]. Thus, we assume that a noisy gate O_{BC} acting upon two qubits B and C can be modeled by

$$O_{BC}(\rho_{BC}) = p_G O_{BC}^{\text{ideal}}(\rho_{BC}) + \frac{1-p_G}{4}\mathbb{1}_{BC}, \tag{19}$$

where O_{BC}^{ideal} is the ideal gate operation and p_G describes the gate quality. Note that, in general, the noisy gates realized in an experiment do not necessarily have this form; however, such a noise model is useful for having an indication as to how good the corresponding gates must be. Other noise models could be analogously incorporated into our analysis. Further, we assume that one-qubit gates are perfect.

3. Entanglement distillation

We consider entanglement distillation only before the first entanglement swapping steps, right after the initial pair distributions over L_0. We employ the Deutsch *et al.*protocol [30] which indeed has some advantages, as shown in the analysis of [24]. In Appendix B2, we review this protocol and we also present the corresponding formulas in the presence of imperfections. We point out that when starting with two copies of depolarized states, the distillation protocol will generate an output state which is no longer a depolarized state, but instead a generic Bell diagonal state. Distillation requires two-qubit gates, which we describe using Eq. (19).

4. Entanglement swapping

The entanglement connections are performed through entanglement swapping by implementing a (noisy) Bell measurement on the photons stored in two local quantum memories. We consider a Bell measurement that is deterministic in the ideal case. It is implemented using a two-qubit gate with gate quality p_G [see Eq. (19)]. Analogous to the case of distillation, starting with two depolarized states, at the end of the noisy Bell measurement, we obtain generic Bell diagonal states. Also in this case, it turns out that a successive depolarization decreases the secret key rate and this step is therefore not performed in our scheme.

[5]Note that the formula for the six-state protocol is independent of the choice of basis, when we assume the state of Alice and Bob ρ_{AB} to be Bell diagonal. Then the secret fraction reduces to $r_\infty^{6S} = 1 - S(\rho_E)$ with $S(\rho)$ the von Neumann entropy and ρ_E is the eavesdropper's state.

B. Performance in the presence of imperfections

The secret key rate Eq. (14) represents our central object of study, as it characterizes the performance of a QKD protocol. It can be written explicitly as a function of the relevant parameters,

$$R^{\mathrm{O}}_{\mathrm{QKD}} = R_{\mathrm{REP}}(L_0,N,k,F_0,p_G,\eta_{\mathrm{d}})P_{\mathrm{click}}(\eta_{\mathrm{d}}) \times R_{\mathrm{sift}} r_\infty(N,k,F_0,p_G), \quad (20)$$

where R_{REP} is given by Eq. (4) when $\eta_{\mathrm{d}} = 1$ (because then $P_{\mathrm{ES}} = 1$) or by Eq. (8) if $\eta_{\mathrm{d}} < 1$.[6] The probability that the QKD measurement is successful is given by $P_{\mathrm{click}} = \eta_{\mathrm{d}}^2$ and the secret fraction r_∞ is given by either Eq. (15) or Eq. (16), depending on the type of QKD protocol. For the asymmetric BB84 protocol, we have $R_{\mathrm{sift}} = 1$ (see Sec. II B). The superscript O refers to the original quantum repeater proposal as considered in this section. In order to have a nonzero secret key rate, it is then necessary that the repeater rate, the probability for a valid QKD measurement event, and the secret fraction are each nonzero too. As typically $R_{\mathrm{REP}} > 0$, $R_{\mathrm{sift}} > 0$, and $P_{\mathrm{click}} > 0$, for $R_{\mathrm{QKD}} > 0$, it is sufficient to have a nonzero secret fraction, $r_\infty > 0$. The value of the secret fraction does not depend on the distance, and therefore some properties of this protocol are distance invariant.

Minimally required parameters. In this paragraph, we discuss the minimal requirements that are necessary to be able to extract a secret key; i.e., we specify the parameter region where the secret fraction is nonzero. From the discussion in the previous paragraph, we know that this region does not depend on the total distance, but only on the initial fidelity F_0, the gate quality p_G, the number of segments 2^N, and the maximal number of distillation rounds k. Moreover, note that even if the secret fraction is not zero, the total secret key rate can be very low (see below).

For calculating the minimally required parameters, we start with the initial state in Eq. (18), we distill it k times (see the formulas in Appendix B2), and then we swap the distilled state $2^N - 1$ times (see the formulas in Appendix B1). At the end, a generic Bell diagonal state is obtained. Using Eq. (13) one can then calculate the QBER, which is sufficient to calculate the secret fraction.

Tables I and II show the minimally required values for F_0 and p_G for different maximal nesting levels N (i.e., different numbers of segments 2^N) and different numbers of rounds of distillation k. Throughout these tables, we can see that for the six-state protocol, the minimal fidelity and the minimal gate quality p_G are lower than for the BB84 protocol. Our results confirm the intuition that the larger the number of distillation rounds, the smaller the affordable initial fidelity can be (at the cost of needing higher gate qualities).

TABLE I. Minimal initial fidelity F_0 (p_G is fixed to one) for extracting a secret key with maximal nesting level N and number of distillation rounds k for the BB84 and six-state protocols.

N \ k	0		1		2		3	
	BB84	6S	BB84	6S	BB84	6S	BB84	6S
0	0.835	0.810	0.733	0.728	0.671	0.669	0.620	0.614
1	0.912	0.898	0.821	0.818	0.742	0.740	0.669	0.664
2	0.955	0.947	0.885	0.884	0.801	0.800	0.713	0.709
3	0.977	0.973	0.929	0.928	0.849	0.848	0.752	0.749
4	0.988	0.987	0.957	0.957	0.887	0.887	0.788	0.785
5	0.994	0.993	0.975	0.975	0.917	0.917	0.819	0.818
6	0.997	0.997	0.985	0.985	0.939	0.939	0.847	0.846
7	0.999	0.998	0.992	0.992	0.956	0.956	0.872	0.870

In Fig. 4, the lines represent the values of the initial infidelity and the gate error for a specific N that allow for extracting a secret key. As shown in Fig. 4, any lower initial fidelity requires a correspondingly higher gate quality and vice versa. Note that above the lines in Fig. 4 it is not possible to extract a secret key.

The secret key rate. In this section, we analyze the influence of the imperfections on the secret key rate; see Eq. (20).

In Fig. 5 we illustrate the effect of gate imperfections on the secret key rate for different numbers of rounds of distillation and for a fixed distance, initial fidelity, and maximal number of nesting levels. Throughout this whole section, we use $\beta = 2$ in Eq. (3) for the fundamental time, which corresponds to the case where a source is placed at one side of an elementary segment (see Fig. 2). The optimal number of distillation rounds decreases as p_G increases. We see from the figure that $k = 2$ is optimal when $p_G = 1$. This is due to the fact that from $k = 1$ to $k = 2$, the raw key rate decreases by 40%, but the secret fraction increases by 850%. However, from $k = 2$ to $k = 3$, the raw key rate decreases once again by 40%, but now the

TABLE II. Minimal p_G (F_0 is fixed to one) for extracting a secret key with maximal nesting level N and number of distillation rounds k for the BB84 and six-state protocols.

N \ k	0		1		2		3	
	BB84	6S	BB84	6S	BB84	6S	BB84	6S
0			0.800	0.773	0.869	0.860	0.891	0.884
1	0.780	0.748	0.922	0.910	0.942	0.937	0.947	0.942
2	0.920	0.908	0.965	0.960	0.973	0.970	0.974	0.972
3	0.965	0.959	0.984	0.981	0.987	0.986	0.987	0.986
4	0.984	0.981	0.992	0.991	0.994	0.993	0.994	0.993
5	0.992	0.991	0.996	0.995	0.997	0.997	0.997	0.997
6	0.996	0.995	0.998	0.998	0.999	0.998	0.999	0.998
7	0.998	0.998	0.999	0.999	0.999	0.999	0.999	0.999

[6]The supposed link between the effect of imperfect detectors and the determinism of the entanglement swapping here assumes the following. Any incomplete detection patterns that occur in the Bell measurements due to imperfect detectors are considered as inconclusive results and will be discarded. Conversely, with perfect detectors, we assume that we always have complete patterns and thus the Bell state discrimination becomes complete too. Note that this kind of reasoning directly applies to Bell measurements in dual-rail encoding, where the conclusive output patterns always have the same fixed total number for every Bell state (namely, two photons leading to twofold detection events), and so any loss of photons will result in patterns considered inconclusive. In single-rail encoding, the situation is more complicated and patterns considered conclusive may be the result of an imperfect detection.

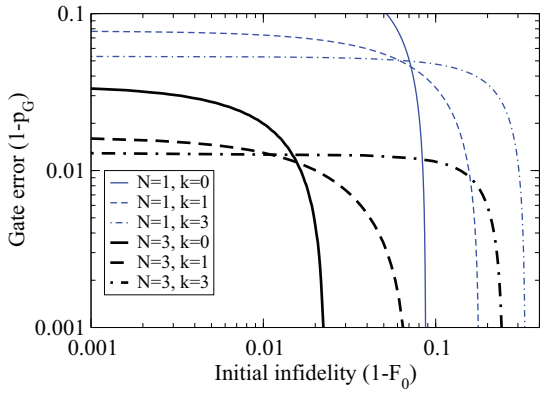


FIG. 4. (Color online) Original quantum repeater and the BB84 protocol: Maximal infidelity $(1 - F_0)$ as a function of gate error $(1 - p_G)$, making it possible to extract a secret key for various maximal nesting levels N and numbers of distillation rounds k (parameter: $L = 600$ km).

secret fraction increases only by 141%. In this case, the net gain is smaller than 1 and therefore three rounds of distillation do not help to increase the secret key rate compared to the case of two rounds. In other words, what is lost in terms of success probability when having three probabilistic distillation rounds is not added to the secret fraction. For a decreasing p_G, more rounds of distillation become optimal. The reason is that when the gates become worse, additional rounds of distillation make it possible to increase the secret key rate sufficiently to compensate the decrease of R_{REP}.

In Fig. 6 we show the optimal number of rounds of distillation k as a function of the imperfections of the gates and the initial fidelity. It turns out that when the experimental parameters are good enough, then distillation is not necessary at all.

Let us now investigate the secret key rate Eq. (20) as a function of the distance L between Alice and Bob. In Fig. 7 the secret key rate for the optimal number of distillation rounds versus the distance for various nesting levels is shown for a fixed initial fidelity and gate quality. These curves should be

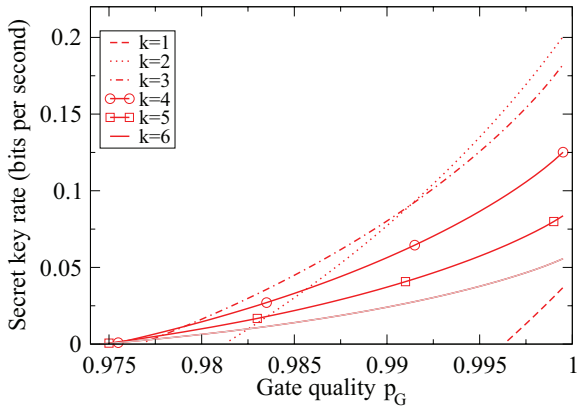


FIG. 5. (Color online) Original quantum repeater and the BB84 protocol: Secret key rate Eq. (20) versus gate quality p_G for different rounds of distillation k. The case $k = 0$ leads to a vanishing secret key rate (parameters: $F_0 = 0.9$, $N = 2$, $L = 600$ km).

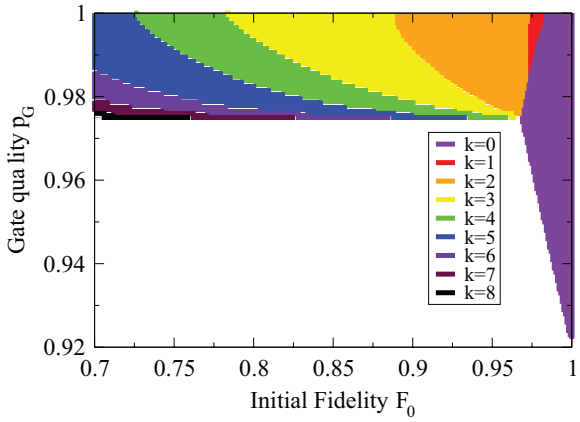


FIG. 6. (Color online) Original quantum repeater and the BB84 protocol: Number of distillation rounds k that maximizes the secret key rate as a function of gate quality p_G and initial fidelity F_0. In the white area, it is no longer possible to extract a secret key (parameters: $N = 2$, $L = 600$ km).

interpreted as upper bounds; when additional imperfections are included, the secret key rate will further decrease. We see that for a distance of more than 400 km, the value $N = 4$ (which corresponds to 16 segments) is optimal. Note that with the initial fidelity and gate quality assumed here, it is no longer possible to extract a secret key for $N = 5$.

In many implementations, detectors are far from being perfect. The general expression of the raw key rate including detector efficiencies η_{d} becomes

$$R_{\mathrm{raw}} = \frac{1}{T_0} R_{\mathrm{sift}} \left(\frac{2}{3}\right)^{N+k} \eta_{\mathrm{d}}^{2(k+N+1)} P_0 \prod_{i=1}^{k} P_D[i], \qquad (21)$$

using Eq. (14) with the repeater rate R_{REP} given by Eq. (8). The term η_{d}^{2k} arises from the twofold detections for the distillation, and, similarly, η_{d}^{2N} comes from the entanglement swapping and η_{d}^{2} from the QKD measurements.

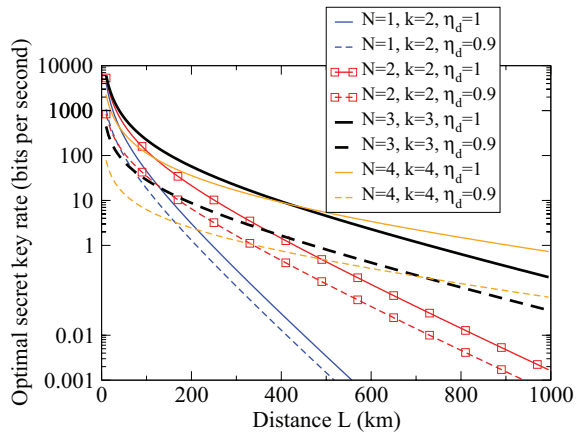


FIG. 7. (Color online) Original quantum repeater and the BB84 protocol: Optimal secret key rate Eq. (20) versus distance for different nesting levels, with and without perfect detectors. For each maximal nesting level N, we have chosen the optimal number of distillation rounds k. A nesting level $N \geqslant 5$ no longer permits to obtain a nonzero secret key rate (parameters: $F_0 = 0.9$ and $p_G = 0.995$).

In Fig. 7 we observe that even if detectors are imperfect, it is advantageous to do the same number of rounds of distillation as for the perfect case. This is due to the fact that the initial fidelity is so low that even with a lower success probability, the gain in the secret fraction produces a net gain greater than 1.

For realistic detectors, the dark count probability is much smaller than their efficiency. We show in Appendix B that, provided that the dark count probability is smaller than 10^{-5}, dark counts can be neglected. This indeed applies to most modern detectors [52].

IV. THE HYBRID QUANTUM REPEATER

In this section, we investigate the so-called hybrid quantum repeater (HQR) introduced by van Loock *et al.* [13] and Ladd *et al.* [53]. In this scheme, the resulting entangled pairs are discrete atomic qubits, but the probe system (also called *qubus*) that mediates the two-qubit entangling interaction is an optical mode in a coherent state. The scheme does not only employ atoms and light at the same time, but it also uses both discrete and continuous quantum variables; hence, the name hybrid. The entangled pair is conditionally prepared by suitably measuring the probe state after it has interacted with two atomic qubits located in the two spatially separated cavities at two neighboring repeater stations. Below we consider a HQR where the detection is based on an unambiguous state discrimination (USD) scheme [54,55]. In this case, arbitrarily high fidelities can be achieved at the expense of low probabilities of success.

A. The setup

1. Elementary entanglement creation

Entanglement is shared between two electronic spins (such as Λ systems effectively acting as two-level systems) in two distant cavities (separated by L_0). The entanglement distribution occurs through the interaction of the coherent-state pulse with both atomic systems. The coherent-state pulse and the cavity are in resonance, but they are detuned from the transition between the ground state and the excited state of the two-level system. This interaction can then be described by the Jaynes-Cummings interaction Hamiltonian in the limit of large detuning, $H_{int} = \hbar\chi Z a^\dagger a$, where χ is the light-atom coupling strength, a ($a^\dagger$) is the annihilation (creation) operator of the electromagnetic field mode, and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ is the Z operator for a two-level atom (throughout this section, $|0\rangle$ and $|1\rangle$ refer to the two Z Pauli eigenstates of the effective two-level matter system and not to the optical vacuum and one-photon Fock states). After the interaction of the qubus in state $|\alpha\rangle$ with the first atomic state, which is initially prepared in a superposition, the output state is $U_{\rm int}[|\alpha\rangle(|0\rangle + |1\rangle)/\sqrt{2}] = (|\alpha e^{-i\theta/2}\rangle|0\rangle + |\alpha e^{i\theta/2}\rangle|1\rangle)/\sqrt{2}$, with $\theta = 2\chi t$ an effective light-matter interaction time inside the cavity. The qubus probe pulse is then sent through the lossy fiber channel and interacts with the second atomic qubit also prepared in a superposition. Here we consider the protocol of [55], where linear optical elements and photon detectors are used for the unambiguous discrimination of the phase-rotated coherent states. Different from [55], however, we use imperfect PNRDs, as described by Eq. (2), instead of threshold detectors.

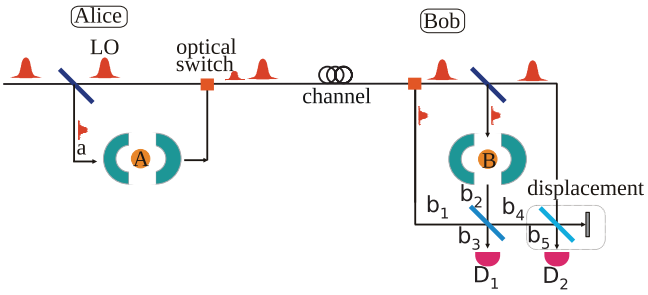


FIG. 8. (Color online) Schematic diagram for the entanglement generation by means of a USD measurement following [55]. The two quantum memories A and B are separated by a distance L_0. The part on the left side (an intermediate Alice) prepares a pulse in a coherent state $|\alpha\rangle_a$ (the subscript refers to the corresponding spatial mode). This pulse first interacts with her qubit A and is then sent to the right side together with the local oscillator pulse (LO). The part on the right side (an intermediate Bob) receives the state $|\sqrt{\eta_t}\alpha\rangle_{b_1}$ and produces from the LO through beam splitting a second probe pulse $|\sqrt{\eta_t}\alpha\rangle_{b_2}$, which interacts with his qubit B. He further applies a 50:50 beam splitter to the pulses in modes b_1 and b_2, and a displacement $D(-\sqrt{2\eta_t}\alpha\cos\theta/2) = e^{-\sqrt{2\eta_t}\alpha\cos\theta/2(a^\dagger - a)}$ to the pulse in mode b_4. The entangled state is conditionally generated depending on the results of detectors D_1 and D_2. The fiber attenuation $\eta_t(L_0)$ has been defined in Eq. (1).

By performing such a USD measurement on the probe state, as illustrated in Fig. 8, the following entangled state can be conditionally prepared,

$$\rho_0 := F_0|\phi^+\rangle\langle\phi^+| + (1 - F_0)|\phi^-\rangle\langle\phi^-|, \tag{22}$$

where we find $F_0 = [1 + e^{-2(1+\eta_t(1-2\eta_d))\alpha^2\sin^2(\theta/2)}]/2$ for α real, $\eta_t(L_0)$ is the channel transmission given in Eq. (1), and η_d is the detection efficiency (see Sec. II A 2). Our derivation of the fidelity F_0 can be found in Appendix C 1. Note that the form of this state is different from the state considered in Sec. III. It is a mixture of only two Bell states, since the two other (bit flipped) Bell states are filtered out through the USD measurement. The remaining mixedness is due to a phase flip induced by the coupling of the qubus mode with the lossy fiber environment. We find the optimal probability of success to generate an entangled pair in state ρ_0,

$$P_0 = 1 - (2F_0 - 1)^{\frac{\eta_t\eta_d}{1+\eta_t(1-2\eta_d)}}, \tag{23}$$

which generalizes the formula for the quantum mechanically optimal USD with perfect detectors, as given in [54], to the case of imperfect PNRDs. We explain our derivation of Eq. (23) in Appendix C 1. [7]

2. Entanglement swapping

A two-qubit gate is essential to perform entanglement swapping and entanglement distillation. In the HQR a controlled-Z

[7] One may also measure the qubus using homodyne detection [13]. However, for this scheme, final fidelities would be limited to $F_0 < 0.8$ for $L_0 = 10$ km [13], whereas by using USD, we can tune the parameters for any distance L_0, such that the fidelity F_0 can be chosen freely and, in particular, made arbitrarily close to unity at the expense of the success probability dropping close to zero [54].

(CZ) gate operation can be achieved by using dispersive interactions of another coherent-state probe with the two input qubits of the gate. This is similar to the initial entanglement distribution, but this time without any final measurement on the qubus [56]. Controlled rotations and uncontrolled displacements of the qubus are the essence of this scheme. The controlled rotations are realized through the same dispersive interaction as explained above. In an ideal scheme, after a sequence of controlled rotations and displacements on the qubus, the qubus mode will automatically disentangle from the two qubits and the only effect will be a sign flip on the $|11\rangle$ component of the input two-qubit state (up to single-qubit rotations), corresponding to a CZ gate operation. Thus, this gate implementation can be characterized as measurement-free and deterministic. Using this gate, one can then perform a fully deterministic Bell measurement (i.e., one is able to distinguish between all four Bell states), and consequently, the swapping occurs deterministically (i.e., $P_{ES} \equiv 1$).

In a more realistic approach, local losses will cause errors in these gates. Following [57], after dissipation, we may consider the more general, noisy two-qubit operation O_{BC} acting upon qubits B and C,

$$\begin{aligned} O_{BC}(\rho_{BC}) = O_{BC}^{\text{ideal}}\{ & p_c^2(x)\rho_{BC} \\ & + p_c(x)[1-p_c(x)](Z^B\rho_{BC}Z^B + Z^C\rho_{BC}Z^C) \\ & + [1-p_c(x)]^2 Z^B Z^C \rho_{BC} Z^C Z^B\}, \end{aligned} \tag{24}$$

where

$$p_c(x) := \frac{1+e^{-x/2}}{2} \tag{25}$$

is the probability for each qubit to not suffer a Z error, and $x := \pi \frac{1-p_G^2}{\sqrt{p_G}(1+p_G)}$; here p_G is the local transmission parameter that incorporates photon losses in the local gates.[8] We derive explicit formulas for entanglement swapping including imperfect two-qubit gates in Appendix C2.

3. *Entanglement distillation*

For the distillation, the same two-qubit operation as described above in Eq. (24) can be used. It is then interesting to notice that if we start with a state given in Eq. (22), after one round of imperfect distillation, the resulting state is a generic Bell diagonal state. The effect of gate errors in the distillation step is derived in Appendix C3.[9]

B. Performance in the presence of imperfections

In the following, we only consider the BB84 protocol, because it is experimentally less demanding and also because we found in our simulations that the six-state protocol produces almost the same secret key rates, due to the symmetry of the state in Eq. (22). The secret key rate per second for the HQR can be written as a function of the relevant parameters:

$$\begin{aligned} R_{\text{QKD}}^{\text{H}} = & R_{\text{REP}}^{\text{det}}(L_0, N, k, F_0, p_G, \eta_{\text{d}}) \\ & \times R_{\text{sift}} r_\infty^{\text{BB84}}(L_0, N, k, F_0, p_G), \end{aligned} \tag{26}$$

where $R_{\text{REP}}^{\text{det}}$ is the repeater pair-creation rate for deterministic swapping Eq. (4) described in Sec. II A 3 and r_∞^{BB84} is the secret fraction for the BB84 protocol Eq. (15). For the asymmetric BB84 protocol, we have $R_{\text{sift}} = 1$ (see Sec. II B). The superscript H stands for HQR. Note that the fundamental time is $T_0 = \frac{2L_0}{c}$, as the qubus is sent from Alice to Bob and then classical communication in the other direction is used (see Sec. II A 3 and Fig. 2). Further notice that the final projective qubit measurements which are necessary for the QKD protocol are assumed to be perfect. Thus, the secret key rate presented here represents an upper bound and, depending on the particular setup adopted for these measurements, it should be multiplied by the square of the detector efficiency.

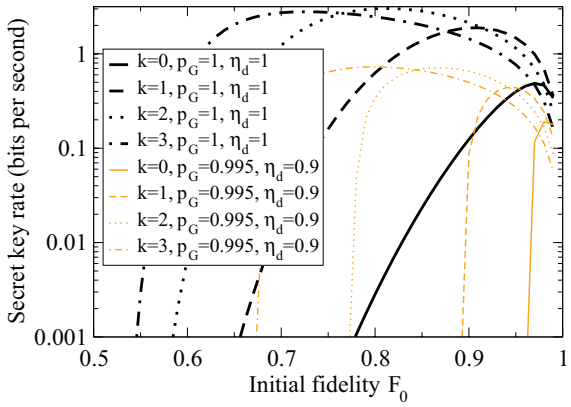


FIG. 9. (Color online) Hybrid quantum repeater with perfect quantum operations ($p_G = 1$) and perfect detectors ($\eta_d = 1$) (black lines) compared to imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_d = 0.9$) (orange lines): Secret key rate per second Eq. (26) as a function of the initial fidelity for 2^3 segments ($N = 3$) and various rounds of distillation k. The distance between Alice and Bob is 600 km.

The secret key rate. Figure 9 shows the secret key rate for 2^3 segments ($N = 3$) for various rounds of distillation. We see from the figure that for the HQR the secret key rate is not a monotonic function of the initial fidelity. The reason is that increasing F_0 decreases P_0 [see Eq. (23)] and vice versa. We find that the optimal initial fidelity, i.e., the fidelity where the secret key rate is maximal, increases as the maximal number of segments increases (see Table III). On the other hand, examining the optimal initial fidelity as a function of the distance, it turns out that it is almost constant for $L > 100$ km. Thus, for such distances, it is neither useful nor necessary to produce higher fidelities, because these would not make it possible to increase the secret key rate.

We also observe that the maximum of the initial fidelity is quite broad for small N, and gets narrower as N increases. If we now consider perfect gates and perfect detectors, we

[8]Note that this error model is considering a CZ gate operation. For a CNOT gate, Z errors can be transformed into X errors.

[9]Note that we assume perfect qubit measurements for the distillation and the swapping, but imperfect two-qubit gates. In principle, these qubit measurements can be done using a local qubus and homodyne measurement [54]. In this case, losses in the qubit measurement can be absorbed into losses of the gates. On the other hand, if we consider imperfect detectors for the qubit measurement then entanglement swapping will succeed with probability given by Eq. (B5).

TABLE III. Hybrid quantum repeater without imperfections ($p_G = 1$ and $\eta_d = 1$): Initial fidelity F_0 that maximizes the secret key rate in Eq. (26) for a given number 2^N of segments and k rounds of distillation.

N \ k	0	1	2	3
1	0.898	0.836	0.765	0.705
2	0.946	0.876	0.788	0.715
3	0.972	0.907	0.812	0.726
4	0.986	0.931	0.834	0.741

see that by fixing a certain secret key rate, we can reach this value with lower initial fidelities by performing distillation. Furthermore, by distilling the initial entanglement, we can even exceed the optimal secret key rate without distillation by one order of magnitude. However, note that distillation for k rounds requires 2^k memories at each side. If we then assume that we choose the protocol with no distillation and perform it in parallel 2^k times, i.e., we use the same amount of memories as for the scheme including distillation, the secret key rate without distillation (as shown in Fig. 9) should be multiplied by 2^k. As a result, the total secret key rate can then be even higher than that obtained with distillation.

Let us now assess the impact of the gate and detector imperfections on the secret key rate (orange lines) in Fig. 9. We notice that p_G has a large impact even if it is only changed by a small amount, like here from $p_G = 1$ to $p_G = 0.995$; the secret key rates drop by one order of magnitude. Imperfect detectors are employed in the creation of entanglement. As we see in Fig. 10, imperfect detectors do not affect the secret key rate significantly. As for $N = 3$ and $k = 0$, improving the detector efficiency from 0.5 to 1 leads to a doubling of the secret key rate. We conclude that for the HQR, the final secret key rates are much more sensitive to the presence of gate errors than to inefficiencies of the detectors. However, recall that in our analysis, we only take into account detector imperfections that occur during the initial USD-based entanglement distribution.

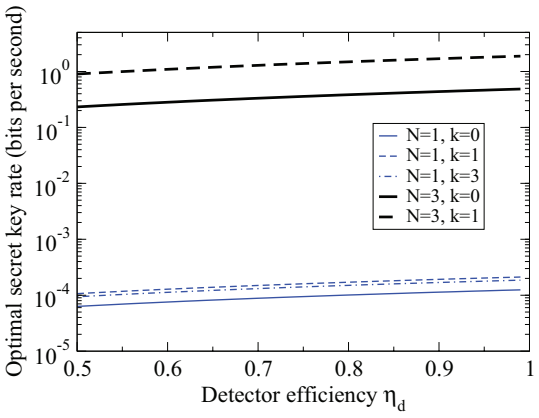


FIG. 10. (Color online) Hybrid quantum repeater with perfect gates ($p_G = 1$): The optimal secret key rate Eq. (26) for the BB84 protocol in terms of the detector efficiency η_d for the distance $L = 600$ km with various numbers of segments 2^N and rounds of distillation k.

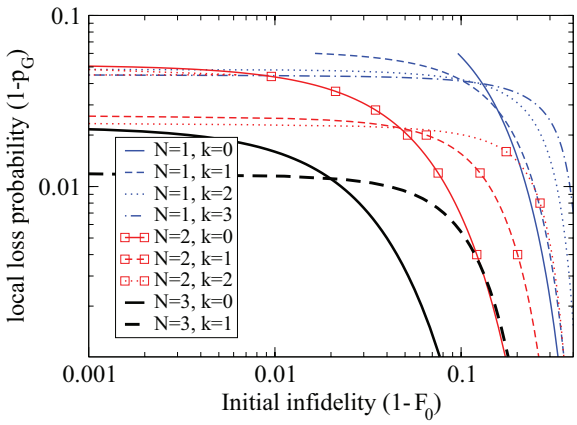


FIG. 11. (Color online) Hybrid quantum repeater with distillation and imperfections: Maximally allowed infidelity $(1 - F_0)$ as a function of the local loss probability $(1 - p_G)$ for various maximal numbers of segments 2^N and rounds of distillation k (distance: $L = 600$ km). Above the curves it is no longer possible to extract a secret key. The lines with $k = 0$ correspond to entanglement swapping without distillation.

For simplicity, any measurements on the memory qubits performed in the local circuits for swapping and distillation are assumed to be perfect, whereas the corresponding two-qubit gates for swapping and distillation are modeled as imperfect quantum operations (see footnote for more details).

Minimally required parameters. As we have seen in the previous section, it is also worth finding the minimal parameters for F_0 and p_G, for which we can extract a secret key. Figure 11 shows the initial infidelity required for extracting a secret key as a function of the local loss probability p_G, which was introduced in Sec. IV A2. We obtain also the minimal values of the local transmission probability $p_{G,N}^{\min}$ without distillation (solid lines in Fig. 11). If $p_G < p_{G,N}^{\min}$, then it is no longer possible to extract a secret key. As shown in Fig. 11, these minimal values (for which the minimal initial fidelity becomes $F_0 = 1$, without distillation) are $p_{G,1}^{\min} = 0.853$ (not shown in the plot), $p_{G,2}^{\min} = 0.948$, $p_{G,3}^{\min} = 0.977$, and $p_{G,4}^{\min} = 0.989$ (not shown in the plot). When including distillation, we can extend the regime of nonzero secret key rate to smaller initial fidelities at the cost of better local transmission probabilities. So there is a trade-off: If we can produce almost perfect Bell pairs, that is, initial states with high fidelities F_0, we can afford larger gate errors. Conversely, if high-quality gates are available, we may operate the repeater with initial states having a lower fidelity. Note that these results and Fig. 11 do not depend on the length of each segment in the quantum repeater, but only on the number of segments.

In Fig. 12 we plotted the optimal secret key rate for a fixed local transmission probability p_G and detector efficiency η_d in terms of the total distance L. We varied the number of segments 2^N and the number of distillation rounds k. We observe that a high value of k is not always advantageous: There exists for every N an optimal k, for which we obtain the highest key rate. We see, for example, that for $N = 1$, the optimal choice is $k = 2$, whereas for $N = 3$, the optimal k is 3. One can also see that there are distances, where it is advantageous to double the number of segments if one wants to avoid distillation, as,

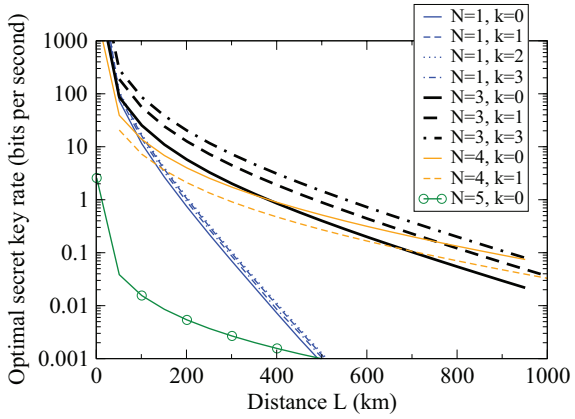


FIG. 12. (Color online) Hybrid quantum repeater with imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_d = 0.9$): Optimal secret key rate Eq. (26) for the BB84 protocol as a function of the total distance L, for various numbers of segments 2^N and rounds of distillation k. For $N = 5$, it is not possible to obtain a secret key when distillation is applied.

for example, for $N = 3$ and $N = 4$ at a distance of around 750 km.

V. QUANTUM REPEATERS BASED ON ATOMIC ENSEMBLES

Probably the most influential proposal for a practical realization of quantum repeaters was made in [12] and it is known as the DLCZ protocol. These authors suggested to use atomic ensembles as quantum memories and linear optics combined with single-photon detection for entanglement distribution, swapping, and (built-in) distillation. This proposal influenced experiments and theoretical investigations and led to improved protocols based on atomic ensembles and linear optics (see [25] for a recent review).

To our knowledge, the most efficient scheme based on atomic ensembles and linear optics was proposed very recently by Minář *et al.* [23]. These authors suggest to use heralded qubit amplifiers [58] to produce entanglement on demand and then to extend it using entanglement swapping based on two-photon detections. The state produced at the end of the protocol no longer contains vacuum components and therefore can be used directly for QKD. This is an improvement over the original DLCZ protocol in which the final long-distance pair is still contaminated by a fairly large vacuum term that accumulates during the imperfect storage and swapping processes.[10]

In this section, we first review the protocol proposed in [23] and then we analyze the role of the parameters and the performance in relation to QKD.

A. The setup

The protocol is organized in three logical steps. First, local entanglement is created in a repeater station, then it is distributed, and finally it is extended over the entire distance [23].

As a probabilistic entangled-pair source we consider spontaneous parametric down-conversion (SPDC) [61] which produces the state (see [23,62])[11]

$$\rho_{\text{pair}} := (1-p)\sum_{m=0}^{\infty}\frac{2^m p^m}{(m!)^2(m+1)}(B^\dagger)^m|0\rangle\langle 0|B^m, \quad (27)$$

where $B^\dagger := (g_H^\dagger \text{in}_H^\dagger + g_V^\dagger \text{in}_V^\dagger)/\sqrt{2}$. The operator $g_i^\dagger$ ($\text{in}_i^\dagger$) denotes a spatial mode with polarization given by $i = H,V$. The *pump parameter* p is related to the probability to have an n-photon pulse by $P(n) = p^n(1-p)$.

A probabilistic single-photon source with efficiency q produces states of the form

$$\rho_{\text{single}}^i := (1-q)\,|0\rangle\,\langle 0| + q a_i^\dagger\,|0\rangle\,\langle 0|\,a_i, \quad (28)$$

where $a_i^\dagger$ (a_i) is the creation (annihilation) operator of a photon with polarization $i = H,V$.

We also define by γ_{rep} the smallest repetition rate among the repetition rates of the SPDC source and the single-photon sources.

1. *On-demand entanglement source*

The protocol that produces local entangled pairs works as follows (see Fig. 13 and [23] for additional details).

(1) The state $\rho_{\text{pair}} \otimes \rho_{\text{single}}^H \otimes \rho_{\text{single}}^V$ is produced.

(2) The single photons, which are in the same spatial mode, are sent through a tunable beam splitter of reflectivity R corresponding to the transformation $a_i \to \sqrt{R}c_i + \sqrt{1-R}\text{out}_i$.

(3) The spatial modes in and c are sent through a linear-optics network which is part of the heralded qubit amplifiers, and the following transformations are realized,

$$c_H \to \frac{d_3 + d_4 + d_2 - d_1}{2},$$
$$c_V \to \frac{d_3 + d_4 - d_2 + d_1}{2},$$
$$\text{in}_H \to \frac{d_2 + d_1 + d_3 - d_4}{2},$$
$$\text{in}_V \to \frac{d_2 + d_1 - d_3 + d_4}{2},$$

where d_1, d_2, d_3, d_4 are four spatial modes, corresponding to the four detectors.

(4) A twofold coincidence detection between d_1 and d_3 (or d_1 and d_4 or d_2 and d_3 or d_2 and d_4) projects the modes g and out onto an entangled state. These are the heralding events that acknowledge the storage of an entangled pair in the

[10] Very recently it was shown that in the context of QKD over continuous variables, an effective suppression of channel losses and imperfections can also be achieved via a virtual, heralded amplification on the level of the classical postprocessing [59,60]. In this case, it is not even necessary to physically realize a heralded amplifier.

[11] In our calculation, similar to [23], we consider only those terms with $m \leqslant 2$. The reason is that the contribution to the total trace of the first three terms is given by $1 - p^3$ and therefore for $p < 0.1$ the state obtained by considering only the first three terms differs in a negligible way from the full state.

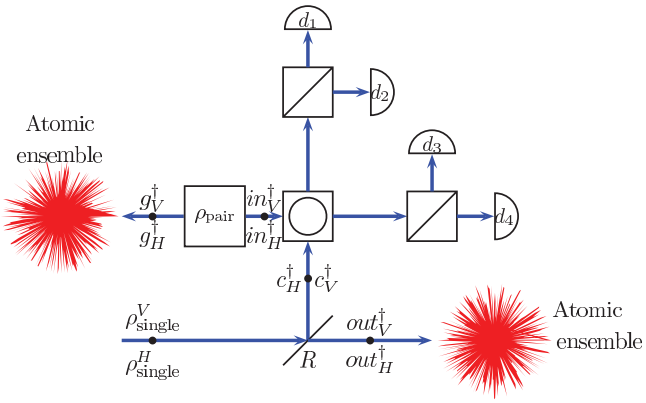


FIG. 13. (Color online) Quantum repeater based on atomic ensembles: Setup for creation of on-demand entanglement (see also [23]). The whole setup is situated at one physical location. A pair source produces the state ρ_{pair}. One part of the pair (the mode g) is stored in an atomic ensemble and the other part (mode in) goes into a linear-optics network. A single-photon source produces the states ρ^H_{single} and ρ^V_{single} which go through a beam splitter of reflectivity R. The output modes of the beam splitter are called c and out. The mode out is stored in a quantum memory and the mode c goes into a linear-optics network which is composed of a polarizing beam splitter in the diagonal basis $\pm 45^\circ$ (square with a circle inside), two polarizing beam splitters in the rectilinear basis (square with a diagonal line inside), and four detectors.

quantum memories out and g.The probability of a successful measurement is given by

$$P_0^s(p,q,R,\eta_{\text{d}}) = 4\text{tr}\big(\Pi^{(1)}_{d_1}(\eta_{\text{d}})\Pi^{(0)}_{d_2}(\eta_{\text{d}})\Pi^{(1)}_{d_3}(\eta_{\text{d}})\Pi^{(0)}_{d_4}(\eta_{\text{d}})\rho'_{g,\text{out},d_1,d_2,d_3,d_4}\big), \tag{29}$$

where $\rho'_{g,\text{out},d_1,d_2,d_3,d_4}$ is the total state obtained at the end of step (iii) and the superscript s stands for source. The POVM for the detectors has been defined in Eq. (2). The factor 4 accounts for the fact that there are four possible twofold coincidences. The resulting state is

$$\rho_0^s(p,q,R,\eta_{\text{d}}) = \frac{4}{P_0^s}\text{tr}_{d_1,d_2,d_3,d_4}\big(\Pi^{(1)}_{d_1}(\eta_{\text{d}})\Pi^{(0)}_{d_2}(\eta_{\text{d}})\Pi^{(1)}_{d_3}(\eta_{\text{d}}) \times \Pi^{(0)}_{d_4}(\eta_{\text{d}})\rho'_{g,\text{out},d_1,d_2,d_3,d_4}\big). \tag{30}$$

This is the locally prepared state that will be distributed between the repeater stations. In the ideal case with perfect detectors and perfect single-photon sources, the resulting state (after a suitable rotation) is $\rho_0^s = |\phi^+\rangle\langle\phi^+|$, which can be obtained with probability $P_0^s = pR(1-R)$. In the realistic case, however, additional higher-order excitations are present. In [23], the explicit form of ρ_0^s and P_0^s can be found for the case when $1 > R \gg p$ and $1 \gg 1-q$.

Therefore, we have seen that the protocol proposed in [23] makes it possible to turn a probabilistic entangled-pair source (SPDC in our case) into an on-demand entangled photon source. In this context *on-demand* means that when a heralding event is obtained then it is known for sure that an entangled quantum state is stored in the quantum memories out and g.

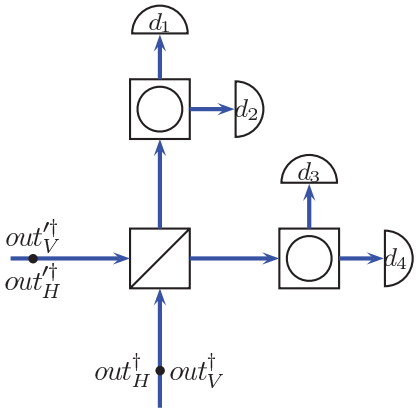


FIG. 14. (Color online) Quantum repeater based on atomic ensembles: Setup used for entanglement distribution (swapping) (see [23] for additional details). The modes out and out' are released from two quantum memories separated by distance L_0 (or located at the same station for the case of swapping) and sent into a linear-optics network consisting of one polarizing beam splitter in the rectilinear basis (square with diagonal line inside), two polarizing beam splitters in the diagonal basis (square with circle inside), and four detectors.

2. *Entanglement distribution and swapping*

Once local entangled states are created, it is necessary to distribute the entanglement over segments of length L_0 and then to perform entanglement swapping. Both procedures are achieved in a similar way (see Fig. 14), as we describe in this section. Entanglement distribution is done as follows (see Fig. 14 and [23] for additional details).

(1) Each of the two adjacent stations create a state of the form ρ_0^s. We call g and out the modes belonging to the first station and g' and out' the modes of the second station.

(2) The modes out and out' are read out from the quantum memories and sent through an optical fiber to a central station where a linear-optics network is used in order to perform entanglement swapping. The transformations of the modes are as follows:

$$\text{out}_H \to \frac{d_3+d_4}{\sqrt{2}}, \quad \text{out}_V \to \frac{d_1-d_2}{\sqrt{2}},$$
$$\text{out}'_H \to \frac{d_1+d_2}{\sqrt{2}}, \quad \text{out}'_V \to \frac{d_3-d_4}{\sqrt{2}},$$

where d_1, d_2, d_3, and d_4 are four spatial modes.

(3) A twofold coincidence detection between d_1 and d_3 (or d_1 and d_4 or d_2 and d_3 or d_2 and d_4) projects the modes out and out' onto an entangled state. The probability of this event is given by

$$P_0(p,q,R,\eta_{\text{d}},\eta_{mtd}) = 4\text{tr}\big(\Pi^{(1)}_{d_1}(\eta_{mtd})\Pi^{(0)}_{d_2}(\eta_{mtd})\Pi^{(1)}_{d_3}(\eta_{mtd}) \times \Pi^{(0)}_{d_4}(\eta_{mtd})\rho'_{g,g',d_1,d_2,d_3,d_4}\big), \tag{31}$$

where $\rho'_{g,g',d_1,d_2,d_3,d_4}$ is the total state obtained at the end of step (ii) and $\eta_{mtd} := \eta_m\eta_t(\frac{L_0}{2})\eta_{\text{d}}$, with η_m being the probability that the quantum memory releases a photon. The factor 4 accounts for the fact that there are four possible twofold coincidences.

The resulting state is

$$\rho_{0,g,g'} = \frac{4}{P_0}\mathrm{tr}_{d_1,d_2,d_3,d_4}\big(\Pi^{(1)}_{d_1}(\eta_{mtd})\Pi^{(0)}_{d_2}(\eta_{mtd}) \times \Pi^{(1)}_{d_3}(\eta_{mtd})\Pi^{(0)}_{d_4}(\eta_{mtd})\rho'_{g,g',d_1,d_2,d_3,d_4}\big). \quad (32)$$

The state $\rho_{0,g,g'}$ is the entangled state shared between two adjacent stations over distance L_0. In order to perform entanglement swapping, the same steps as described above are repeated until those two stations separated by distance L are finally connected. Formally, the probability that entanglement swapping is successful in the nesting level n is given by

$$P^{(n)}_{ES}(p,q,R,\eta_{\mathrm{d}},\eta_{mtd}) = 4\mathrm{tr}\big(\Pi^{(1)}_{d_1}(\eta_{md})\Pi^{(0)}_{d_2}(\eta_{md})\Pi^{(1)}_{d_3}(\eta_{md}) \times \Pi^{(0)}_{d_4}(\eta_{md})\rho'_{n-1,g,g',d_1,d_2,d_3,d_4}\big), \quad (33)$$

where $\rho'_{n-1,g,g',d_1,d_2,d_3,d_4}$ is the total state resulting from steps (i) and (ii) described above in this section, and $\eta_{md} := \eta_m\eta_{\mathrm{d}}$.

The swapped state is given by

$$\rho_{k,g,g'} = \frac{4}{P^{(i)}_{ES}}\mathrm{tr}_{d_1,d_2,d_3,d_4}\big(\Pi^{(1)}_{d_1}(\eta_{md})\Pi^{(0)}_{d_2}(\eta_{md}) \times \Pi^{(1)}_{d_3}(\eta_{md})\Pi^{(0)}_{d_4}(\eta_{md})\rho'_{k-1,g,g',d_1,d_2,d_3,d_4}\big). \quad (34)$$

The state $\rho_{n,g,g'}$ is the state that will be used for QKD when $n = N$. In a regime where higher-order excitations can be neglected, the state $\rho_{n,g,g'}$ is a maximally entangled Bell state. In [23] is given the expression of the state $\rho_{n,g,g'}$ under the same assumptions on the reflectivity R and the efficiency q of the single-photon sources as discussed regarding ρ^s_0 in Eq. (30).

Given the final state $\rho_{AB} := \rho_{N,g,g'}$ it is possible to calculate P_{click} and the QBER, using the formalism of Sec. II B 3 and inserting η_{md} for the detector efficiency.

The final secret key rate then reads

$$R^{\mathrm{AE}}_{\mathrm{QKD}} = R_{\mathrm{REP}}(L_0,p,N,\eta_{\mathrm{d}},\eta_m,\gamma_{\mathrm{rep}},q)P_{\mathrm{click}}(L_0,p,N,\eta_{\mathrm{d}},\eta_m,q) \times R_{\mathrm{sift}}r^{\mathrm{BB84}}_{\infty}(L_0,p,N,\eta_{\mathrm{d}},\eta_m,q), \quad (35)$$

where R_{REP} is given by Eq. (8) with $\beta = 1$ for the communication time [see Fig. 2(c)]. As for the QKD protocol, we consider the asymmetric BB84 protocol ($R_{\mathrm{sift}} = 1$, see Sec. II B). The superscript AE stands for atomic ensembles.

Note that even though for the explicit calculations we used PNRD, the previous formulas hold for any type of measurement.

B. Performance in the presence of imperfections

As in the previous sections, we shall focus on the secret key rate. The free parameters are the pump parameter p and the reflectivity of the beam splitter R. In all plots, we optimize these parameters in such a way that the secret key rate is maximized. As all optimizations have been done numerically, our results may not correspond to the global maximum, but only to a local maximum. In general, we observed that if we treat the secret key rate as a function of p (calculated at the optimal R), the maximum of the secret key rate is rather narrow. On the other hand, when calculated as a function of R (at the optimal p), this maximum is quite broad.

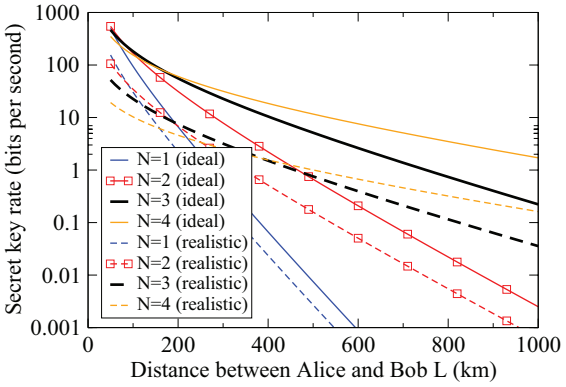


FIG. 15. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the distance between Alice and Bob. The secret key rate has been obtained by maximizing over p and R. Ideal setup (solid line) with parameters $\eta_m = \eta_{\mathrm{d}} = q = 1, \gamma_{\mathrm{rep}} = \infty$. More realistic setup (dashed line) with parameters $\eta_m = 1$, $\eta_{\mathrm{d}} = 0.9$, $q = 0.96$, $\gamma_{\mathrm{rep}} = 50$ MHz.

The most favorable scenario (ideal case) is characterized by perfect detectors ($\eta_{\mathrm{d}} = 1$), perfect quantum memories ($\eta_m = 1$), and deterministic single-photon sources ($q = 1$) which can emit photons at an arbitrarily high rate ($\gamma_{\mathrm{rep}} = \infty$). In this case, the heralded qubit amplifier is assumed to be able to create perfect Bell states and the secret fraction therefore becomes one. The only contribution to the secret key rate is then given by the repeater rate. In Fig. 15 the optimal secret key rate versus the distance, obtained by maximizing over p and R, is shown (see solid lines).

For the calculation of Fig. 15, we have assumed that the creation of local entanglement, i.e., of state ρ^s_0, is so fast that we can neglect the creation time. In the case of SPDC, the repetition rate of the source is related to the pump parameter p and, moreover, the single-photon sources also have finite generation rates that should be taken into account. For this purpose, we introduce the photon-pair preparation time which is given by $T^s_0 = \frac{1}{\gamma_{\mathrm{rep}}P^s_0}$ [23]. The formula for the repeater rate in this case corresponds to Eq. (8) with $T_0 \to T_0 + T^s_0$. As shown in Fig. 16, when $\eta_{\mathrm{d}} = 1$ the secret key rate is

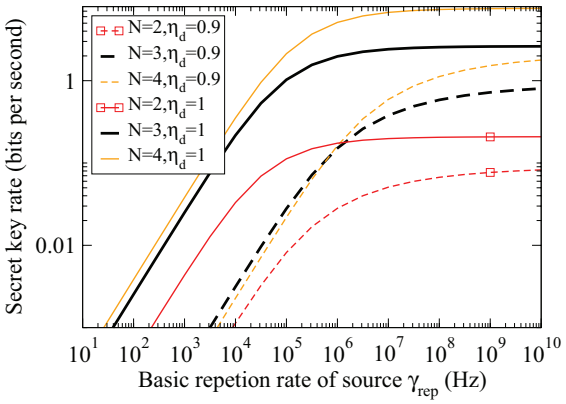


FIG. 16. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the basic repetition rate of the source γ_{rep}. The secret key rate has been obtained by maximizing over p and R (parameters: $\eta_{\mathrm{d}} = \eta_m = q = 1$).

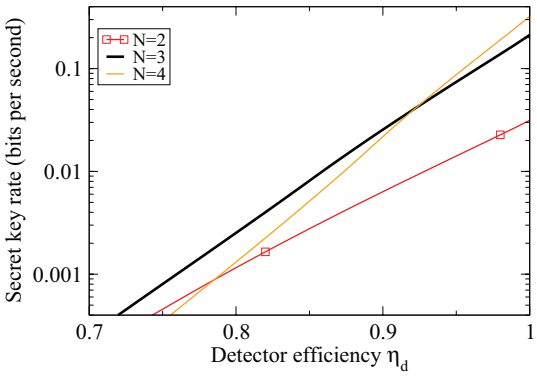


FIG. 17. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the efficiency of the detectors $\eta_{\rm d}$. The secret key rate has been obtained by maximizing over p and R (parameters: $\eta_m = q = 1$, $\gamma_{\rm rep} = 50$ MHz, $L = 600$ km).

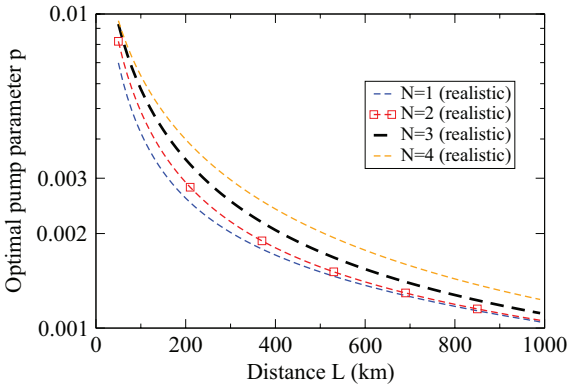


FIG. 19. (Color online) Quantum repeaters based on atomic ensembles: Optimal value of p versus the distance between Alice and Bob. The corresponding secret key rate is shown in Fig. 15 (parameters: $\eta_m = 1$, $\eta_D = 0.9$, $q = 0.96$, $\gamma_{\rm rep} = 50$ MHz, $L = 600$ km).

constant for $\gamma_{\rm rep} > 10^7$; however, for realistic detectors with $\eta_{\rm d} = 0.9$, much higher repetition rates are required in order to reach the asymptotic value. Nowadays, SPDC sources reach a rate of about 100 MHz, whereas single-photon sources have a repetition rate of a few MHz [52]. Recently, a new single-photon source with repetition rate of 50 MHz has been realized [63]. In the following, we employ $\gamma_{\rm rep} = 50$ MHz.

A consequence of imperfect detectors is that multiphoton pulses contribute to the final state. The protocol we are considering here is less robust against detector inefficiencies than the original DLCZ protocol. This is due to the fact that successful entanglement swapping is conditioned on twofold detection as compared to one-photon detection of the DLCZ protocol. However, twofold detections make it possible to eliminate the vacuum in the memories [25], thus increasing the final secret key rate. As shown in Fig. 17, the secret key rate spans four orders of magnitude as $\eta_{\rm d}$ increases from 0.7 to 1. Thus, an improvement of the detector efficiency causes a considerable increase of the secret key rate. For example, for $N = 3$, an improvement from $\eta_{\rm d} = 0.85$ to $\eta_{\rm d} = 0.88$ leads to a threefold increase of the secret key rate. Notice that we have considered photon detectors which are able to resolve photon numbers. Photon detectors with an efficiency as high as 95% have been realized [64]. These detectors work at the telecom bandwidth of 1556 nm and they have negligible dark counts. The drawback is that they need to operate at very low temperatures of 100 mK. The reading efficiency of the quantum memory η_m plays a similar role as the detector efficiency. In accordance with [25], intrinsic quantum memory efficiencies above 80% have been realized [65]; however, total efficiencies where coupling losses are included are much lower.

A single-photon source is also characterized by its efficiency, i.e., the probability q to emit a photon. As shown in Fig. 18, we see that it is necessary to have single-photon sources with high efficiencies, in particular, when detectors are imperfect. The source proposed in [63] reaches $q = 0.96$.

In Fig. 15 we show the secret key rate as a function of the distance between Alice and Bob for parameters (dashed lines) which are optimistic in the sense that they could be possibly reached in the near future. We observe that with an imperfect setup and for $N = 4$, the realistic secret key rate is by one order of magnitude smaller than the ideal value. This decrease is mainly due to finite detector efficiencies. For

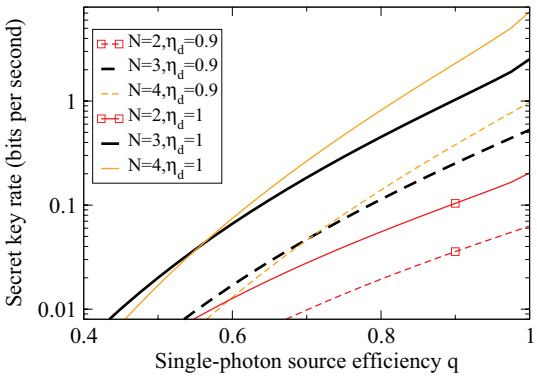


FIG. 18. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the probability to emit a single photon. The secret key rate has been obtained by maximizing over p and R (parameters: $\eta_m = 1, \gamma_{\rm rep} = 50$ MHz, $L = 600$ km).

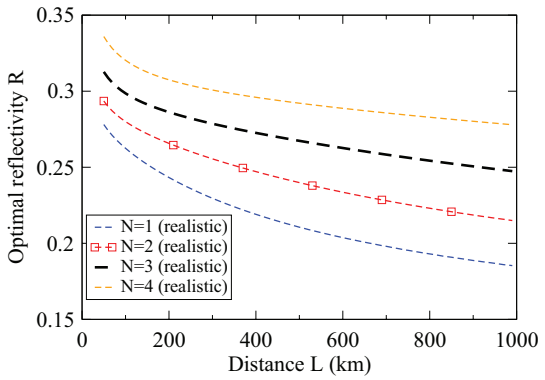


FIG. 20. (Color online) Quantum repeaters based on atomic ensembles: Optimal value of the reflectivity R versus the distance between Alice and Bob. The corresponding secret key rate is shown in Fig. 15 (parameters: $\eta_m = 1, \eta_D = 0.9, q = 0.96, \gamma_{\rm rep} = 50$ MHz).

$N = 4$, the secret key rate scales proportionally to $\eta_d^2\eta_d^2\eta_d^{2\cdot4}\eta_d^2$ (local creation, distribution, entanglement swapping, and QKD measurement). For $\eta_d = 0.9$, finite detector efficiencies lead to a decrease of the secret key rate by 78%. Regarding the optimal pump parameter p, we observe in Fig. 19 that for large distances ($L > 600$ km) its value is about 0.15%. The order of magnitude of this value is in agreement with the results found in [20] regarding the original DLCZ protocol and the BB84 protocol.

The optimal reflectivity R is given in Fig. 20. We observe that as N increases, the optimal value of R has a modest increase.

VI. CONCLUSIONS AND OUTLOOK

Quantum repeaters represent nowadays the most promising and advanced approach to create long-distance entanglement. Quantum key distribution is a developed technology which has already reached the market. One of the main limitations of current QKD is that the two parties have a maximal separation of 150 km, due to losses in optical fibers. In this paper, we have studied long-distance QKD by using quantum repeaters.

We have studied three of the main protocols for quantum repeaters, namely, the original protocol, the HQR, and a variation of the so-called DLCZ protocol. Our analysis differs from previous treatments, in which only final fidelities have been investigated, because we maximize the main figure of merit for QKD, the secret key rate. Such an optimization is nontrivial, since there is a trade-off between the repeater pair-generation rate and the secret fraction: The former typically decreases when the final fidelity grows, whereas the latter increases when the final fidelity becomes larger. Our analysis makes it possible to calculate secret key rates under the assumption of a single repeater chain with at most 2^k quantum memories per half station for respectively k distillation rounds occurring strictly before the swappings start. The use of additional memories when parallelizing or even multiplexing several such repeater chains as well as the use of additional quantum error detection or even correction will certainly improve these rates, but also render the experimental realization much more difficult.

The comparison of different protocols is highly subjective, as there are different experimental requirements and difficulties for each of them; therefore, here we investigated the main aspects for every protocol separately.

The general type of quantum repeater is a kind of prototype for a quantum repeater based on the original proposal [7]. We have provided an estimate of the experimental parameters needed to extract a secret key and showed what the role of each parameter is. We have found that the requirement on the initial fidelity is not so strong if distillation is allowed. However, quantum gates need to be very good (errors of the order of 1%).

Further, we have studied the HQR. This protocol makes it possible to perform both the initial entanglement distribution and the entanglement swapping with high efficiencies. The reason is that bright light sources are used for communication and cavity quantum electrodynamics (CQED) interactions are employed for the local quantum gates, making the swapping, in principle, deterministic. Using PNRDs, we have derived explicit formulas for the initial fidelity and the probability of success for entanglement distribution. Furthermore, we have found the form of the states after entanglement swapping and entanglement distribution in the presence of gate errors. We have seen that finite detector efficiencies do not play a major role regarding the generation probability. This makes it possible to have high secret key rates in a setup where it is possible to neglect imperfections of the detectors. By studying imperfect gates we found that excellent gates are necessary (errors of the order of 0.1%).

Finally, we have considered repeaters with atomic ensembles and linear optics. There exist many experimental proposals and therefore we have studied the scheme which is believed to be the fastest [23]. This scheme uses heralded qubit amplifiers for creating dual-rail encoded entanglement and entanglement swapping based on twofold detection events. In contrast to the previous two schemes, the Bell measurement used for entanglement swapping is not able to distinguish all four Bell states. We have characterized all common imperfections and we have seen that using present technology, the performance of this type of quantum repeater in terms of secret key rates is only about one order of magnitude different from the corresponding ideal setup. Thus, this scheme seems robust against most imperfections. These types of repeater schemes, as currently being restricted to linear optics, could still be potentially improved by allowing for additional nonlinear-optics elements. This may render the entanglement swapping steps deterministic, similar to the HQR using CQED, and thus further enhance the secret key rates.

For the protocols considered here, single-qubit rotations were assumed to be perfect. Obviously, this assumption is not correct in any realistic situation. However, most of these single-qubit rotations can be replaced by simple bit flips of the classical outcomes which are used when the QKD protocol starts. Therefore, we see that in this case, specifically building a quantum repeater for QKD applications permits to relax the requirements on certain operations that otherwise must be satisfied for a more general quantum application, such as distributed quantum computation.

As an outlook our analysis can be extended in various directions: In our work we have considered standard QKD, in which Alice and Bob trust their measurement devices. To be more realistic, it is possible to relax this assumption and to consider device-independent quantum key distribution (DI-QKD) [1–5]. An analysis of the performance of long-distance DI-QKD can also be done using the methods that we developed in this paper.

A possible continuation of our work is the analysis of multiplexing [25,46]. It has been shown that this technique has significant advantage in terms of the decoherence time required by the quantum memories. On the other hand, it produces only a moderate increase of the repeater rate [25,66,67]. Possible future analyses include the effect on the secret key rate by distilling in all nesting levels [24] or by optimizing the repeater protocol as done in Refs. [68,69]. Moreover, other repeater protocols which are based on quantum error correction codes [70–72] may help to increase the secret key rate.

ACKNOWLEDGMENTS

The authors acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, Project

QuOReP). The authors would like to thank the organizers and participants of the quantum repeater workshops (Project QuOReP) held in Hannover and Bad Honnef. N.K.B. and P.v.L. thank the Emmy Noether Program of the Deutsche Forschungsgemeinschaft for financial support. S.A. thanks J. Minář for enlightening discussions and insightful comments.

APPENDIX A: ADDITIONAL MATERIAL FOR THE GENERAL FRAMEWORK

1. Generation rate with probabilistic entanglement swapping and distillation

In this Appendix, we give the derivation of Eq. (8) in Sec. II A2, which describes the generation rate of entangled pairs per time unit T_0 with probabilistic entanglement swapping and distillation; i.e.,

$$R_{\mathrm{REP}}^{\mathrm{prob}} = \frac{1}{T_0}\left(\frac{2}{3a}\right)^{N+k} P_0 P_{ES}^{(1)} P_{ES}^{(2)} \cdots P_{ES}^{(N)} \prod_{i=1}^{k} P_D[i]. \quad \text{(A1)}$$

In [25] the formula has been derived only for the case without distillation and there it reads as

$$R_{\mathrm{REP}}^{\mathrm{prob}} = \frac{1}{T_0}\left(\frac{2}{3}\right)^{N} P_0 P_{ES}^{(1)} P_{ES}^{(2)} \cdots P_{ES}^{(N)}, \quad \text{(A2)}$$

where P_0 is the probability to generate a pair for entanglement swapping. This formula was derived for small P_0.

In order to incorporate distillation into Eq. (A2) we use the definition of the recursive probability $P_{L_0}[k]$ given in Eq. (6); see [35]. It describes the generation probability of an entangled pair after k rounds of purification. If we choose an appropriate $a < 1$ such that $Z_1(x) = \frac{3-2x}{x(2-x)} \geqslant \frac{3}{2x}a$, we can rewrite $P_{L_0}[k]$,

$$\begin{aligned} P_{L_0}[k] &= \frac{P_D[k]}{Z_1(P_{L_0}[k-1])} \leqslant \frac{2}{3a} P_D[k] P_{L_0}[k-1] \\ &= \frac{2}{3a} P_D[k] \frac{P_D[k-1]}{Z_1(P_{L_0}[k-2])} \\ &\leqslant \cdots \leqslant \left(\frac{2}{3a}\right)^{k} P_0 \prod_{i=1}^{k} P_D[i], \end{aligned} \quad \text{(A3)}$$

where in the last line $P_{L_0}[k]$ is a recursive formula. For deriving Eq. (A1), we replace in Eq. (A2) P_0 with P_{L_0} and we use Eq. (A3).

For the plots we have $L = 600$ km and usually $\eta_d = 0.9$, which leads to $P_{L_0}[k] \leqslant 0.037$ and $a \leqslant 0.994$.

APPENDIX B: ADDITIONAL MATERIAL FOR THE ORIGINAL QUANTUM REPEATER

1. Entanglement swapping

In this Appendix we present the formulas of the state after entanglement swapping and the distillation protocol. Moreover, we bound also the role of dark counts in the entanglement swapping probability.

(a) The protocol

We consider the total state $\rho_{ab} \otimes \rho_{cd}$. The entanglement swapping algorithm consists of the following steps.

(1) A CNOT is applied on system b as source and c as target.

(2) One output system is measured in the computational basis and the other one in the basis $\{|+\rangle := \frac{|H\rangle+|V\rangle}{\sqrt{2}}, |-\rangle = \frac{|H\rangle-|V\rangle}{\sqrt{2}}\}$, obtained by applying a Hadamard gate.

(3) In the standard entanglement swapping algorithm, a single qubit rotation depending on the outcome of the measurement is performed. However, for the purpose of QKD it is not necessary to do this single-qubit rotation.[12] We propose that Bob collects the results of the Bell measurements, performs the standard QKD measurement and then he can apply a classical bit flip depending on the QKD measurement basis and on the Bell measurement outcomes.

(b) Formulas in the presence of imperfections

We consider a setup with two detectors d_1 and d_2. We associate the detection pattern of these two detectors with a two-dimensional Hilbert space, e.g., $d_1 =$ click, $d_2 =$ noclick $\Rightarrow |H\rangle = |1_{d_1}, 0_{d_2}\rangle$ and $d_1 =$ no click, $d_2 =$ click $\Rightarrow |V\rangle = |0_{d_1}, 1_{d_2}\rangle$, where $\{|H\rangle, |V\rangle\}$ are a basis of a two-dimensional Hilbert space which can be, for example, identified with horizontal and vertical polarizations of a qubit. We discard those events where there are no clicks or when both detectors click. If the detectors are imperfect, we may have an error in the detection of the quantum state. The POVM consists of two elements Π_H (Π_V) which detect mode $|H\rangle$ ($|V\rangle$):

$$\Pi_H := \gamma\, |H\rangle\langle H| + (1-\gamma)\, |V\rangle\langle V|, \quad \text{(B1)}$$

$$\Pi_V := \gamma\, |V\rangle\langle V| + (1-\gamma)\, |H\rangle\langle H|, \quad \text{(B2)}$$

with

$$\gamma := \frac{\eta_{\mathrm{d}} + p_{\mathrm{dark}}(1-\eta_{\mathrm{d}})}{\eta_{\mathrm{d}} + 2p_{\mathrm{dark}}(1-\eta_{\mathrm{d}})}, \quad \text{(B3)}$$

where p_{dark} is the dark count probability of the detectors and η_{d} is their efficiency.[13]

The POVM above has been used also in [7,73]; however, the connection with the imperfections of the detectors was not made.

---

[12] Note that this step is different from [7], where the single-qubit rotations were explicitly included.

[13] The coefficient γ can be calculated as follows. The POVM for having a click under the assumption of single-photon sources and imperfect detectors is given by

$$E^{(\mathrm{click})} = p_{\mathrm{dark}}\, |0\rangle\langle 0| + (1 - (1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}}))\, |1\rangle\langle 1|$$

and that for no click is given by

$$E^{(\mathrm{noclick})} = (1-p_{\mathrm{dark}})\, |0\rangle\langle 0| + (1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}})\, |1\rangle\langle 1|.$$

When we say that the detector a clicked, and b did not click and we discard the vacuum events, and those where both detectors clicked, the POVM looks as follows:

$$\begin{aligned} &E_a^{(\mathrm{click})} \otimes E_b^{(\mathrm{noclick})} \\ &\quad = [1-(1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}})](1-p_{\mathrm{dark}})\, |1_a, 0_b\rangle\langle 1_a, 0_b| \\ &\qquad + p_{\mathrm{dark}}(1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}})\, |0_a, 1_b\rangle\langle 0_a, 1_b|. \end{aligned}$$

The trace is $(1-p_{\mathrm{dark}})[\eta_{\mathrm{d}} + 2p_{\mathrm{dark}}(1-\eta_{\mathrm{d}})]$, which is exactly the probability that we have this measurement. If we normalize this measurement and relate it to the POVM in Eq. (B1), we get γ.

If we start with the states $\rho_{ab} = \rho_{cd} = A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|$, the resulting state after entanglement swapping between a and d is still a Bell diagonal state with coefficients of the form [74]

$$\begin{aligned}
A' &= \frac{1-p_G}{4} + p_G[\gamma^2(A^2+B^2+C^2+D^2) + 2(1-\gamma)^2(AD+BC) + 2\gamma(1-\gamma)(A+D)(C+B)],\\
B' &= \frac{1-p_G}{4} + p_G[2\gamma^2(AB+CD) + 2(1-\gamma)^2(AC+BD) + \gamma(1-\gamma)(A^2+B^2+C^2+D^2+2AD+2BC)],\\
C' &= \frac{1-p_G}{4} + p_G[2\gamma^2(AC+BD) + 2(1-\gamma)^2(AB+CD) + \gamma(1-\gamma)(A^2+B^2+C^2+D^2+2AD+2BC)],\\
D' &= \frac{1-p_G}{4} + p_G[2\gamma^2(AD+BC) + (1-\gamma)^2(A^2+B^2+C^2+D^2) + 2\gamma(1-\gamma)(A+D)(B+C)],
\end{aligned} \tag{B4}$$

and the probability to obtain the state above is equal to

$$P_{ES}(\eta_{\rm d}, p_{\rm dark}) := \{[1-p_{\rm dark}][\eta_{\rm d} + 2p_{\rm dark}(1-\eta_{\rm d})]\}^2, \tag{B5}$$

which can be interpreted as the probability that entanglement swapping is successful.[14] Note that $P(\eta,0) = \eta^2$ and $P(1,0) = 1$ as we expect. When we consider dark counts $p_{\rm dark} < 10^{-5}$, then these are negligible as $(P_{ES}(0.1,10^{-5})/(P_{ES}(0.1,0)))^N < 1.03^N$, so the impact on the secret key rate is minimal. Note that we open the gates only for a short time window, which is the interval of time where we expect the arrival of a photon. The dark count probability $p_{\rm dark}$ represents the probability that in the involved time window the detector gets a dark count.

2. Distillation

(a) The protocol

We assume that Alice and Bob hold two Bell diagonal states ρ_{a_1,b_1} and ρ_{a_2,b_2}. The algorithm is as follows.

(1) In the computational basis, Alice rotates her particles by $\frac{\pi}{2}$ about the X-axis, whereas Bob applies the inverse rotation $(-\frac{\pi}{2})$ on his particles.

(2) Then they apply on both sides a CNOT operation, where the states a_1 (b_1) serve as source and a_2 (b_2) as target.

(3) The states corresponding to the target are measured in the computational basis. If the measurement results coincide, the resulting state ρ_{a_1,b_1} is a purified state; otherwise, the resulting state is discarded. Therefore, this entanglement distillation scheme is probabilistic.

(b) Formulas in the presence of imperfections

Given a Bell diagonal state with the coefficients

$$\begin{aligned}
\rho_{ab} = {} & A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+|\\
& + D|\psi^-\rangle\langle\psi^-|,
\end{aligned} \tag{B6}$$

the coefficients transform according to the map [30]

$$A' = \frac{1}{P_D}(A^2 + D^2), \tag{B7}$$

$$B' = \frac{1}{P_D}(2AD), \tag{B8}$$

$$C' = \frac{1}{P_D}(B^2 + C^2), \tag{B9}$$

$$D' = \frac{1}{P_D}(2BC), \tag{B10}$$

where P_D is the probability that the measurement outcomes are both the same for Alice and Bob, and thus the probability of successful distillation is

$$P_D[k] = (A_{k-1} + D_{k-1})^2 + (B_{k-1} + C_{k-1})^2. \tag{B11}$$

Including the gate quality p_G, these formulas change to [74]

$$P_D[k] = \tfrac{1}{2}\left\{1 + p_G^2(-1 + 2A_{k-1} + 2D_{k-1})^2\right\}, \tag{B12}$$

with

$$\begin{aligned}
A' = {} & \left\{1 + p_G^2\left[(A-B-C+D)(3A+B\right.\right.\\
& \left.\left. + C + 3D) + 4(A-D)^2\right]\right\}/(8P_D),\\
B' = {} & \left\{1 - p_G^2\left[A^2 + 2A(B+C-7D)\right.\right.\\
& \left.\left. + (B+C+D)^2\right]\right\}/(8P_D),\\
C' = {} & \left\{1 + p_G^2\left[4(B-C)^2 - (A-B\right.\right.\\
& \left.\left. - C + D)(A + 3(B+C) + D)\right]\right\}/(8P_D),\\
D' = {} & \left\{1 - p_G^2\left[A^2 + 2A(B+C+D) + B^2\right.\right.\\
& \left.\left. + 2B(D-7C) + (C+D)^2\right]\right\}/(8P_D).
\end{aligned}$$

APPENDIX C: ADDITIONAL MATERIAL FOR THE HYBRID QUANTUM REPEATER

In this Appendix we derive the formula for successful entanglement generation when PNRD are used for the measurements. Moreover, we present the formulas for the states after entanglement swapping and entanglement distillation.

1. Entanglement generation

The total state before the detector measurements is described by [55]

$$\begin{aligned}
\rho_{AB,b_3,b_5} = {} & p\{[|0\rangle_{b_3}(|00\rangle_{AB}|\beta\rangle_{b_5} + |11\rangle_{AB}|-\beta\rangle_{b_5})/2\\
& + |0\rangle_{b_5}(|01\rangle_{AB}|-\beta\rangle_{b_3} + |10\rangle_{AB}|\beta\rangle_{b_3})/2] \times \text{H.c.}\}\\
& + (1-p)\{[|0\rangle_{b_3}(|00\rangle_{AB}|\beta\rangle_{b_5} - |11\rangle_{AB}|-\beta\rangle_{b_5})/2\\
& + |0\rangle_{b_5}(|01\rangle_{AB}|-\beta\rangle_{b_3} - |10\rangle_{AB}|\beta\rangle_{b_3})/2] \times \text{H.c.}\},
\end{aligned} \tag{C1}$$

[14] This probability was derived by taking the probability of the measurement in the preceding footnote squared, as we need two coincident clicks for the Bell measurement.

where H.c. stays for the Hermitian conjugate of the previous term, A (B) represents the qubit at Alice's (Bob's) side, b_3 is the coherent-state mode arriving at the detector D_1, b_5 is the coherent-state mode arriving at the detector D_2, and $\beta = i\sqrt{2\eta_t}\sin(\theta/2)$ [see Eq. (8)]. The probability of error caused by photon losses in the transmission channel is given by $(1-p)$, with $p = (1+e^{-2(1-\eta_t)\alpha^2\sin^2(\theta/2)})/2$. It is possible to observe from Eq. (C1) that whenever Bob detects a click in either one of the detectors D_1 or D_2, an entangled state has been distributed between qubits A and B.

We discuss in the following the case that D_1 and D_2 are imperfect PNRD [see Eq. (2)]. When detector D_1 does not click and D_2 clicks, the resulting state ρ_{AB} is then given by

$$\rho_{AB} = \frac{\mathrm{tr}_{b_3b_5}\left(\Pi^{(0)}_{b_3}\Pi^{(n)}_{b_5}\rho_{AB,b_3,b_5}\right)}{\mathrm{tr}\left(\Pi^{(0)}_{b_3}\Pi^{(n)}_{b_5}\rho_{AB,b_3,b_5}\right)}, \tag{C2}$$

with $n > 0$. The same result up to local operations can be obtained in the opposite case (a click in detector D_1 and no click in detector D_2).

Depending on the outcome of the detector, a local operation maybe applied to change the resulting state into the desired state. In this way, if the outcome is an even number, nothing should be done; otherwise, a Z operation should be applied. Following this, the resulting state can be written as

$$\rho = F_0|\phi^+\rangle\langle\phi^+| + (1-F_0)|\phi^-\rangle\langle\phi^-|,$$

where

$$\begin{aligned} F_0 &= \frac{[\langle 00|_{AB} + (-1)^n\langle 11|_{AB}]}{\sqrt{2}}\rho_{A,B}\frac{[|00\rangle_{AB} + (-1)^n|11\rangle_{AB}]}{\sqrt{2}} \\ &= \frac{1+e^{-2[1+\eta_t(1-2\eta_d)]\alpha^2\sin^2(\theta/2)}}{2}. \end{aligned} \tag{C3}$$

The probability of success is calculated by adding all successful events, and is given by

$$P_0 = \sum_{n=1}^{\infty}\mathrm{tr}\left(\Pi^{(0)}_{b_3}\Pi^{(n)}_{b_5}\rho_{AB,b_3,b_5} + \Pi^{(0)}_{b_5}\Pi^{(n)}_{b_3}\rho_{AB,b_3,b_5}\right). \tag{C4}$$

Combining Eqs. (C1) and (2) we obtain Eq. (23).

2. Entanglement swapping

The initial states used in the swapping operation are a full rank mixture of the Bell states, $\rho_0 := A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|$. After the connection, the resulting state will remain in the same form, $A'|\phi^+\rangle\langle\phi^+| + B'|\phi^-\rangle\langle\phi^-| + C'|\psi^+\rangle\langle\psi^+| + D'|\psi^-\rangle\langle\psi^-|$, but with new coefficients:

$$\begin{aligned} A' &= 2BC + 2AD + 2[-2BC + A(B+C-2D) + (B+C)D]p_G + (A-B-C+D)^2p_G^2, \\ B' &= 2AC + 2BD + [A^2 + (B+C)^2 - 4BD + D^2 + 2A(-2C+D)]p_G - (A-B-C+D)^2p_G^2, \\ C' &= 2AB + 2CD + [A^2 + (B+C)^2 - 4CD + D^2 + 2A(-2B+D)]p_G - (A-B-C+D)^2p_G^2, \\ D' &= A^2 + B^2 + C^2 + D^2 - 2[A^2 + B^2 + C^2 - A(B+C) - (B+C)D + D^2]p_G + (A-B-C+D)^2p_G^2. \end{aligned} \tag{C5}$$

It is possible to see that $A' + B' + C' + D' = 1$, such that even for the case of imperfect connection operations, the swapping occurs deterministically.

3. Entanglement distillation

We calculated also the effect of the gate error in the distillation step. Starting with two copies of states in the form of $\rho_0 := A|\phi^+\rangle\langle\phi^+| + B|\phi^-\rangle\langle\phi^-| + C|\psi^+\rangle\langle\psi^+| + D|\psi^-\rangle\langle\psi^-|$, the resulting state after one round of distillation is given by $A'|\phi^+\rangle\langle\phi^+| + B'|\phi^-\rangle\langle\phi^-| + C'|\psi^+\rangle\langle\psi^+| + D'|\psi^-\rangle\langle\psi^-|$, where

$$\begin{aligned} A' &= \frac{1}{P_D}\left(D^2 + A^2[1+2(-1+p_G)p_G]^2 - 2A(-1+p_G)p_G\left[C + 2D + 2(B-C-2D)p_G + 2(-B+C+2D)p_G^2\right]\right. \\ &\quad \left. -2D(-1+p_G)p_G\{-2D - 2(C+D)(-1+p_G)p_G + B[1+2(-1+p_G)p_G]\}\right), \\ B' &= \frac{1}{P_D}\left[-2\left(D(-1+p_G)p_G\left(C + D + 2Bp_G - 2Cp_G - 2Dp_G - 2Bp_G^2 + 2Cp_G^2 + 2Dp_G^2\right) + A^2p_G\left(-1+3p_G - 4p_G^2 + 2p_G^3\right)\right.\right. \\ &\quad \left.\left. -A\left\{D\left(1-2p_G+2p_G^2\right)^2 - (-1+p_G)p_G\left[-2C(-1+p_G)p_G + B\left(1-2p_G+2p_G^2\right)\right]\right\}\right)\right], \\ C' &= \frac{1}{P_D}\left(B^2\left(1-2p_G+2p_G^2\right)^2 - 2B(-1+p_G)p_G\left[-2A(-1+p_G)p_G + D\left(1-2p_G+2p_G^2\right) + C\left(2-4p_G+4p_G^2\right)\right]\right. \\ &\quad \left. +C\left\{C\left(1-2p_G+2p_G^2\right)^2 - 2(-1+p_G)p_G\left[-2D(-1+p_G)p_G + A\left(1-2p_G+2p_G^2\right)\right]\right\}\right), \\ D' &= \frac{1}{P_D}\left\{-2\left(C(-1+p_G)p_G(C + D + 2Ap_G - 2Cp_G - 2Dp_G - 2Ap_G^2 + 2Cp_G^2 + 2Dp_G^2\right) + B^2p_G\left(-1+3p_G - 4p_G^2 + 2p_G^3\right)\right. \\ &\quad \left.\left. -B\left\{C\left(1-2p_G+2p_G^2\right)^2 - (-1+p_G)p_G\left[-2D(-1+p_G)p_G + A\left(1-2p_G+2p_G^2\right)\right]\right\}\right)\right\}. \end{aligned} \tag{C6}$$

P_D is the distillation probability of success and is given by

$$P_D = (B+C)^2 + (A+D)^2 - 2(A-B-C+D)^2 p_G + 2(A-B-C+D)^2 p_G^2. \tag{C7}$$

For the case of $p_G = 1$, Eqs. (C6) and (C7) are in accordance with [30].

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[2] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus, Phys. Rev. A **84**, 022325 (2011).
[3] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304 (2011).
[4] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[5] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[7] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[9] D. Collins, N. Gisin, and H. De Riedmatten, J. Mod. Opt. **52**, 735 (2005).
[10] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, Phys. Rev. Lett. **92**, 047904 (2004).
[11] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002).
[12] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[13] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).
[14] N. Sangouard, R. Dubessy, and C. Simon, Phys. Rev. A **79**, 042340 (2009).
[15] B. Zhao, M. Müller, K. Hammerer, and P. Zoller, Phys. Rev. A **81**, 052329 (2010).
[16] Y. Han, B. He, K. Heshami, C.-Z. Li, and C. Simon, Phys. Rev. A **81**, 052311 (2010).
[17] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. A **72**, 052330 (2005).
[18] A. Scherer, B. C. Sanders, and W. Tittel, Opt. Express **19**, 3004 (2011).
[19] M. Razavi, J. Amirloo, and A. Majedi, in *Optical Fiber Communication (OFC), Collocated National Fiber Optic Engineers Conference, 2010 Conference on (OFC/NFOEC)* (IEEE, New York, 2010), pp. 1–3.
[20] J. Amirloo, M. Razavi and A. H. Majedi, Phys. Rev. A **82**, 032304 (2010).
[21] N. Lo Piparo and M. Razavi, arXiv:1210.8042v1.
[22] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, Phys. Rev. A **76**, 050301 (2007).
[23] J. Minář, H. de Riedmatten, and N. Sangouard, Phys. Rev. A **85**, 032313 (2012).
[24] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, arXiv:1303.3456v1.
[25] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).
[26] V. Tatarskǐ, *Wave Propagation in a Turbulent Medium* (McGraw-Hill, New York, 1961).
[27] P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, 2010).
[28] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).
[29] C. Simon *et al.*, Eur. Phys. J. D: Plasma Phys. **58**, 1 (2010).
[30] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[31] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[32] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[33] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, Phys. Rev. A **59**, 1025 (1999).
[34] X.-L. Feng, Z.-M. Zhang, X.-D. Li, S.-Q. Gong, and Z.-Z. Xu, Phys. Rev. Lett. **90**, 217902 (2003).
[35] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).
[36] R. Renner, Int. J. Quantum Inf. **6**, 1 (2008).
[37] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[38] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[39] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[40] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[41] Chi-Hang Fred Fung, H. F. Chau, and H.-K. Lo, Phys. Rev. A **84**, 020303 (2011).
[42] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).
[43] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[44] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[45] H. K. Lo, H. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
[46] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).
[47] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography*, edited by J. Kilian, Lecture Notes in Computer Science Vol. 3378 (Springer, Berlin/Heidelberg, 2005), pp. 386–406.
[48] R. Renner and R. König, in *Theory of Cryptography Conference (TCC)* (Springer, Berlin, 2005), Vol. 3378, p. 407.
[49] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
[50] I. Wolfram Research, *Mathematica Edition: Version 8.0* (Wolfram Research, Champaign, IL, 2010).

[51] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[52] M. Eisaman, J. Fan, A. Migdall, and S. Polyakov, Rev. Sci. Instrum. **82**, 071101 (2011).
[53] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. **8**, 184 (2006).
[54] P. van Loock, N. Lütkenhaus, W. J. Munro, and K. Nemoto, Phys. Rev. A **78**, 062319 (2008).
[55] K. Azuma, N. Sota, R. Namiki, Ş. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. A **80**, 060303 (2009).
[56] P. van Loock, W. J. Munro, K. Nemoto, T. P. Spiller, T. D. Ladd, S. L. Braunstein, and G. J. Milburn, Phys. Rev. A **78**, 022303 (2008).
[57] S. G. R. Louis, W. J. Munro, T. P. Spiller, and K. Nemoto, Phys. Rev. A **78**, 022326 (2008).
[58] T. Ralph and A. Lund, AIP Conf. Proc. **1110**, 155 (2009).
[59] J. Fiurášek and N. J. Cerf, Phys. Rev. A **86**, 060302(R) (2012).
[60] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, Phys. Rev. A **87**, 020303 (2013).
[61] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[62] P. Kok and S. L. Braunstein, Phys. Rev. A **61**, 042304 (2000).
[63] K. Lee, X. Chen, H. Eghlidi, P. Kukura, R. Lettow, A. Renn, V. Sandoghdar, and S. Götzinger, Nat. Photon. **5**, 166 (2011).
[64] A. Lita, A. Miller, and S. Nam, Opt. Express **16**, 3032 (2008).
[65] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **98**, 190503 (2007).
[66] L. Jiang, J. M. Taylor, and M. D. Lukin, Phys. Rev. A **76**, 012301 (2007).
[67] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).
[68] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, Proc. Natl. Acad. Sci. USA **104**, 17291 (2007).
[69] R. Van Meter, T. Ladd, W. Munro, and K. Nemoto, IEEE/ACM Trans. Networking **17**, 1002 (2009).
[70] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. V. Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).
[71] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, Phys. Rev. Lett. **104**, 180503 (2010).
[72] N. K. Bernardes and P. van Loock, Phys. Rev. A **86**, 052301 (2012).
[73] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).
[74] W. Dür, Diplomarbeit, Leopold-Franzens-Universität Innsbruck, Innsbruck, 1998.

"Quantum repeaters and quantum key distribution: Analysis of secret-key rates."
Abruzzo, S., Bratzik, S., Bernardes, N.K., Kampermann, H., van Loock, P. und Bruß, D.
Physical Review A **87**, 052315, 2013.

Journal: Physical Review A
Impact factor: 3,042
Anteil an der Arbeit: 35%, 2. Autor, Editieren des Manuskriptes, Verfassen von einigen Kapiteln, Ausführung von Berechnungen

PHYSICAL REVIEW A **87**, 012315 (2013)

Secret key rates for coherent attacks

Markus Mertz,* Hermann Kampermann, Sylvia Bratzik, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany
(Received 29 June 2012; published 17 January 2013)

We develop a method to quantify the secret key rate for permutation-invariant protocols for coherent attacks and finite resources. The method reduces the calculation of secret key rates for coherent attacks to the calculation for collective attacks by bounding the smooth min-entropy of permutation-invariant states via the smooth min-entropy of corresponding tensor-product states. The comparison of the results to the well-known postselection technique for the BB84 and six-state protocol shows the high relevance of this method. Since our calculation of secret key rates for coherent attacks strongly depends on the way of treating collective attacks, a prospective progress in the analysis of collective attacks will immediately cause progress in our strategy.

DOI: 10.1103/PhysRevA.87.012315 PACS number(s): 03.67.Dd

I. INTRODUCTION

The aim of quantum key distribution (QKD) is the generation of a secret key between two authorized parties Alice and Bob in the presence of an eavesdropper Eve. In practical implementations the number of signals used to establish a secure key is finite. An essential element of the calculation of key rates for a finite number of signals is the evaluation of the smooth min-entropy [1] for high-dimensional states, which is in general hard or even impossible to compute. In the last years many results have appeared [1–11] considering the calculation of secret key rates for finite resources under the restriction of the eavesdropper's attack to a collective attack [12,13], where Eve interacts with each signal independently and identically. This restriction leads to a state, which has tensor-product form and allows one to bound the smooth min-entropy by the conditional von Neumann entropy of a single-signal state by using the asymptotic equipartition property (AEP) [1,14].

In studies of coherent attacks [15,16] the eavesdropper is not restricted at all (i.e., she may interact with all signals simultaneously). Already in the year 2005 it was shown in Refs. [17,18] that for protocols, which are invariant under permutations of single-signal states, collective and coherent attacks are equivalent in the case of infinitely many signals. But for a finite number of signals this equivalence has not been proven yet. As a consequence the development of tools to compute a secret key for finite resources in the presence of coherent attacks is necessary.

Up to now direct strategies that treat coherent attacks only exist for the BB84 [19] protocol (see [10,11]). In Ref. [10] Tomamichel *et al.* used an uncertainty relation for smooth entropies [20] to circumvent the evaluation of the smooth min-entropy by the computation of the smooth max-entropy [1]. Since the resulting max-entropy has to be evaluated for a classical state, the calculation becomes analytically solvable.

In comparison to these direct strategies, many studies have focused on indirect approaches like postselection [21] or the de Finetti approach [1,22] to quantify secret key rates, where the analysis for coherent attacks is traced back to the investigation of collective attacks. In Ref. [7], these indirect approaches have been compared to each other for the BB84 protocol with the result that the postselection technique exceeds the de Finetti approach in terms of secure key rates.

In this paper we present a strategy to calculate secret key rates for general permutation-invariant (i.e., the output of the protocol remains the same under permutations of the input pairs) protocols for coherent attacks. In particular, we relate the secret key rate for coherent attacks to the calculation of secret key rates for collective attacks by bounding the smooth min-entropy of a permutation-invariant state via the min-entropy of a corresponding tensor-product state "smoothed" over a reduced environment. We compare the results to the postselection technique by applying the AEP bound for the treatment of collective attacks. Note that most of the protocols studied in the literature already fulfill the condition of permutation invariance or can made to be permutation invariant, like, for example, the BB84 and six-state [23,24] protocol. Note that in this paper we only consider single-photon pulses. An analogous investigation of weak coherent pulses could be fruitful by following the strategy in Ref. [25].

The paper is organized as follows. In Sec. II we explain the protocol and fix the notation. We clarify the formalism used to calculate secret key rates under the assumption of collective attacks in Sec. III. The formalism to analyze coherent attacks, the main result of this paper, is presented in Sec. IV. Section V shortly reviews the postselection technique, which is then compared to our strategy with respect to secret key rates for the BB84 and six-state protocol in Sec. VI. Finally, Sec. VII concludes the paper.

II. PRELIMINARIES

In this paper we consider permutation-invariant entanglement-based QKD protocols, which consist of these steps: state distribution, sifting, parameter estimation (PE), error correction (EC), error verification, and privacy amplification (PA) (for a detailed description, see [17,18]). Here, permutational invariance means that for any permutation of the input pairs the output of the protocol remains unchanged. In the following we denote by ρ_{AB}^{N} the initial state of N signals shared by Alice and Bob, and by ρ_{ABE}^{N} a purification of ρ_{AB}^{N}, which describes the state shared by Alice, Bob, and Eve after the state distribution. Now, let $\mathcal{N}_{\mathrm{AB}}$ be the operation, that represents the procedures, which Alice and Bob perform on their states (i.e., measurement, sifting, parameter estimation,

*mertz@thphy.uni-duesseldorf.de

error correction, and error verification. (Note that privacy amplification is not included here, since the output of this procedure is the final bit-string used as key.) Then we define the resulting classical-quantum state containing Alice's bit string and Eve's quantum state as $\rho^n_{XE} := (\mathcal{N}_{AB} \otimes \mathbb{1}_E)\rho^N_{ABE}$. As the main quantity for the calculation of secret key rates we use the smooth min-entropy [1],

$$H^{\varepsilon}_{\min}(\rho_{AE}|E) := \sup_{\sigma_{AE}\in\mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{AE})} \sup_{\rho_E\in\mathcal{S}(\mathcal{H}_E)} H_{\min}(\sigma_{AE}|\rho_E), \quad (1)$$

defined as an optimization of the min-entropy,

$$H_{\min}(\sigma_{AE}|\rho_E) := \sup\{\lambda \in \mathbb{R} : 2^{-\lambda}\mathbb{1}_A \otimes \rho_E - \sigma_{AE} \geqslant 0\}, \quad (2)$$

over an $\frac{\varepsilon}{2}$ environment given by

$$\mathcal{B}^{\frac{\varepsilon}{2}}(\rho) := \left\{\sigma : \frac{1}{2}||\sigma - \rho||_1 \leqslant \frac{\varepsilon}{2}\right\}, \quad (3)$$

with the 1-norm $||A||_1 = \mathrm{tr}(\sqrt{AA^\dagger})$. $\mathcal{S}(\mathcal{H}_E)$ denotes the set of density operators on the Hilbert space $\mathcal{H}_E$.

III. COLLECTIVE ATTACKS

In contrast to coherent attacks, the assumption of collective attacks forces the eavesdropper Eve to interact with each of the signals separately. Under this restriction the distributed state can for permutation-invariant protocols regarded as a product state $\rho^{\otimes N}_{AB}$, which is diagonal in the Bell basis [17,18]. We denote by m the number of randomly chosen signals used for parameter estimation and by n the remaining number of signals for privacy amplification. Then, the rate of an ε-secure key can be quantified in the following way.

Theorem 1. [3] Let $\varepsilon_{PE},\varepsilon_{EC},\varepsilon_{PA},\bar{\varepsilon} > 0$ and let $\rho^{\otimes n}_{XE} = (\mathcal{N}_{AB} \otimes \mathbb{1}_E)\rho^{\otimes N}_{ABE}$ be a tensor-product state for a purification ρ_{ABE} in $\mathcal{H}_{ABE}$ of the state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$. Then the rate of an $\varepsilon_{coll} := (\varepsilon_{PE} + \varepsilon_{EC} + \varepsilon_{PA} + \bar{\varepsilon})$-secure key is given by

$$r := \frac{1}{N} \inf_{\rho_{AB}\in\Gamma_{coll}} \left(H^{\bar{\varepsilon}}_{\min}\left(\rho^{\otimes n}_{XE}|E\right) - \mathrm{leak}_{EC}\right) + \frac{2}{N}\log_2(2\varepsilon_{PA}). \quad (4)$$

The smooth min-entropy of the classical-quantum state $\rho^{\otimes n}_{XE}$ shared by Alice and Eve and the correction $2\log_2(2\varepsilon_{PA})$ arise from the analysis of privacy amplification. The entropy quantifies Eve's uncertainty of Alice's bit string.

The term leak_{EC} stands for the number of bits which Alice and Bob leak to the eavesdropper due to public communication during the error correction procedure and cost for the error verification. In total, the leakage can be estimated by [3,10]

$$\mathrm{leak}_{EC} := n1.1H(X|Y) + \log_2\left(\frac{2}{\varepsilon_{EC}}\right). \quad (5)$$

Here, the factor 1.1 denotes the efficiency of a specific error-correction protocol used during the key generation. The minimization of the smooth min-entropy is due to parameter estimation, where we only except qubit states ρ_{AB} which are contained in the set [10],

$$\Gamma_{coll} := \left\{\sigma_{AB} : \tfrac{1}{2}||P_m - P_n||_1 \leqslant \xi(\varepsilon_{PE},n,m)\right\}, \quad (6)$$

with

$$\xi(\varepsilon_{PE},n,m) := \sqrt{\frac{(n+m)(m+1)\ln(1/\varepsilon_{PE})}{8m^2n}}. \quad (7)$$

This means, that the tolerated quantum bit error rate (QBER) P_m due to an m-fold independent application of a POVM $\mathcal{E}$ on a tensor-product state is ξ close to the parameter P_n, which corresponds to a virtual measurement on the remaining n signals, which are used for the key generation, except with probability ε_{PE} (see Lemma 6 in the Appendix). Note that this estimate has been developed in Ref. [10] for coherent attacks on permutation-invariant states. As tensor-product states in collective attacks are permutation invariant, Lemma 6 can be applied.

For product states $\rho^{\otimes n}_{XE}$ we can use the asymptotic equipartition property [see Eq. (B7)] to bound the smooth min-entropy by the conditional von Neumann entropy of a single copy ρ_{XE}. Finally, we get for the rate of an $\varepsilon_{coll} := (\varepsilon_{PE} + \varepsilon_{EC} + \varepsilon_{PA} + \bar{\varepsilon})$-secure key:

$$r_{coll} := \frac{n}{N}\left[\inf_{\rho_{AB}\in\Gamma_{coll}}\left(S(X|E) - \frac{\mathrm{leak}_{EC}}{n}\right) - 5\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}\right] + \frac{2}{N}\log_2(2\varepsilon_{PA}), \quad (8)$$

where

$$S(X|E) = S(\rho_{XE}) - S(\rho_E), \quad (9)$$

with $S(\rho) := -\mathrm{tr}(\rho\log_2\rho)$.

In the next section we present a formalism to treat coherent attacks. We will see that the analysis of secret key rates for coherent attacks can be traced back to the calculation of secret key rates under the assumption of collective attacks [see Eq. (8)].

IV. COHERENT ATTACKS

A coherent attack is the most general attack an eavesdropper can perform (i.e., Eve is not restricted at all). For the investigation of secret key rates for coherent attacks, we have to consider nonproduct states for the evaluation of the smooth-min entropy. No changes are needed in the analysis of parameter estimation for collective attacks [see Eq. (6)], because it also holds for coherent attacks [i.e., nonproduct states (see Lemma 6 in the Appendix)]. Since error correction and error verification are also independent of the underlying attack of the eavesdropper (they are purely classical procedures), the protocol analysis for these steps can be adopted from the one for collective attacks.

For permutation-invariant protocols it has been shown in Refs. [17,18] that we can assume w.l.o.g. that, after the distribution of N qubit pairs, Alice and Bob share a permutation-invariant quantum state, which is a convex combination of tensor products of Bell states:

$$\rho^N_{AB} = \mathcal{P}_N\left(\sum_{\mathbf{n}\in\Lambda^N} \mu_{\mathbf{n}}\sigma_1^{\otimes n_1} \otimes \sigma_2^{\otimes n_2} \otimes \sigma_3^{\otimes n_3} \otimes \sigma_4^{\otimes n_4}\right), \quad (10)$$

with probabilities $\mu_{\mathbf{n}}$ for the "realization" $\mathbf{n}$ and the set of realizations,

$$\Lambda^N := \left\{ \mathbf{n} = (n_1,n_2,n_3,n_4) : \sum_{i=1}^{4} n_i = N \right\}. \tag{11}$$

The σ_i for $i = 1,\ldots,4$ correspond to the projector onto the four Bell-states in $\mathcal{H}_A \otimes \mathcal{H}_B$, that is,

$$\begin{aligned} \sigma_1 &= |\phi^+\rangle\langle\phi^+|, \quad \sigma_2 = |\phi^-\rangle\langle\phi^-|, \\ \sigma_3 &= |\psi^+\rangle\langle\psi^+|, \quad \sigma_4 = |\psi^-\rangle\langle\psi^-|, \end{aligned} \tag{12}$$

with

$$|\phi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \tag{13}$$

and

$$|\psi^{\pm}\rangle := \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{14}$$

$\mathcal{P}_N$ denotes the completely positive map (CPM) which symmetrizes the state with respect to all possible distinguishable permutations of the N qubit pairs.

The following section explains the analysis of parameter estimation for permutation-invariant states [see Eq. (10)].

A. Parameter estimation

Let the sifting procedure now be such that $n+m$ signals remain, where m denotes the number of randomly chosen signals used for parameter estimation and n denotes the remaining number of signals for privacy amplification. Then we can adopt Lemma 6 to estimate the QBER Q_n by the tolerated QBER Q_m coming from a measurement on general permutation-invariant states [see also the arguments below Eq. (7)].

Theorem 2. Let $\varepsilon_{\mathrm{PE}} > 0$ and $m,n > 0$. Let $\rho_{\mathrm{AB}}^{m+n} \in \mathcal{S}(\mathcal{H}_{AB}^{\otimes m+n})$ be a permutation-invariant quantum state, and let $\mathcal{E}$ be a POVM on $\mathcal{H}_{\mathrm{AB}}$ which measures the QBER. Let $\mathbf{Q}_m$ and $\mathbf{Q}_n$ be the frequency distributions when applying the measurement $\mathcal{E}^{\otimes m}$ and $\mathcal{E}^{\otimes n}$, respectively, to different subsystems of ρ_{AB}^{m+n}. Then for any element Q_m and Q_n from $\mathbf{Q}_m$ and $\mathbf{Q}_n$ except with probability $\varepsilon_{\mathrm{PE}}$

$$\tfrac{1}{2}||Q_m - Q_n||_1 \leqslant \xi(\varepsilon_{\mathrm{PE}},n,m), \tag{15}$$

with $\xi(\varepsilon_{\mathrm{PE}},n,m) := \sqrt{\frac{(m+n)(m+1)\ln(1/\varepsilon_{\mathrm{PE}})}{8m^2n}}$.

Proof: This follows directly from Lemma 6 in the Appendix, which is a consequence of [10]. ■

Now with the definition of the set of states, which pass the parameter estimation procedure,

$$\Gamma_{\varepsilon_{\mathrm{PE}}}^{n} := \left\{ \sigma_{\mathrm{AB}}^{n} : \tfrac{1}{2}||Q_m - Q_n||_1 \leqslant \xi(\varepsilon_{\mathrm{PE}},n,m) \right\}, \tag{16}$$

we are able to give an analytic expression for the rate of an ε-secure key for coherent attacks.

Corollary 1. Let $\varepsilon_{\mathrm{PE}},\varepsilon_{\mathrm{EC}},\varepsilon_{\mathrm{PA}},\bar{\varepsilon} > 0$ and let $\rho_{XE}^{n} = (\mathcal{N}_{\mathrm{AB}} \otimes \mathbb{1}_E)\rho_{\mathrm{ABE}}^{N}$ be a permutation-invariant state for a purification ρ_{ABE}^{N} in $\mathcal{H}_{\mathrm{ABE}}^{\otimes N}$ of $\rho_{\mathrm{AB}}^{N} \in \mathcal{S}(\mathcal{H}_{\mathrm{AB}}^{\otimes N})$. Then the rate of an $\varepsilon_{\mathrm{coh}} := (\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}} + \bar{\varepsilon})$-secure key is given by

$$r := \frac{1}{N} \inf_{\rho_{\mathrm{AB}}^{n} \in \Gamma_{\varepsilon_{\mathrm{PE}}}^{n}} \left(H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{n}\middle|E\right) - \mathrm{leak}_{\mathrm{EC}} \right) + \frac{2}{N}\log_2(2\varepsilon_{\mathrm{PA}}). \tag{17}$$

In the following section we show that the smooth min-entropy for permutation-invariant states can be mainly bounded by the min-entropy for corresponding product states "smoothed" over a reduced ε environment.

B. Privacy amplification

In order to get a calculable formula for the key rate [Eq. (17)] we bound the smooth min-entropy for permutation-invariant states by the smooth min-entropy for tensor-product states, which then can be easily evaluated by the asymptotic equipartition property [Eq. (B7)] as explained in Sec. III.

We now define analogously to Eq. (10) the permutation-invariant state with n signals, which Alice and Bob share after the parameter estimation procedure.

$$\rho_{\mathrm{AB}}^{n} := \mathcal{P}_n\left(\sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \sigma_1^{\otimes n_1} \otimes \sigma_2^{\otimes n_2} \otimes \sigma_3^{\otimes n_3} \otimes \sigma_4^{\otimes n_4} \right), \tag{18}$$

where σ_i with $i = 1,\ldots,4$ correspond to the projectors onto the four Bell states in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\Lambda^n := \{\mathbf{n} = (n_1,n_2,n_3,n_4) : \sum_{i=1}^{4} n_i = n\}$ [see Eq. (10)]. Additionally, we denote the single-copy state shared by Alice and Bob in the following as

$$\sigma_{\mathrm{AB}}[\boldsymbol{\lambda}] := \sum_{i=1}^{4} \lambda_i \sigma_i, \tag{19}$$

with $\boldsymbol{\lambda} := (\lambda_1,\lambda_2,\lambda_3,\lambda_4) = (\frac{n_1}{n},\frac{n_2}{n},\frac{n_3}{n},\frac{n_4}{n})$.

The next theorem is one of our central results. It gives a relation between the smooth min-entropy for permutation-invariant states and the smooth min-entropy for tensor-product states. The proof is inspired by [18] and uses the fact, that there exists a certain measurement on $\sigma_{\mathrm{AB}}[\boldsymbol{\lambda}]^{\otimes n}$, such that the resulting state is equal to the state ρ_{AB}^{n} for a specific realization $\mathbf{n}$. Then, the application of some fundamental properties of the smooth min-entropy leads to the result.

Theorem 3. Let $\bar{\varepsilon} > 0$, $\boldsymbol{\lambda} = (\frac{n_1}{n},\frac{n_2}{n},\frac{n_3}{n},\frac{n_4}{n})$ and $\mathcal{M}_{\mathrm{AB}}$ be the quantum operation which describes the local measurements Alice and Bob perform followed by a partial-trace operation on Bob's part ($\mathcal{H}_B$). Let $\rho_{XE}^{n} = (\mathcal{M}_{\mathrm{AB}} \otimes \mathbb{1}_E)^{\otimes n}\rho_{\mathrm{ABE}}^{n}$ be the classical quantum state obtained after applying the quantum operation $(\mathcal{M}_{\mathrm{AB}} \otimes \mathbb{1}_E)^{\otimes n}$ on a purification ρ_{ABE}^{n} in $\mathcal{H}_{\mathrm{ABE}}^{\otimes n}$ of a permutation-invariant state $\rho_{\mathrm{AB}}^{n} \in \mathcal{S}(\mathcal{H}_{\mathrm{AB}}^{\otimes n})$. Analogously let $\sigma_{XE}[\boldsymbol{\lambda}]^{\otimes n} = (\mathcal{M}_{\mathrm{AB}} \otimes \mathbb{1}_E)^{\otimes n}\sigma_{\mathrm{ABE}}[\boldsymbol{\lambda}]^{\otimes n}$ be the classical quantum state obtained after applying the quantum operation $(\mathcal{M}_{\mathrm{AB}} \otimes \mathbb{1}_E)^{\otimes n}$ on a purification $\sigma_{\mathrm{ABE}}[\boldsymbol{\lambda}]^{\otimes n}$ of a tensor-product state $\sigma_{\mathrm{AB}}[\boldsymbol{\lambda}]^{\otimes n} \in \mathcal{S}(\mathcal{H}_{\mathrm{AB}}^{\otimes n})$. Let $\mathcal{E}$ be a POVM on $\mathcal{H}_A \otimes \mathcal{H}_B$ which measures the QBER. Let Q_n, P_n be an element of the frequency distribution $\mathbf{Q}_n$, $\mathbf{P}_n$ of the outcomes when applying the measurement $\mathcal{E}^{\otimes n}$ to ρ_{AB}^{n} and $\sigma_{\mathrm{AB}}^{\otimes n}$, respectively. Then except with probability $\bar{\varepsilon}$,

$$H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{n}\middle|E\right) \geqslant \inf_{\sigma_{\mathrm{AB}}\in\Gamma_{\bar{\varepsilon}_{\mathrm{coh}}}} H_{\min}^{\bar{\varepsilon}/(2n^2)}\left(\sigma_{XE}^{\otimes n}\left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}\right]\middle|E\right) - 1, \tag{20}$$

where

$$\Gamma_{\mathrm{coh}} := \left\{ \tau_{\mathrm{AB}} : \tfrac{1}{2}||Q_m - P_n||_1 \leqslant \xi_{\mathrm{coh}}(\bar{\varepsilon},n,m) \right\}, \tag{21}$$

with

$$\xi_{\mathrm{coh}}(\bar{\varepsilon},n,m) := \frac{1}{2}\xi_{\mathrm{att}}(\bar{\varepsilon},2,n) + \xi\left(\frac{\bar{\varepsilon}}{2},n,m\right), \tag{22}$$

where

$$\xi_{\mathrm{att}}(\bar{\varepsilon},2,n) := \sqrt{\frac{16\ln(2) + 8\ln(1/\bar{\varepsilon})}{n}}, \tag{23}$$

and

$$\xi\left(\frac{\bar{\varepsilon}}{2},n,m\right) := \sqrt{\frac{(m+n)(m+1)\ln(2/\bar{\varepsilon})}{8m^2 n}} \tag{24}$$

defines the set of tensor-product states $\tau^{\otimes n}$ which pass the parameter estimation procedure.

Proof: The state to be considered is given by ρ^n_{XE} and can be expressed as a convex combination of states for all possible realizations $\mathbf{n}$ with probability $\mu_{\mathbf{n}}$, that is,

$$\rho^n_{XE} = \sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \rho^n_{XE}[\mathbf{n}]. \tag{25}$$

Note that this structure is provided in Eq. (18) and is conserved due to the linearity of $\mathcal{M}_{\mathrm{AB}}$ and a purification of ρ^n_{AB}, which is optimal for Eve.

The first part proves the theorem for the special case, that only one $\mu_{\mathbf{n}}$ in Eq. (25) is nonzero (i.e., we consider a single realization $\mathbf{n}$). Then, part 2 extends part 1 to the general case.

Part 1*:* Let $|\phi_i\rangle$ be an extension to $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ of σ_i [see Eq. (18)] with the condition, that the remaining states $\mathrm{tr}_{\mathrm{AB}}(P_{|\phi_i\rangle})$ are mutually orthogonal for $i \in \{1,\ldots,4\}$. Note that this choice of orthogonal ancillas is optimal, since it enables the eavesdropper to distinguish perfectly the reduced states shared by Alice and Bob. Let S_n be the set of distinguishable permutations π on n qubits for a fixed realization $\mathbf{n}$. Then, with

$$|\psi\rangle^{\mathbf{n}}_{\mathrm{ABE}} := \frac{1}{\sqrt{|S_n|}} \sum_{\pi\in S_n} \pi\left(\bigotimes_{i=1}^{4} |\phi_i\rangle^{\otimes n_i}\right), \tag{26}$$

and

$$|\phi\rangle^{\boldsymbol{\lambda}}_{\mathrm{ABE}} := \sum_{i=1}^{4} \sqrt{\lambda_i}|\phi_i\rangle, \tag{27}$$

we define

$$\rho^n_{XE}[\mathbf{n}] := (\mathcal{M}_{AB} \otimes \mathbb{1}_E)^{\otimes n} P_{|\psi\rangle^{\mathbf{n}}_{\mathrm{ABE}}}, \tag{28}$$

$$\sigma_{XE}[\boldsymbol{\lambda}] := (\mathcal{M}_{AB} \otimes \mathbb{1}_E) P_{|\phi\rangle^{\boldsymbol{\lambda}}_{\mathrm{ABE}}}, \tag{29}$$

for an arbitrary, but fixed realization $\mathbf{n}$. For any $i \in \{1,\ldots,4\}$ let P_i be the projector onto the support of $(\mathcal{M} \otimes \mathbb{1}_E)P_{|\phi_i\rangle}$ which by definition are orthogonal for distinct i. Let $\mathcal{F}$ be a measurement defined by

$$\mathcal{F} : \rho \to \sum_{z=0}^{1} F_z \rho F_z^\dagger \otimes |z\rangle\langle z|, \tag{30}$$

where

$$F_0 := \sum_{\pi\in S_n} \pi\left(P_1^{\otimes n_1} \otimes P_2^{\otimes n_2} \otimes P_3^{\otimes n_3} \otimes P_4^{\otimes n_4}\right), \tag{31}$$

and $F_1 := \mathbb{1} - F_0$. Then F_0 picks out a specific realization $\mathbf{n}$ from the tensor-product state $\sigma_{XE}[\boldsymbol{\lambda}]^{\otimes n}$, that is,

$$\rho^n_{XE}[\mathbf{n}] = \frac{1}{P_Z(Z=0)} F_0(\sigma_{XE}[\boldsymbol{\lambda}]^{\otimes n}) F_0^\dagger, \tag{32}$$

with $P_Z(Z=0) = \mathrm{tr}(F_0(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}])F_0^\dagger) = |S_n| \prod_{i=1}^4 \lambda_i^{n_i}$ (For a detailed proof see [18], Lemma $A.4$).

Now let $\bar{\rho}^n_{XEZ}[\mathbf{n}]$ be the resulting state after applying $\mathcal{F}$ on $\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]$ and let Z be the classical measurement outcome, that is,

$$\bar{\rho}^n_{XEZ}[\mathbf{n}] = \sum_{z=0}^{1} F_z \sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}] F_z^\dagger \otimes |z\rangle\langle z| \tag{33}$$

$$=: \sum_{z=0}^{1} P_Z(Z=z) \bar{\rho}^{nZ=z}_{XE}[\mathbf{n}] \otimes |z\rangle\langle z|. \tag{34}$$

Then it follows directly from Eq. (32) that

$$\rho^n_{XE}[\mathbf{n}] = \bar{\rho}^{nZ=0}_{XE}[\mathbf{n}], \tag{35}$$

and therefore

$$H^{\bar{\varepsilon}}_{\min}\left(\rho^n_{XE}[\mathbf{n}]|E\right) = H^{\bar{\varepsilon}}_{\min}\left(\bar{\rho}^{nZ=0}_{XE}[\mathbf{n}]|E\right). \tag{36}$$

With some fundamental properties of the smooth min-entropy we get

$$\begin{aligned} H^{\bar{\varepsilon}}_{\min}\left(\bar{\rho}^{nZ=0}_{XE}[\mathbf{n}]|E\right) &\overset{\text{Eq.(A7)}}{\geqslant} H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]|EZ\right) \\ &\overset{\text{Eq.(B1)}}{\geqslant} H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]|E\right) \\ &\quad - \log_2\left(\mathrm{rank}(\rho_Z)\right). \end{aligned} \tag{37}$$

By definition, the orthogonality and completeness of the set $\{F_z\}$ ensures that $\mathrm{tr}_Z(\bar{\rho}^n_{XEZ}[\mathbf{n}]) = \sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]$, such that we can apply Eq. (A2) in the Appendix. This leads to

$$\begin{aligned} &H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]|E\right) - \log_2\left(\mathrm{rank}(\rho_Z)\right) \\ &\overset{\text{Eq.(A2)}}{\geqslant} H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]|E\right) - \log_2\left(\mathrm{rank}(\rho_Z)\right) \\ &\geqslant H^{\bar{\varepsilon}/n^2}_{\min}\left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]|E\right) - 1, \end{aligned} \tag{38}$$

where we used in the last step that $\mathrm{rank}(\rho_Z) \leqslant 2$ and from Lemma 7 in the Appendix that

$$p_Z(Z=0) = |S_n| \prod_{i=1}^{4} \lambda_i^{n_i} > 1/n^2. \tag{39}$$

The following part generalizes the proof to the unrestricted case.

Part 2*:* Now let $\rho^n_{\mathrm{ABE}} := P_{|\psi\rangle}$ with

$$|\psi\rangle := \sum_{\mathbf{n}\in\Lambda^n} \sqrt{\mu_{\mathbf{n}}}|\psi\rangle^{\mathbf{n}}_{\mathrm{ABE}} \tag{40}$$

be a purification of ρ^n_{AB}. For any $\mathbf{n} \in \Lambda^n$ let $\mathcal{H}^n_E$ be the smallest subspace of $\mathcal{H}^{\otimes n}_E$ containing the support of the traces $\rho^n_E[\mathbf{n}] = \mathrm{tr}_{\mathcal{H}^{\otimes n}_{\mathrm{AB}}}(\rho^n_{\mathrm{ABE}}[\mathbf{n}])$. By the definition of the vectors $|\phi_i\rangle$ as in part 1, the subspaces $\mathcal{H}^n_E$ are orthogonal for distinct $\mathbf{n} \in \Lambda^n$. There exists a projective measurement $\mathcal{F}'$ onto the subspaces $\mathcal{H}^{\otimes n}_{\mathrm{AB}} \otimes \mathcal{H}^n_E$. Now let the state $\tilde{\rho}^n_{XEZ'}$ be the resulting state from the measurement $\mathcal{F}'$ of the state ρ^n_{XE} and let $Z' \in \Lambda^n$ be the

classical outcome, that is,

$$\tilde{\rho}^n_{XEZ'} = \sum_{\mathbf{n}\in\Lambda^n} F'_{\mathbf{n}}\rho^n_{XE}F'^{\dagger}_{\mathbf{n}} \otimes |\mathbf{n}\rangle\langle\mathbf{n}| \tag{41}$$

$$=: \sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}}\rho^n_{XE}[\mathbf{n}] \otimes |\mathbf{n}\rangle\langle\mathbf{n}|. \tag{42}$$

By the definition of the state ρ^n_{XE} we know that for a tolerated QBER Q_m the parameter Q_n for a virtual measurement on n signals has to fulfill except with probability $\frac{\bar{\varepsilon}}{2}$ that

$$\frac{1}{2}||Q_m - Q_n||_1 \leqslant \xi\left(\frac{\bar{\varepsilon}}{2},n,m\right). \tag{43}$$

Note that the choice of $\frac{\bar{\varepsilon}}{2}$ is arbitrary. In principle, the introduction of a new parameter could lead to better results. Now, this condition implies that realizations $\mathbf{n}$ in the permutation-invariant state $\rho^n_{\mathrm{AB}} = \sum_{\mathbf{n}\in\Lambda^n}\mu_{\mathbf{n}}\rho^n_{\mathrm{AB}}[\mathbf{n}]$, whose corresponding parameter Q_n does not fulfill the condition in Eq. (43), only appear with small probability, that is, more precisely,

$$\sum_{\mathbf{n}:\frac{1}{2}||Q_m-Q_n||_1>\xi(\frac{\bar{\varepsilon}}{2},n,m)} \mu_{\mathbf{n}} \leqslant \frac{\bar{\varepsilon}}{2}. \tag{44}$$

This behavior of the probabilities enables us to apply Eq. (A6) in the Appendix for probability $\varepsilon' = \frac{\bar{\varepsilon}}{2}$ to restrict the states $\rho^n_{\mathrm{AB}}[\mathbf{n}]$ (or equivalently their corresponding realizations $\mathbf{n}$) to the set,

$$\tilde{\Gamma}^n_{\bar{\varepsilon}/2} := \left\{\sigma^n_{\mathrm{AB}}[\mathbf{n}] : \frac{1}{2}||Q_m - Q_n||_1 \leqslant \xi\left(\frac{\bar{\varepsilon}}{2},n,m\right)\right\}. \tag{45}$$

Namely, we have

$$H^{\bar{\varepsilon}}_{\min}\left(\rho^n_{XE}|E\right) \overset{\text{Eq.(A4)}}{\geqslant} H^{\bar{\varepsilon}}_{\min}\left(\tilde{\rho}^n_{XEZ'}|EZ'\right) \overset{\text{Eq.(A6)}}{\geqslant} \inf_{\rho^n_{\mathrm{AB}}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/2}_{\min}\left(\rho^n_{XE}[\mathbf{n}]|E\right). \tag{46}$$

Then Eq. (46) becomes, together with Eqs. (36)–(38),

$$\inf_{\rho^n_{\mathrm{AB}}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/2}_{\min}\left(\rho^n_{XE}[\mathbf{n}]|E\right) \geqslant \inf_{\rho^n_{\mathrm{AB}}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/(2n^2)}_{\min}\left(\sigma^{\otimes n}_{XE}\left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}\right]\middle|E\right) - 1. \tag{47}$$

Since the min-entropy is now a function of a tensor-product state, we would like to express the restricting infimum in terms of the statistics $\mathbf{P}_n$ of this tensor product. By definition, we have $\rho^1_{XE}[\mathbf{n}] = \sigma_{XE}[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}]$, such that we can apply Lemma 8 in the Appendix (for $k = N = n$), which states that, except with probability $\bar{\varepsilon}$, the statistics $\mathbf{P}_n$ of the tensor-product state $\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}]$ is ξ_{att} close to $\mathbf{Q}_n$, that is,

$$\tfrac{1}{2}||\mathbf{Q}_n - \mathbf{P}_n||_1 \leqslant \xi_{\mathrm{att}}(\bar{\varepsilon},|\mathcal{E}|,n). \tag{48}$$

(Here the choice of $\bar{\varepsilon}$ is arbitrary. The consideration of a new parameter could in general lead to better results.) Now we are able to bound the distance between $\mathbf{P}_n$ and the tolerated QBER $\mathbf{Q}_m$ measured during parameter estimation by using the triangular inequality.

$$\begin{aligned}\frac{1}{2}||Q_m - P_n||_1 &\leqslant \frac{1}{2}||Q_m - Q_n||_1 + \frac{1}{2}||Q_n - P_n||_1 \\ &\leqslant \xi\left(\frac{\bar{\varepsilon}}{2},n,m\right) + \frac{\xi_{\mathrm{att}}(\bar{\varepsilon},2,n)}{2} \\ &=: \xi_{\mathrm{coh}}(\bar{\varepsilon},n,m),\end{aligned} \tag{49}$$

where we used that for the POVM applied for parameter estimation [see Eq. (6) and Sec. IV A] the number of POVM elements becomes 2 (see [8]) and that [8]

$$\tfrac{1}{2}||Q_n - P_n||_1 \leqslant \tfrac{1}{2}\tfrac{1}{2}||\mathbf{Q}_n - \mathbf{P}_n||_1. \tag{50}$$

Consequently we end up in

$$\inf_{\rho^n_{\mathrm{AB}}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/(2n^2)}_{\min}\left(\sigma^{\otimes n}_{XE}\left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}\right]\middle|E\right) - 1 \geqslant \inf_{\sigma_{\mathrm{AB}}\in\Gamma_{\xi_{\mathrm{coh}}}} H^{\bar{\varepsilon}/(2n^2)}_{\min}\left(\sigma^{\otimes n}_{XE}\left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}\right]\middle|E\right) - 1. \tag{51}$$

The assertion then follows by putting Eqs. (51) and (47) into Eq. (46). ■

Finally, we are able to formulate a calculable rate of an $\varepsilon_{\mathrm{coh}}$-secure key for coherent attacks.

Theorem 4. Let $\varepsilon_{\mathrm{PE}},\varepsilon_{\mathrm{EC}},\varepsilon_{\mathrm{PA}},\bar{\varepsilon} > 0$ and let $\rho^n_{XE} = (\mathcal{N}_{\mathrm{AB}} \otimes \mathbb{1}_E)\rho^N_{\mathrm{ABE}}$ be a permutation-invariant state for a purification ρ^N_{ABE} in $\mathcal{H}^{\otimes N}_{\mathrm{ABE}}$ of $\rho^N_{\mathrm{AB}} \in \mathcal{S}(\mathcal{H}^{\otimes N}_{\mathrm{AB}})$. Then the rate of an $\varepsilon_{\mathrm{coh}} := (\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}} + 2\bar{\varepsilon})$-secure key is given by

$$r_{\mathrm{coh}} := \frac{n}{N}\left[\inf_{\rho_{\mathrm{AB}}\in\Gamma_{\mathrm{coh}}}\left(S(X|E) - \frac{\mathrm{leak}_{\mathrm{EC}}}{n}\right) - 5\sqrt{\frac{\log_2(4n^2/\bar{\varepsilon})}{n}}\right] - \frac{1}{N} + \frac{2}{N}\log_2(2\varepsilon_{\mathrm{PA}}), \tag{52}$$

where

$$\Gamma_{\mathrm{coh}} = \left\{\sigma_{\mathrm{AB}} : \tfrac{1}{2}||Q_m - P_n||_1 \leqslant \xi_{\mathrm{coh}}(\bar{\varepsilon},n,m)\right\}, \tag{53}$$

with

$$\xi_{\mathrm{coh}}(\bar{\varepsilon},n,m) := \frac{\xi_{\mathrm{att}}(\bar{\varepsilon},2,n)}{2} + \xi\left(\frac{\bar{\varepsilon}}{2},n,m\right), \tag{54}$$

for

$$\xi\left(\frac{\bar{\varepsilon}}{2},n,m\right) := \sqrt{\frac{(m+n)(m+1)\ln(2/\bar{\varepsilon})}{8m^2n}}, \tag{55}$$

$$\xi_{\mathrm{att}}(\bar{\varepsilon},2,n) := \sqrt{\frac{16\ln(2) + 8\ln(1/\bar{\varepsilon})}{n}}, \tag{56}$$

and

$$S(X|E) = S(\rho_{XE}) - S(\rho_E), \tag{57}$$

with $S(\rho) := -\mathrm{tr}(\rho\log_2\rho)$.

Proof: The proof follows by inserting the result from Eq. (20) into Eq. (17) and using Eq. (B7) to express the smooth min-entropy of product states by the conditional von Neumann entropy of a single-copy state. ■

A careful analysis of the proof of Eq. (20) enables us to obtain the main corrections for the secret key rate for coherent attacks [Eq. (52)] in comparison to collective attacks [Eq. (8)]: First, for coherent attacks the probability of measuring a single realization $\mathbf{n}$ for a given tensor-product state is rather small,

which makes the ε environment, for example, in Eq. (51) small. Second, the statistics for the different attacks are not identical in general. Additional fluctuations have to be taken into account as done by considering ξ_{att} [see Eqs. (54) and (56)]. These corrections lose their corrupting influence on the secret key rate, when considering the asymptotic limit ($N \to \infty$, $\varepsilon \to 0$). In this case ξ_{att} becomes zero and no additional fluctuations have to be added to the QBER, thus the corrections vanish. This confirms the equivalence of collective and coherent attacks for permutation-invariant protocols stated in Refs. [17,18] in the asymptotic limit. But for a finite number of signals these corrections have a dramatic impact on the secret key rate. And, since these additional terms seem unavoidable, this might be a hint, that the equivalence of collective and coherent attacks might not hold for permutation-invariant states in the regime of finite resources.

The following section shortly reviews the known postselection technique [21], which we then will compare to Eq. (52).

V. POSTSELECTION—A SHORT REVIEW

In order to determine the quality of r_{coh} [Eq. (52)] from the previous section, we have to compare it to key rates obtained by strategies existing in the literature. Up to now, there exist two main techniques to quantify secret key rates for finite resources for coherent attacks for the whole class of permutation-invariant protocols, namely the de Finetti approach [1,22] and the postselection technique [21]. Since Sheridan *et al.* showed in [7] that the latter technique leads to higher secret key rates, we only take the postselection technique for comparison.

The postselection technique applied to QKD estimates the deviation of the finite key rate r_{post} obtained from a permutation-invariant protocol against coherent attacks from the corresponding rate r_{coll} against collective attacks. The rate of an $\varepsilon_{\text{post}}$-secure key is given by [21]

$$r_{\text{post}} = r_{\text{coll}} - 30 \log_2 (N+1)/N, \tag{58}$$

where r_{coll} is given by Eq. (8) evaluated for the security parameter $\varepsilon_{\text{coll}} = \varepsilon_{\text{post}}(N+1)^{-15}$.

VI. COMPARISON

In this section we compare our newly developed secret key rate r_{coh} [Eq. (52)] and the known rate r_{post} [Eq. (58)] for coherent attacks to the secret key rate evaluated under the assumption of collective attacks r_{coll} [Eq. (8)] for the BB84 protocol and the six-state protocol.

The finite-key rates are calculated for a total security parameter of $\varepsilon := \varepsilon_{\text{coll}} = \varepsilon_{\text{post}} = \varepsilon_{\text{coh}} = 10^{-9}$. In the following let QBER:=Q_m denote the tolerated QBER from the POVM used for parameter estimation [see Eq. (6) and Sec. IV A]. Then the values of $S(X|E)$ and leak_{EC} are fully determined via the estimated QBER P_n. For the BB84 protocol the exact shape of dependence is given by [4]

$$S(X|E) = 1 - h(P_n), \tag{59}$$

$$H(X|Y) = h(P_n), \tag{60}$$

where $h(P) := -P \log_2 P - (1-P)\log_2 (1-P)$ denotes the binary Shannon entropy. This enables us to determine the crucial terms in r_{coh} [Eq. (52)] by

$$\inf_{\rho_{\text{AB}} \in \Gamma_{\text{coh}}} S(X|E) = 1 - h(Q_m + 2\xi_{\text{coh}}(\bar{\varepsilon},n,m)), \tag{61}$$

$$\inf_{\rho_{\text{AB}} \in \Gamma_{\text{coh}}} H(X|Y) = h(Q_m + 2\xi_{\text{coh}}(\bar{\varepsilon},n,m)), \tag{62}$$

and analogously by

$$\inf_{\rho_{\text{AB}} \in \Gamma_{\text{coll}}} S(X|E) = 1 - h(Q_m + 2\xi(\varepsilon_{\text{PE}},n,m)), \tag{63}$$

$$\inf_{\rho_{\text{AB}} \in \Gamma_{\text{coll}}} H(X|Y) = h(Q_m + 2\xi(\varepsilon_{\text{PE}},n,m)), \tag{64}$$

for r_{coll} [Eq. (8)]. For the six-state protocol the entropies can be obtained as [1]

$$S(X|E) = (1-P_n)\left(1 - h\left(\frac{1-\frac{3}{2}P_n}{1-P_n}\right)\right), \tag{65}$$

$$H(X|Y) = h(P_n). \tag{66}$$

Then, analogously to the BB84 case, the evaluation of the infimum in r_{coh} [Eq. (52)] and r_{coll} [Eq. (8)] is determined by replacing P_n by $Q_m + 2\xi_{\text{coh}}(\bar{\varepsilon},n,m)$ and $Q_m + 2\xi(\varepsilon_{\text{PE}},n,m)$, respectively.

The results are obtained from a numerical optimization procedure, which maximizes the key rate with respect to the parameters $m,\bar{\varepsilon},\varepsilon_{\text{PE}},\varepsilon_{\text{EC}},\varepsilon_{\text{PA}}$. Note that then n follows from the fact that for a fixed total number of signals N, the number of sifted bits $n+m$ is fully determined as being a ratio of N. This ratio depends on the actual used protocol. To obtain our results we used an asymmetric protocol, which means that the probabilities of measuring in a certain basis are different. Since in our calculations we take the signals measured in the x (x and y) basis for parameter estimation and generate the key from signals measured in the z (z) basis for the BB84 (six-state) protocol, the measurement probabilities are directly connected to the signals m used for parameter estimation or the signals n used for the key generation. Consequently, the optimization of m determines the measurement probabilities and therefore n.

In Fig. 1 the secret key rates are shown as a function of the initial number of signals N for different QBERs for the BB84 protocol. Figure 2 presents an analogous calculation for the six-state protocol. Note that, as mentioned in Sec. IV B, in both cases we recover the known result that coherent attacks become collective attacks in the limit of infinitely many signals N. For finite N the figures show that the new rate r_{coh} is always significantly higher in comparison to the rate r_{post} obtained from the postselection technique. This advantage of r_{coh} can be seen for a rather small QBER $= 0.01$ as well as for a high value QBER $= 0.1$. For example, we obtain that the increase of r_{coh} in comparison to r_{post} is around 43% for a QBER of 0.01 ($N = 10^6$) and 33% for a QBER of 0.1 ($N = 10^{10}$) for the BB84 protocol. In case of the six-state protocol r_{coh} exceeds r_{post} by around 51% for a QBER of 0.01 ($N = 10^6$) and 45% for a QBER of 0.1 ($N = 10^8$).

The trends of the rates $\frac{m}{N}$ and $\frac{n}{N}$ for different N show in all three approaches that the importance of parameter estimation decreases with increasing N. More precisely, the fraction $\frac{m}{N}$ decreases from a value about $10\% - 20\%$ (for the minimal

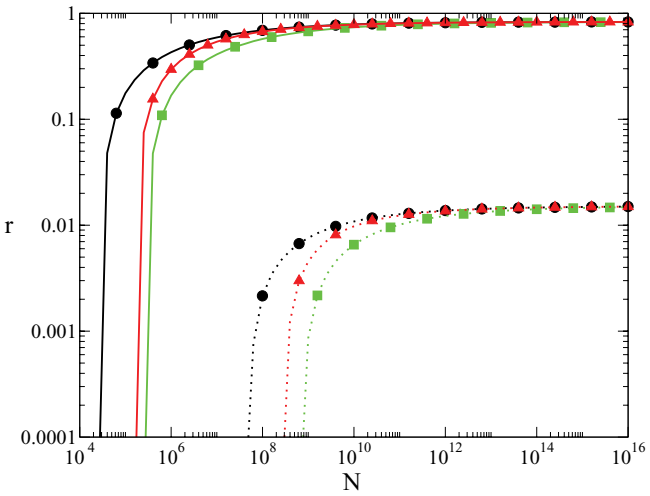


FIG. 1. (Color online) Comparison of the secret key rates r_{coll} [Eq. (8)] (black circles), r_{post} [Eq. (58)] (green squares), and r_{coh} [Eq. (52)] (red triangles) versus the number N of initial signals for different QBERs with security parameter $\varepsilon = 10^{-9}$ for the BB84 protocol in logarithmic scale; QBER $= 0.01$ (straight lines) and QBER $= 0.1$ (dotted lines).

number of signals needed to extract a nonzero key rate) to near 0% (for $N = 10^{16}$) while the ratio of signals $\frac{n}{N}$ related with the final key rate increases from about 60% (for the minimal number of signals needed to extract a nonzero key rate) to near 100% (for $N = 10^{16}$). Note that the effect that the total ratio of sifted signals $\frac{m+n}{N}$ increases from about $70\% - 80\%$ to near 100% is due to the asymmetry in the protocol (see above). In comparison to the case of low numbers of N, where the probability of measuring in different bases has a significant portion, the probability to measure in a single basis used for the generation of the key becomes almost one for large N,

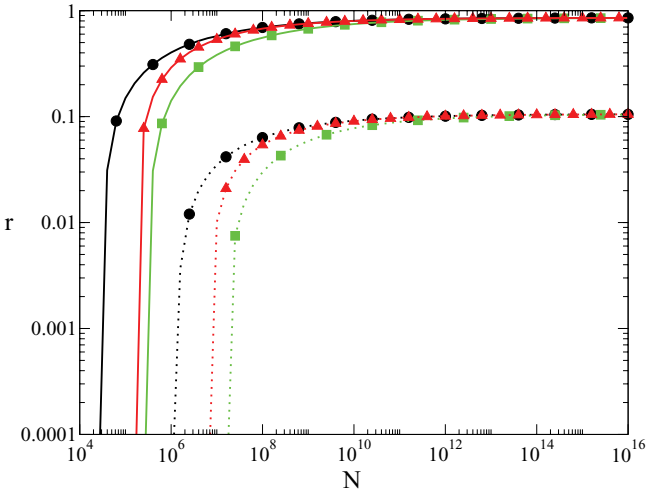


FIG. 2. (Color online) Comparison of the secret key rates r_{coll} [Eq. (8)] (black circles), r_{post} [Eq. (58)] (green squares), and r_{coh} [Eq. (52)] (red triangles) versus the number N of initial signals for different QBERs with security parameter $\varepsilon = 10^{-9}$ for the six-state protocol in logarithmic scale; QBER $= 0.01$ (straight lines) and QBER $= 0.1$ (dotted lines).

such that in this case the number of sifted signals is close to N.

VII. CONCLUSION

In this paper we presented a method to quantify the rate of a secret key for general permutation-invariant protocols for coherent attacks. We show a technique to trace the calculation of secret key rates for coherent attacks back to the analysis of collective attacks. The high quality of this method manifests itself by a comparison to the up to now best-known strategy, the postselection technique. For the treatment of collective attacks we applied the von Neumann entropy bound. We showed that for a finite number of initial signals the secret key rates for the BB84 and the six-state protocol obtained by our method exceed the rates coming from the postselection technique significantly. In case of the BB84 protocol, higher secret key rates have been obtained in Refs. [10,11] by a specialized method, which can, however, not be applied to the six-state protocol. Our method, in contrast, can be applied to all permutation-invariant quantum key distribution protocols for which an analysis of collective attacks is available. Since our results strongly depend on the underlying analysis of collective attacks, a prospective progress in the analysis of collective attacks will automatically cause a progress in our strategy with respect to secret key rates.

Additionally the results of our derivation confirm the known result that, in the limit of infinitely many initial signals, coherent attacks are as powerful as collective attacks. Furthermore, we point out the main impact on the corrections for the key rate against coherent attacks in comparison to collective attacks. Since this extensive impact seems unavoidable, this might give some evidence for the inequivalence of the two types of attacks for finite resources.

Since the assumption of permutation invariance is fairly weak (most protocols used in the literature are permutation invariant or can be made to be), the results of this paper can be widely applied.

ACKNOWLEDGMENTS

We would like to thank Silvestre Abruzzo, Renato Renner, and Marco Tomamichel for helpful discussions. This work was financially supported by Deutsche Forschungsgemeinschaft (DFG) and Bundesministerium für Bildung und Forschung (BMBF), project QuOReP.

APPENDIX A

1. Properties of the (smooth) min-entropy

Lemma 1. Let $\rho_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho^z_{\text{AB}} \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_Z)$ be a classical-quantum state with $\rho_{\text{AB}} = \text{tr}_Z(\rho_{ABZ})$ and $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$, then

$$H^{\varepsilon}_{\min}(\rho_{ABZ}|B) \geqslant H^{\varepsilon}_{\min}(\rho_{\text{AB}}|B). \tag{A1}$$

Proof: For any $\nu > 0$ there exists $\bar{\rho}_{\text{AB}} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{\text{AB}})$ such that for any σ_B,

$$H_{\min}(\bar{\rho}_{\text{AB}}|\sigma_B) \geqslant H^{\varepsilon}_{\min}(\rho_{\text{AB}}|\sigma_B) - \nu.$$

Then it follows with Eq. (B4) that

$$H_{\min}(\bar{\rho}_{ABZ}|\sigma_B) \geqslant H_{\min}(\bar{\rho}_{\mathrm{AB}}|\sigma_B).$$

To conclude the proof it suffices to verify that $\bar{\rho}_{ABZ} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{ABZ})$.

$$\frac{1}{2}||\bar{\rho}_{ABZ} - \rho_{ABZ}||_1 \leqslant \frac{1}{2}||\bar{\rho}_{\mathrm{AB}} - \rho_{\mathrm{AB}}||_1 \leqslant \frac{\varepsilon}{2},$$

where we used the fact that the trace distance cannot increase when applying a quantum operation (see [1], Lemma $A.2.1$). The assertion then follows by choosing σ_B such that

$$H^{\varepsilon}_{\min}(\rho_{\mathrm{AB}}|\sigma_B) = H^{\varepsilon}_{\min}(\rho_{\mathrm{AB}}|B),$$

and the fact that

$$H_{\min}(\bar{\rho}_{ABZ}|B) \geqslant H_{\min}(\bar{\rho}_{ABZ}|\sigma_B). \qquad \blacksquare$$

Lemma 2. Let $\rho_{\mathrm{AB}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $\{|z\rangle\}_z$ a family of orthogonal vectors in $\mathcal{H}_Z$ and $\varepsilon > 0$. Then for a state $\bar{\rho}_{ABZ} := \sum_{z\in\mathcal{Z}} F_z \rho_{\mathrm{AB}} F_z^{\dagger} \otimes |z\rangle\langle z|$ with $\sum_{z\in\mathcal{Z}} F_z^{\dagger} F_z = \mathbb{1}$ and $\mathrm{tr}_Z(\bar{\rho}_{ABZ}) = \rho_{\mathrm{AB}}$,

$$H^{\varepsilon}_{\min}(\rho_{\mathrm{AB}}|B) \leqslant H^{\varepsilon}_{\min}(\bar{\rho}_{ABZ}|B). \tag{A2}$$

Proof: From the definition of $\bar{\rho}_{ABZ}$ it follows immediately that

$$H^{\varepsilon}_{\min}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) = H^{\varepsilon}_{\min}(\rho_{\mathrm{AB}}|B).$$

Then the assertion follows with Lemma 1,

$$H^{\varepsilon}_{\min}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) \leqslant H^{\varepsilon}_{\min}(\bar{\rho}_{ABZ}|B). \tag{A3}$$

$\blacksquare$

Lemma 3. Let $\rho_{\mathrm{AB}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $\{|z\rangle\}_z$ a family of orthogonal vectors in $\mathcal{H}_Z$ and $\varepsilon > 0$. Then for a state $\bar{\rho}_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(Z = z) F'_z \rho_{\mathrm{AB}} F'^{\dagger}_z \otimes |z\rangle\langle z|$ with $\sum_{z\in\mathcal{Z}} F'^{\dagger}_z F'_z = \mathbb{1}$ and $\mathrm{tr}_Z(\bar{\rho}_{ABZ}) = \rho_{\mathrm{AB}}$.

$$H^{\varepsilon}_{\min}(\rho_{AB}|B) \geqslant H^{\varepsilon}_{\min}(\bar{\rho}_{ABZ}|BZ). \tag{A4}$$

Proof: From the definition of $\bar{\rho}_{ABZ}$ it follows immediately that

$$H^{\varepsilon}_{\min}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) = H^{\varepsilon}_{\min}(\rho_{\mathrm{AB}}|B).$$

Then the assertion follows from the strong subadditivity of the smooth min-entropy [see Eq. (B3)], that is,

$$H^{\varepsilon}_{\min}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) \geqslant H^{\varepsilon}_{\min}(\bar{\rho}_{ABZ}|BZ). \tag{A5}$$

$\blacksquare$

Lemma 4. Let $\rho_{ABZ} = \sum_{z\in\mathcal{Z}} P_Z(z) \rho^z_{\mathrm{AB}} \otimes |z\rangle\langle z|$ be a classical quantum state and $\varepsilon, \varepsilon' > 0$, then for any subset $\mathcal{Z}' \subseteq \mathcal{Z}$ such that $\mathrm{Prob}[z \in \mathcal{Z}'] > 1 - \varepsilon'$,

$$H^{\varepsilon+\varepsilon'}_{\min}(\rho_{ABZ}|BZ) \geqslant \inf_{z\in\mathcal{Z}'} H^{\varepsilon}_{\min}\left(\rho^z_{\mathrm{AB}}|B\right). \tag{A6}$$

Proof: For any $\nu > 0$ and $z \in \mathcal{Z}'$ there exists $\bar{\rho}^z_{\mathrm{AB}} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho^z_{\mathrm{AB}})$ such that for any σ^z_B,

$$H_{\min}\left(\bar{\rho}^z_{\mathrm{AB}}|\sigma^z_B\right) \geqslant H^{\varepsilon}_{\min}\left(\rho^z_{\mathrm{AB}}|\sigma^z_B\right) - \nu.$$

Let

$$\bar{\rho}_{ABZ} := \sum_{z\in\mathcal{Z}'} P_{Z'}(z) \bar{\rho}^z_{\mathrm{AB}} \otimes |z\rangle\langle z|.$$

Then it follows with Eq. (B2) that

$$\begin{aligned} H_{\min}(\bar{\rho}_{ABZ}|\sigma_{BZ}) &= \inf_{z\in\mathcal{Z}'} H_{\min}\left(\bar{\rho}^z_{\mathrm{AB}}|\sigma^z_B\right) \\ &\geqslant \inf_{z\in\mathcal{Z}'} H^{\varepsilon}_{\min}\left(\rho^z_{\mathrm{AB}}|\sigma^z_B\right) - \nu. \end{aligned}$$

To conclude the proof it suffices to verify that $\bar{\rho}_{ABZ} \in \mathcal{B}^{\frac{\varepsilon+\varepsilon'}{2}}(\rho_{ABZ})$.

$$\begin{aligned} \frac{1}{2}||\bar{\rho}_{ABZ} - \rho_{ABZ}||_1 &\overset{\text{Eq.(B6)}}{=} \sum_{z\in\mathcal{Z}'} P_{Z'}(z) \frac{1}{2}\left\|\bar{\rho}^z_{\mathrm{AB}} - \rho^z_{\mathrm{AB}}\right\|_1 \\ &\quad + \sum_{z\in\mathcal{Z}\setminus\mathcal{Z}'} P_{Z\setminus Z'}(z) \frac{1}{2}\left\|\rho^z_{\mathrm{AB}}\right\|_1 \\ &\leqslant \frac{\varepsilon}{2} \sum_{z\in\mathcal{Z}'} P_{Z'}(z) + \frac{1}{2} \sum_{z\in\mathcal{Z}\setminus\mathcal{Z}'} P_{Z\setminus Z'}(z) \\ &\leqslant \frac{\varepsilon+\varepsilon'}{2}. \end{aligned}$$

The assertion then follows by choosing σ^z_B such that

$$H^{\varepsilon}_{\min}\left(\rho^z_{\mathrm{AB}}|\sigma^z_B\right) = H^{\varepsilon}_{\min}\left(\rho^z_{\mathrm{AB}}|B\right),$$

and the fact that

$$H_{\min}(\bar{\rho}_{ABZ}|BZ) \geqslant H_{\min}(\bar{\rho}_{ABZ}|\sigma_{BZ}). \qquad \blacksquare$$

Lemma 5. Let $\rho_{ABZ} = \sum_{z\in\mathcal{Z}} P_Z(z) \rho^z_{\mathrm{AB}} \otimes |z\rangle\langle z|$ be a classical quantum state and $\varepsilon_z := P_Z(z)\varepsilon$, then

$$H^{\varepsilon_z}_{\min}(\rho_{ABZ}|BZ) \leqslant H^{\varepsilon}_{\min}\left(\rho^z_{\mathrm{AB}}|B\right). \tag{A7}$$

Proof: For any $\nu > 0$ and $z \in \mathcal{Z}$ there exists $\rho'_{ABZ} \in \mathcal{B}^{\frac{\varepsilon_z}{2}}(\rho_{ABZ})$ such that for any σ_{BZ},

$$H_{\min}(\rho'_{ABZ}|\sigma_{BZ}) \geqslant H^{\varepsilon_z}_{\min}(\rho_{ABZ}|\sigma_{BZ}) - \nu.$$

Then it follows with Eq. (B5) that

$$H_{\min}\left(\rho'^z_{\mathrm{AB}}|\sigma^z_B\right) \geqslant H^{\varepsilon_z}_{\min}(\rho_{ABZ}|\sigma_{BZ}) - \nu.$$

To conclude the proof it suffices to verify that $\rho'^z_{\mathrm{AB}} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho^z_{\mathrm{AB}})$.

$$\begin{aligned} \frac{\varepsilon_z}{2} \geqslant \frac{1}{2}\|\rho'_{ABZ} - \rho_{ABZ}\|_1 &\overset{\text{Eq.(B6)}}{=} \sum_{z\in\mathcal{Z}} P_Z(z) \frac{1}{2}\left\|\rho'^z_{\mathrm{AB}} - \rho^z_{\mathrm{AB}}\right\|_1 \\ &\geqslant P_Z(z) \frac{1}{2}\left\|\rho'^z_{\mathrm{AB}} - \rho^z_{\mathrm{AB}}\right\|_1. \end{aligned}$$

The assertion then follows by choosing σ_{BZ} such that

$$H^{\varepsilon_z}_{\min}(\rho_{ABZ}|\sigma_{BZ}) = H^{\varepsilon_z}_{\min}(\rho_{ABZ}|BZ),$$

and the fact that

$$H_{\min}\left(\rho'^z_{\mathrm{AB}}|B\right) \geqslant H_{\min}\left(\rho'^z_{\mathrm{AB}}|\sigma^z_B\right). \qquad \blacksquare$$

2. Estimation of frequency distributions

Lemma 6. Let $\varepsilon_{\mathrm{PE}} > 0$ and $0 \leqslant k \leqslant N$. Let $\rho^N \in \mathcal{S}(\mathcal{H}^{\otimes N})$ be a permutation-invariant quantum state, and let $\mathcal{E}$ be a POVM on $\mathcal{H}$ which measures the quantum bit error rate (QBER). Let Q_k and Q_{N-k} be the QBERs when applying the measurement $\mathcal{E}^{\otimes k}$ and $\mathcal{E}^{\otimes N-k}$, respectively, to different subsystems of ρ^N.

Then except with probability $\varepsilon_{\mathrm{PE}}$ it holds that

$$\tfrac{1}{2}\|Q_{N-k}-Q_k\|_1 \leqslant \xi(\varepsilon_{\mathrm{PE}},N-k,k), \tag{A8}$$

with $\xi(\varepsilon_{\mathrm{PE}},N-k,k) := \sqrt{\frac{N(k+1)\ln(1/\varepsilon_{\mathrm{PE}})}{8k^2(N-k)}}$.

Proof: It follows from the supplementary information (note 2) of [10] that with $\varepsilon_{\mathrm{PE}} := e^{-\frac{2k(N-k)}{N}\frac{k}{k+1}(2\xi(\varepsilon_{\mathrm{PE}},N-k,k))^2}$,

$$\mathrm{Prob}[Q_n \geqslant Q_k + 2\xi(\varepsilon_{\mathrm{PE}},N-k,k)] \leqslant \varepsilon_{\mathrm{PE}}. \tag{A9}$$

The assertion then follows by negation of the statement. ■

3. Multinomial distribution

Lemma 7. Let $n \in \mathbb{N}$ and $\lambda_i = \frac{n_i}{n}$ for $i = 1,\ldots,4$ with $\sum_{i=1}^4 n_i = n$. Then

$$\frac{n!}{n_1!n_2!n_3!n_4!}\prod_{i=1}^4 \lambda_i^{n_i} > \frac{1}{n^2}, \tag{A10}$$

for $n > 500$.

Proof: After applying the logarithm we get

$$\ln\left(\frac{n!}{n_1!n_2!n_3!n_4!}\prod_{i=1}^4 \lambda_i^{n_i}\right) = \ln(n!) - \sum_{i=1}^4 \ln(n_i!) + n_i \ln\left(\frac{n_i}{n}\right). \tag{A11}$$

By using the Stirling formula,

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n < n! < \left(1+\frac{1}{11n}\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n, \tag{A12}$$

we get for $n > 0$,

$$\begin{aligned}
&\ln(n!) - \sum_{i=1}^4 \ln(n_i!) + n_i \ln\left(\frac{n_i}{n}\right) \\
&> \frac{1}{2}\ln(2\pi n) - \left(\sum_{i=1}^4 \frac{1}{2}\ln(2\pi n_i) + \ln\left(1+\frac{1}{11n_i}\right)\right) \\
&= -\frac{3}{2}\ln(2\pi n) - \left(\sum_{i=1}^4 \frac{1}{2}\ln\left(\frac{n_i}{n}\right) + \ln\left(1+\frac{1}{11n_i}\right)\right) \\
&> -\frac{3}{2}\ln(2\pi n) - 4\ln\left(\frac{12}{11}\right),
\end{aligned} \tag{A13}$$

where we used in the last line that $\frac{1}{2}\ln(\frac{n_i}{n}) < 0$ and $\ln(1+\frac{1}{11n_i}) < \ln(1+\frac{1}{11})$ for $n_i > 0\ \forall i = 1,\ldots,4$. After exponentiation we end up in

$$\frac{n!}{n_1!n_2!n_3!n_4!}\prod_{i=1}^4 \lambda_i^{n_i} > \frac{1}{(2\pi n)^{3/2}}\left(\frac{11}{12}\right)^4 > \frac{1}{n^2}, \tag{A14}$$

which holds for $n > 500$. ■

APPENDIX B: KNOWN RESULTS

Here, we review known results, which are crucial for derivations in the paper.

1. Properties of the (smooth) min-entropy

(1) Chain rule (see [1], Theorem 3.2.12): Let $\rho_{\mathrm{ABC}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ and $\varepsilon \geqslant 0$. Then for $\rho_C = \mathrm{tr}_{\mathrm{AB}}(\rho_{\mathrm{ABC}})$,

$$H_{\min}^{\varepsilon}(\rho_{\mathrm{ABC}}|B) \leqslant H_{\min}^{\varepsilon}(\rho_{\mathrm{ABC}}|BC) + \log_2(\mathrm{rank}(\rho_C)). \tag{B1}$$

(2) Conditioning on classical information (see [1], Theorem 3.2.12): Let $\rho_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_{\mathrm{AB}}^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_Z)$ a classical-quantum state, then

$$H_{\min}(\rho_{ABZ}|BZ) = \inf_{z\in\mathcal{Z}} H_{\min}\left(\rho_{\mathrm{AB}}^z\middle|B\right). \tag{B2}$$

(3) Strong subadditivity (see [1], Theorem 3.2.12): Let $\rho_{\mathrm{ABC}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ and $\varepsilon \geqslant 0$, then

$$H_{\min}^{\varepsilon}(\rho_{\mathrm{ABC}}|BC) \leqslant H_{\min}^{\varepsilon}(\rho_{\mathrm{AB}}|B). \tag{B3}$$

(4) Partial-trace operation on classical subsystem can only decrease min-entropy (see [1], Lemma 3.1.9): Let $\rho_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_{\mathrm{AB}}^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_Z)$ be a classical-quantum state with $\rho_{\mathrm{AB}} = \mathrm{tr}_Z(\rho_{ABZ})$ and $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$, then

$$H_{\min}(\rho_{ABZ}|\sigma_B) \geqslant H_{\min}(\rho_{\mathrm{AB}}|\sigma_B). \tag{B4}$$

(5) Quantum operations can only increase min-entropy (see [26], Theorem 18): Let $\rho_{\mathrm{AB}} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and let $\mathcal{E}$ be a quantum operation such that $\bar{\rho}_{\mathrm{AC}} = (\mathbb{1}_A \otimes \mathcal{E})\rho_{\mathrm{AB}}$, then

$$H_{\min}^{\varepsilon}(\bar{\rho}_{\mathrm{AC}}|C) \geqslant H_{\min}^{\varepsilon}(\rho_{\mathrm{AB}}|B). \tag{B5}$$

(6) Trace distance of mixtures (see [1], Lemma A.2.2): Let $\rho_{AZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_A^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_Z)$ be a classical-quantum state and an analogous definition for ρ'_{AZ}, then

$$\frac{1}{2}\|\rho_{AZ}-\rho'_{AZ}\|_1 = \sum_{z\in\mathcal{Z}} P_Z(z)\frac{1}{2}\left\|\rho_A^z - \rho_A'^z\right\|_1. \tag{B6}$$

(7) Smooth min-entropy of quantum tensor-product states (see [1], Corollary 3.3.7): Let $\rho_{XE}^{\otimes n} \in \mathcal{S}((\mathcal{H}_X \otimes \mathcal{H}_E)^{\otimes n})$ a classical-quantum tensor-product state and $\varepsilon \geqslant 0$, then

$$H_{\min}^{\varepsilon}\left(\rho_{XE}^{\otimes n}\middle|E\right) \geqslant n\left(S(X|E) - 5\sqrt{\frac{\log_2(2/\varepsilon)}{n}}\right), \tag{B7}$$

where $S(X|E) = S(\rho_{XE}) - S(\rho_E)$ with $S(\rho) := -\mathrm{tr}(\rho\log_2\rho)$.

2. Estimation of frequency distributions

Lemma 8. [18,27] Let $\varepsilon_{\mathrm{att}} > 0$ and $0 \leqslant k \leqslant N$. Let $\rho^N \in \mathcal{S}(\mathcal{H}^{\otimes N})$ be a permutation-invariant quantum state, and let $\mathcal{E}$ and $\mathcal{F}$ be POVMs on $\mathcal{H}$ with $|\mathcal{E}|$ and $|\mathcal{F}|$ outcomes, respectively. Let $\mathbf{Q}_k^{\mathcal{E}}$ and $\mathbf{Q}_{N-k}^{\mathcal{F}}$ be the frequency distribution of the outcomes when applying the measurement $\mathcal{E}^{\otimes k}$ and $\mathcal{F}^{\otimes N-k}$, respectively, to different subsystems of ρ^N. Finally, let Ω be any convex set of density operators such that, for any operator A on $n-1$ subsystems, the normalization of $\mathrm{tr}_{n-1}(\mathbb{1}\otimes A\rho^n\mathbb{1}\otimes A^\dagger)$ is contained in Ω. Then except with

probability ε_{att}, there exists a state $\sigma \in \Omega$ such that

$$\frac{k}{N}\frac{1}{2}\left|\left|\mathbf{Q}_k^{\mathcal{E}} - \mathbf{P}_k^{\mathcal{E}}\right|\right|_1 + \frac{N-k}{N}\frac{1}{2}\left|\left|\mathbf{Q}_{N-k}^{\mathcal{F}} - \mathbf{P}_{N-k}^{\mathcal{F}}\right|\right|_1 \leqslant \xi_{\text{att}}(\varepsilon_{\text{att}}, |\mathcal{E}| + |\mathcal{F}|, N), \tag{B8}$$

where $\mathbf{P}_k^{\mathcal{E}}, \mathbf{P}_{N-k}^{\mathcal{F}}$ denote the probability distributions of the outcomes when measuring σ with respect to $\mathcal{E}$ and $\mathcal{F}$, respectively, and $\xi_{\text{att}}(\varepsilon_{\text{att}}, |\mathcal{E}| + |\mathcal{F}|, N) := \sqrt{\frac{8\ln(2)(|\mathcal{E}|+|\mathcal{F}|)+8\ln(1/\varepsilon_{\text{att}})}{N}}$.

[1] R. Renner, Int. J. Quant. Inf. **6**, 1 (2008).
[2] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).
[3] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by Y. Kawano and M. Mosca (Springer, Berlin/Heidelberg, 2008), Vol. 5106 of Lecture Notes in Computer Science, pp. 83–95.
[4] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[5] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[6] R. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).
[7] L. Sheridan, T. P. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).
[8] S. Bratzik, M. Mertz, M. Kampermann, and D. Bruss, Phys. Rev. A **83**, 022330 (2011).
[9] S. Abruzzo, H. Kampermann, M. Mertz, and D. Bruß, Phys. Rev. A **84**, 032321 (2011).
[10] M. Tomamichel, C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).
[11] M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012).
[12] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Algorithmica **34**, 372 (2002).
[13] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).
[14] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).
[15] J. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[16] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[17] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[18] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[19] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[20] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[21] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[22] R. Renner, Nature Physics **3**, 645 (2007).
[23] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[24] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[25] B. Kraus, C. Branciard, and R. Renner, Phys. Rev. A **75**, 012316 (2007).
[26] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).
[27] M. Christandl, R. Renner, and A. Ekert, arXiv:cond-mat/0402131.

"Secret key rates for coherent attacks."
Mertz, M., Kampermann, H., Bratzik, S. und Bruß, D.
Physical Review A **87**, 012315, 2013.

Journal: Physical Review A
Impact factor: 3,042
Anteil an der Arbeit: 5%, Revision und Editieren des Manuskriptes

Erklärung

Die vorliegende Dissertation habe ich eigenständig und ohne Verwendung unerlaubter Hilfsmittel angefertigt. Sie wurde bisher nicht in identischer oder ähnlicher Form bei einer anderen Institution eingereicht. Ich habe bisher keine erfolglosen Promotionsversuche unternommen.

Düsseldorf, 26. März 2014

(Sylvia Marta Bratzik)

Eidesstattliche Versicherung

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.

Düsseldorf, 26. März 2014

(Sylvia Marta Bratzik)