Long distance quantum key distribution with quantum repeaters

Inaugural-Dissertation

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

vorgelegt von

Silvestre Abruzzo
aus Nocera Inferiore, Italien

Düsseldorf, November 2013

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

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

Referent: Prof. Dr. Dagmar Bruß
1. Koreferent: Prof. Dr. Peter van Loock

Tag der mündlichen Prüfung: 16.01.2014

Acknowledgments

I would like to thank Prof. Dr. Dagmar Bruß for taking me as a doctoral researcher in her group. I have appreciated it and I thank for all the help, the discussions, the advice and the support in these last years. Then I thank Dr. Hermann Kampermann for always having the door open to hear my ideas, my problems and complaints. I thank him for giving me very useful advice and critics. Then, I thank my room mate S. Bratzik for the many hours spent in scientific discussions. I wish to thank all components of our group and in particular Dr. Alex Streltsov, Dr. Marcus Mertz, Junyi Wu, Michael Epping, Jochen Szangolies, Dr. Zahra Shadman and Dr. Colin Wilmott. A special thanks goes also to Matteo Rossi who visited our group for six months. In addition, I would like to thank Nadja K. Bernardes and Peter van Loock for many hours spent in discussing quantum repeaters. There are many persons , I have met and with whom I have discussed during the time of my doctoral research. In the following there is a not complete list of persons which I would like to thank: Dr. Matthias Kleinmann, Dr. Tobias Moroder, Prof. Dr. Otfried Gühne, Dr. Sabine Wölk, Renè Schwonnek, Prof. Dr. Norbert Lütkenhaus, Dr. Marco Tomamichel, Prof. Dr. Renato Renner, Dr. Fabian Furrer, Dr. Torsten Franz, Jörg Duhme, Dr. Michele Dall'Arno, Dr. Irene Bolognino, Dr. Andrea Cavagliá, Michele Allegra, Prof. Dr. Miloslav Dusek, Prof. Dr. Giovanna Morigi and Dr. Stephan Ritter.

Finally, last but not least, I thank my wife, my father, my mother, my mother- and father-in-law for supporting me in these last years. A special thank goes also to my dear son Pietro who with his big progresses everyday motivates me to improve and do my best always.

List of included publications

Finite-key analysis of the six-state protocol with photon-number-resolution detectors.
S. Abruzzo, M. Mertz, H. Kampermann, and D. Bruß.
Proc. SPIE, 8189:818917, 2011.

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

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

Measurement-device independent quantum key distribution with quantum memories.
S. Abruzzo, H. Kampermann, and D. Bruß.
ArXiv: 1306.3095, 2013. (accepted in Phys. Rev.A)

Finite-range multiplexing enhances quantum key distribution via quantum repeaters.
S. Abruzzo, H. Kampermann, and D. Bruß.
ArXiv: 1309.1106, 2013. (accepted in Phys. Rev.A)

Abstract

Quantum cryptography, or more precisely, quantum key distribution (QKD) allows two parties to share a secret key which can be used for symmetric-key cryptography. The advantage to use quantum states over classical bits is that they permit to catch a possible eavesdropper who tries to acquire information about the secret key. Therefore, QKD has attracted a lot of attention in recent years. After the initial developments and experimental realizations there are now very complex protocols and quantum devices to realize such protocols. However, it would be desirable to enable quantum key distribution over large distances, i.e. continental and intercontinental distances. For this purpose quantum repeaters have been proposed. These are protocols which exploit entanglement and quantum information primitives as entanglement swapping and entanglement distillation. The final aim is to create a long-distance entangled pair. This pair may be then used for quantum key distribution. Although quantum repeaters have been proposed 15 years ago, the analysis of their requirements and performance in connection to QKD is still in its infancy.

In this dissertation we give first a short presentation of quantum key distribution and quantum repeaters. Then we discuss our results. In order to study the efficiency of a quantum repeater we consider the secret key rate, and for analyzing minimal requirements we calculate the threshold quantum bit error rate, which represents the maximal noise that is compatible with the generation of a secret key.

We start our analysis by describing the requirements and the performance of three important quantum repeater protocols, namely the original quantum repeater, the hybrid quantum repeater and the quantum repeater based on linear optics and atomic ensembles. Then we optimize the quantum repeater protocols and we find the trade-off between the amount of entanglement distillation and entanglement swapping as a function of the quantum device parameters.

After this general investigation, we concetrate on protocols which may be realized in the near future, i.e. protocols with only one repeater station. Such protocols, when considered without quantum memories are called measurement-device independent QKD. This kind of protocols have attracted considerable attention in the last two years both from the experimental and theoretical side. In this thesis we have generalized such protocols to the scenario where there are quantum memories. We have proven that even when quantum memories are imperfect it is possible to improve over protocols with quantum memories. Then we have considered scenarios where in the quantum repeater there are many quantum memories and we have studied the performance of multiplexing. We have introduced the concept of finite-range multiplexing and we have shown that finite-range connections are sufficient in order to have most of the advantage of full-range multiplexing.

Finally we have considered finite-key corrections for the six-state protocol when common imperfections are considered. The result of this work can be used as a basis for future study of finite-key corrections in protocols with quantum repeaters.

The results of this dissertation clarify the role of imperfections in quantum repeaters when used for quantum key distribution. Our calculation of the minimal requirements help experimental groups to concentrate their effort on proper figure of merits. On the other side, our study on quantum repeaters with two segments are promising to beat in the near-future long distance QKD without quantum repeaters.

Zusammenfassung

Quantenkryptographie, oder genauer gesagt, Quantenschlüsselverteilung, ermöglicht zwei Parteien einen Geheimschlüssel zu teilen, der im Rahmen der symmetrischen Kryptographie benutzt werden kann. Im Unterschied zu klassischen Bits haben die Quantenzustände den Vorteil, dass sie erlauben den eventuellen Eavesdropper abzufangen, der nach Informationen über Geheimschlüssel sucht. Deswegen hat Quantenschlüsselverteilung in den letzten Jahren viel Aufmerksamkeit auf sich gezogen. Dank den ersten Entwicklungen und experimentellen Versuchen gibt es heutzutage sehr komplexe Protokolle und Quantengeräte, um diese Protokolle auszuführen. Jedenfalls wäre es wünschenswert die Quantenschlüsselverteilung auf großen Entfernungen, kontinental und interkontinental, einsetzen zu können. Zu diesem Zweck werden die Quantenrepeater vorgeschlagen. Darunter versteht man Protokolle, die Verschränkungstausch und Verschränkungsdestillierung verwenden. Das Endziel ist dabei ein verschränktes Paar für große Entfernungen zu erzeugen. Dieses Paar könnte dann für Quantenschlüsselverteilung gebraucht werden. Obwohl die Quantenrepeater bereits vor 15 Jahren vorgeschlagen wurde, befindet sich die Voraussetzungs-und Leistungsanalyse in Verbindung mit Quantenverschlüsselung immer noch in der Anfangsphase.

In dieser Arbeit gehen wir kurz auf die Grundlagen der Quantenschlüsselverteilung und auf die Quantenrepeater ein. Anschließend diskutieren wir unsere Ergebnisse. Um die Effizienz von Quantenrepeatern zu erforschen berücksichtigen wir die Schlüsselrate, und zur Analyse der minimalen Voraussetzungen berechnen wir die Schwellen-Quantenfehlerrate, die das maximal tolerierbare Rauschen darstellt, bei dem die Schlüsselerzeugung noch möglich ist. Wir beginnen die Analyse mit der Beschreibung von Voraussetzungen und Leistung von drei wichtigen Quantenrepeatern, und zwar sind das der originale Quantenrepeater, Hybridquantenrepeater und Quantenrepeater mit linearer Optik und atomaren Ensembles. Danach optimieren wir die Quantenrepeaterprotokolle und finden den Trade-Off zwischen der Anzahl der Verschränkungsdestillierungsrunden und dem Verschränkungstausch als Funktion der Quantenrepeaterparameter.

Nach diesen allgemeinen Forschungen konzentrieren wir uns auf die Protokolle, die in der nächsten Zukunft realisiert werden könnten, d.h. von Protokollen mit einer einzigen Repeaterstation. Solche Protokolle, wenn ohne Quantenspeicher, werden als ”von Messgeräten unabhängige Quantenverschlüsselung”genannt. Diese Protokollart zog auf sich beträchtliche Aufmerksamkeit in den letzten zwei Jahren, sowohl von theoretischer als auch von experimenteller Seite. In dieser Arbeit verallgemeinern wir solche Protokolle zum Szenario mit den vorhandenen Quantenspeichern. Wir haben bewiesen, dass auch bei nicht-perfekten Quantenspeichern es möglich ist die Protokolle mit den Quantenspeichern zu verbessern. Außerdem beachten wir die Szenarien, wo ein Quantenrepeater mehrere Quantenspeicher besitzt und studieren die Leistung von Multiplexing. Wir führen das Konzept von ”Kurz-LängeMultiplexing ein und zeigen, dass Kurz-Länge Verbindungen ausreichend sind um die meisten Vorteile von ”Voll-LängeMultiplexing auszunutzen.

Am Ende werden finite-key Korrekturen für Six-State-Protokoll bei gewöhnlichen Fehlerquellen in Betracht gezogen. Die Ergebnisse dieser Arbeit können als Grundlage für zukünftige Forschung der finite-key Korrekturen bei Protokollen mit Quantenrepeatern gebraucht werden.

Die Ergebnisse dieser Doktorarbeit definieren die Rolle von Fehlerquellen bei Quantenrepeatern, die für Quantenverschlüsselung benutzt werden. Unsere Berechnung von minimalen Voraussetzungen hilft den experimentellen Gruppen sich auf relevante Leistungszahl zu konzentrieren. Andererseits versprechen unsere Forschungen von Quantenrepeatern

mit zwei Segmenten die Möglichkeit in der nächsten Zukunft Quantenverschlüsselung auf großer Entfernung ohne Quantenrepeatern zu übertreffen.

Contents

1 Introduction

Quantum theory [53] has fascinated at least four generations of physicists, scientists and even non-specialists. Common feelings and discussions are related to its oddities as for example the superposition principle, quantum nonlocality expressed by entangled states, the complementarity and the uncertainty principle. Most of these features have been considered mostly philosophical aspects of quantum theory and the main focus has been the examination of property of matter. The success of quantum theory has been enormous. Examples of technological devices based on quantum theory are lasers, transistors, superconducting materials and nanotechnology [79].

At the same time of the creation of quantum theory, a different group of scientists created information [93] and complexity [100] theory. The purpose of the first is to find optimal protocols for transmitting information and to characterize optimal performances of transmission channels. The goal of the second is to quantify minimal resources needed for a certain computation. Achievements of these two theories are visible in our life everyday: computers, mobile communication devices, online banking based on cryptographic algorithms, etc. One common feature of all these applications is that they are based on classical physics and on the notion of *bit* which is a variable that can assume only two values.

Quantum information theory [18] was born with the purpose to exploit quantum mechanics for communication and computation algorithms. This is a paradigm shift, all features of quantum mechanics considered oddities before the creation of quantum information were considered resources to exploit for faster computation algorithms or more secure cryptographic protocols. Quantum mechanics has become a tool for extracting information from matter.

Quantum key distribution (QKD) has been created by Bennett and Brassard in 1984 (BB84) [16] after the first pioneering work of S. Wiesner about quantum money [104]. BB84 is a protocol for permitting two parties, usually called Alice and Bob to share a secret key. This is a very important task because as proven by Shannon [94] in order to transmit a secret message it is necessary (and sufficient) to have a secret key which has the same length of the message and that it is completely random. According to [89], initially, QKD has not attracted much attention probably because [16] was published in the proceeding of a conference. This field has been then rediscovered by A. Ekert [42] who created a conceptually different protocol w.r.t. BB84 based on entanglement. This protocol was published in a physical journal and it attracted much more attention. Very soon in [17] Bennett, Brassard and Mermin proved that the original BB84 is equivalent to the protocol based on entanglement created by Ekert. More or less at the same time also the first experimental realization of QKD has been made [15]. Right now, according to academic databases there are at least 3000 scientific papers on the field of quantum key distribution and quantum cryptography. There are several companies selling devices for QKD as for example: id Quantique (Geneva), MagiQ Technologies (New York), QuintessenceLabs (Australia) and SeQureNet (Paris). Moreover, other companies including Toshiba, HP, IBM and NEC have active research programs in QKD. Famous and popular achievements of quantum key distribution include a bank transfer which was performed in Vienna, Austria in 2004. Moreover, QKD has been used for transferring ballot results in the Swiss canton of Geneva in 2007.

Common to the achievements we have considered in the previous paragraph is that QKD has been performed at distances not larger than a few tens of kilometers. The reason is that the preferred means used for preparing quantum states are photons which are sent through optical fibers. Due to photon losses the actual maximal distance where QKD remains practical is about 150 km. Therefore, in 1998 H. Briegel and W. Dür, J. I Cirac and P. Zoller proposed the concept of a *quantum repeater* [28]. A quantum repeater protocol is based on entanglement swapping [19, 59] and entanglement distillation [21, 37, 28]. Using these ingredients it is possible to increase the final rate and to have entangled states and hence quantum key distribution at continental and intercontinental distances. Since the first paper, scientist made a great effort to find new protocols which are more experimentally suitable and also to develop quantum devices permitting to enable the construction of a whole quantum repeater. According to [87] all ingredients and basic building blocks for a quantum repeater have been realized. However, it is still missing a quantum repeater which outperforms direct transmission.

The work of this dissertation has been performed within a project of the Federal Ministry of Education and Research (BMBF) with name *QuOReP - Quanten-Repeater-Plattform mit Methoden der Quantenoptik*. Our group in Düsseldorf concentrated on the analysis of the security and efficiency of realistic quantum repeaters (Titel: Sicherheits- und Effizienzanalyse für realistische Quantenrepeater).

The dissertation is organized as follows:

- in Chapter 2 we review fundamental notions of quantum mechanics and quantum information,
- in Chapter 3 we describe entanglement-based QKD,
- in Chapter 4 we treat quantum repeaters and its building blocks,
- in Chapter 5 we will introduce all main results of this dissertation,
- in Chapter 6 we will give our conclusions and we will outline possible future directions.

All five publications which are discussed in Chapter 5 are included in the attachment of this thesis.

2 Fundamentals

This chapter is organized in two conceptual parts. The first part consists of three sections and explains what are quantum states, how they evolve and how they can be measured. During the explanations we will give relevant examples that will be used throughout the thesis. In the second part, in sec. 2.4, we will give basic definitions of classical and quantum information theory. References covering the topics of this chapter are [36, 64, 80, 30, 53, 62, 48, 35].

2.1 Quantum states

In this section we introduce the qubit, we present how to treat composite systems and we give the definition of separable and entangled quantum states. Finally, we introduce several useful quantum states.

2.1.1 Qubits

A quantum bit or qubit[1] is a two-state quantum mechanical system. This is the direct generalization of a classical bit which can assume values 0 and 1. In contrast to this one, a qubit can be also in a generic superposition of the basis states $|0\rangle$ and $|1\rangle$, i.e.

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

The complex coefficients α, β are such that $|\alpha|^2 + |\beta|^2 = 1$ which corresponds physically to the requirement that the probability to find the state $|\psi\rangle$ in one of the states $|0\rangle$ or $|1\rangle$ is 1. Mathematically, the states $|0\rangle, |1\rangle$ are vectors forming a basis of a two-dimensional Hilbert space[2] $\mathcal{H}$. Examples of qubits are:

- **Polarization states of a photon**:
  - Rectilinear polarization with basis $|0\rangle$ and $|1\rangle$
  - Diagonal polarization with basis $|\pm\rangle := \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$
  - Circular polarization with basis $|\tilde{\pm}\rangle := \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}$
- **electron spin** with basis $|\uparrow\rangle$ and $|\downarrow\rangle$.

[1] The term qubit has been coined by B. Schumacher in [92]. However, two-level systems in quantum information had been used already by S. Wiesner in [104].

[2] In this thesis we deal only with finite-dimensional spaces and the following definition is restricted to this case. A *complex vector space* is a vector space where linear combinations of vectors can be made with arbitrary complex numbers. An *inner product space* is a space where for each two elements, an inner product $(\cdot, \cdot) \to [0, \infty)$ is defined. A *Hilbert space* $\overline{\mathcal{H}}$ is a complex vector space equipped with an inner product. A *projective Hilbert space* $\mathcal{H}$ is a set of equivalence classes where the equivalence relation $\sim$ is

$$\mathbf{a} \sim \mathbf{b} \quad \Longleftrightarrow \quad \mathbf{a} = \lambda \mathbf{b}, \tag{2.2}$$

where λ is a complex number. We denote with a ket $|a\rangle$ the element of the equivalence with norm 1, i.e. $\langle a|a\rangle = 1$. In the following whenever we will use the expression *Hilbert space* we always mean *projective Hilbert space.*

The most general representation of a quantum state can be given in terms of a density matrix ρ. Density matrices are hermitian ($\rho = \rho^\dagger$), positive semi-definite ($\rho > 0$) and with trace one ($\mathrm{tr}(\rho) = 1$).

The most general qubit can be written as

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{n} \cdot \boldsymbol{\sigma}), \tag{2.3}$$

where the polarization vector $\mathbf{n}$ is a three-dimensional vector with real coefficients such that $|\boldsymbol{n}|^2 \leq 1$ and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ with $\sigma_x, \sigma_y, \sigma_z$ being the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.4}$$

Quantum states for which the density operator ρ is also a projector are called pure states ($\mathrm{tr}(\rho^2) = 1$) otherwise they are called mixed states ($\mathrm{tr}(\rho^2) < 1$) .

2.1.2 Composite systems

Consider two quantum systems A and B and let us denote by $\mathcal{H}_A$ and $\mathcal{H}_B$ the Hilbert spaces related to these two systems. Then the total space is the tensor product[3]

$$\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B. \tag{2.8}$$

A general pure state in $\mathcal{H}_{AB}$ is

$$|\psi\rangle_{AB} := \sum_{x,y} q_{x,y} |x\rangle_A \otimes |y\rangle_B, \tag{2.9}$$

with $q_{x,y}$ such that $|\psi\rangle_{AB}$ is a quantum state. The state $|\psi\rangle_{AB}$ is called *separable* if $q_{x,y} := c_x p_y$ and therefore $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\zeta\rangle_B$. If a state is not separable, then it is *entangled.* Examples of *maximally entangled states* are the *Bell states*

$$|\phi^\pm\rangle_{AB} := \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}), \tag{2.10}$$

$$|\psi^\pm\rangle_{AB} := \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}). \tag{2.11}$$

Regarding mixed states[4], a state is separable if

$$\rho_{AB} := \sum_i p_i \phi_A^{(i)} \otimes \zeta_B^{(i)}, \tag{2.12}$$

where p_i are positive numbers such that $\sum_i p_i = 1$ and $\phi_A^{(i)}, \zeta_B^{(i)}$ are density matrices. A mixed state which is not separable is entangled. Examples are:

[3] For all couples of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ we define the *tensor product space* $\mathcal{H}_A \otimes \mathcal{H}_B$ as the Hilbert space spanned by the elements $|a\rangle \otimes |b\rangle$ with $|a\rangle \in \mathcal{H}_A$ and $|b\rangle \in \mathcal{H}_B$ such that the following relations

$$(|a\rangle + |a'\rangle) \otimes |b\rangle = |a\rangle \otimes |b\rangle + |a'\rangle \otimes |b\rangle, \tag{2.5}$$

$$|a\rangle \otimes (|b\rangle + |b'\rangle) = |a\rangle \otimes |b\rangle + |a\rangle \otimes |b'\rangle, \tag{2.6}$$

hold for any $|a\rangle, |a'\rangle \in \mathcal{H}_A$ and $|b\rangle, |b'\rangle \in \mathcal{H}_B$. The inner product is defined as follows:

$$(\langle a| \otimes \langle b|)(|a'\rangle \otimes |b'\rangle) = \langle a|a'\rangle\langle b|b'\rangle. \tag{2.7}$$

[4] According to [57] this definition is due to [103].

- **Depolarized Bell states**. These are states of the form

$$\rho(p) := p|\phi^+\rangle\langle\phi^+| + \frac{1-p}{4}\mathbb{1}. \tag{2.13}$$

It is possible to show that for $p > \frac{1}{3}$ the state above is entangled, otherwise it is separable. The state $\rho(p)$ can also be written as

$$\rho(p) \equiv \frac{1+3p}{4}|\phi^+\rangle\langle\phi^+| + \frac{1-p}{4}\left(|\phi^-\rangle\langle\phi^-| + |\psi^-\rangle\langle\psi^-| + |\psi^+\rangle\langle\psi^+|\right) \tag{2.14}$$

The coefficient $F := \frac{1+3p}{4}$ is called the fidelity of $\rho(p)$ with respect to the quantum state $|\phi^+\rangle\langle\phi^+|$ and it represents the overlap between these two states, i.e. $F := \mathrm{tr}(\rho(p)|\phi^+\rangle\langle\phi^+|)$.

- **Binary states**: These are states of the form

$$\rho(p) := p|\phi^+\rangle\langle\phi^+| + (1-p)|\phi^-\rangle\langle\phi^-|. \tag{2.15}$$

This state is entangled for $p \neq \frac{1}{2}$.

2.1.3 Fock states

For application to quantum repeaters it is necessary to introduce the Fock space [46] and to give a notation for the quantum states in this space. For simplicity we consider bosonic systems, as we are interested in quantum states of light and photons are bosons. The *annihilation* and *creation operators* d and $d^\dagger$ are such that

$$[d, d^\dagger] := dd^\dagger + d^\dagger d = \mathbb{1}. \tag{2.16}$$

We define the *number operator* as $n := dd^\dagger$ and we denote its eigenstates as $|n\rangle$, i.e.,[5]

$$n|n_F\rangle = n|n_F\rangle. \tag{2.17}$$

The operator $d^\dagger$ is called creation operator because $d^\dagger|n_F\rangle = \sqrt{n+1}|n+1_F\rangle$, and d is called annihilation operator because $d|n_F\rangle = \sqrt{n}|n-1_F\rangle$. We denote the vacuum as $|0_F\rangle$. A generic Fock state is a state of the form

$$|\phi\rangle := \sum_{n=0}^{\infty} \alpha_n |n_F\rangle, \tag{2.18}$$

where the complex coefficients α_n are such that $\sum_{n=0}^{\infty} |\alpha_n|^2 = 1$.

We give now examples of relevant quantum states in quantum repeater setups:

1. **Coherent states** [51]. Proposed by R.J. Glauber, the general form is

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}} |n_F\rangle, \tag{2.19}$$

with α being an arbitrary complex number. Coherent states will be considered during the discussion of hybrid quantum repeaters.

[5] We use the notation $|n_F\rangle$ for not generating confusion with the states $|0\rangle$ and $|1\rangle$ defined in sec. 2.1.1.

2. **Phase randomized coherent states** [72]. These states are used in quantum key distribution. Let $\alpha = e^{i\theta}\sqrt{\mu}$, then they are defined by

$$\rho_\mu := \int_0^{2\pi} \frac{d\theta}{2\pi} |e^{i\theta}\sqrt{\mu}\rangle\langle e^{i\theta}\sqrt{\mu}| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n_F\rangle\langle n_F|. \tag{2.20}$$

The quantity $\mu = |\alpha|^2$ is the mean photon number. For application to QKD, it is necessary to consider $\mu \ll 1$ in such a way that $\rho_\mu \propto |0_F\rangle\langle 0_F| + \mu|1_F\rangle\langle 1_F|$. The state above called weak phase randomized coherent pulses and can be used as an approximation of a single photon state.

3. **Spontaneous parametric down conversion (SPDC)** [65, 61]. This type of state is used for producing Bell states probabilistically,

$$\rho_{\text{pair}} := (1-p) \sum_{m=0}^{\infty} \frac{2^m p^m}{(m!)^2(m+1)} (B^\dagger)^m |0_F\rangle\langle 0_F| B^m, \tag{2.21}$$

where $B^\dagger := ({g_H}^\dagger {in_H}^\dagger + {g_V}^\dagger {in_V}^\dagger)/\sqrt{2}$. The operator $g_i^\dagger$ ($in_i^\dagger$) denotes a spatial mode with polarization given by $i = H, V$. The *pumping parameter* p is related to the probability to have an n-photon pulse by $P(n) = p^n(1-p)$. For $p \ll 1$ we obtain $\rho_{\text{pair}} \propto |0_F\rangle\langle 0_F| + p|\phi^+\rangle\langle\phi^+|$.

2.2 Quantum gates and channels

In sec. 2.2.1 we describe unitary evolutions of closed systems. We give examples of quantum gates and describe some linear optics components. Then, in sec. 2.2.2 we treat operations which act only on subsystems and we introduce general quantum channels and some relevant examples for this thesis.

2.2.1 Quantum gates

One postulate of quantum mechanics says that a closed quantum system evolves under a unitary evolution U as follows

$$\rho(t) = U\rho(0)U^\dagger, \tag{2.22}$$

with $UU^\dagger = \mathbb{1}$. The unitary U is related to the Hamiltonian of the system through the Liouville-Von Neumann equation [53]. In quantum information, particular unitaries acting on the space of qubits are called quantum gates [6]. This is in relation to classical gates, which can be composed in order to create more complicated gates. In order to give examples, we fix a basis $\{|0\rangle, |1\rangle\}$ on the space of qubits. The gates presented in the following examples are expressed in this basis:

- **Hadamard gate**. This gate acts on the basis such that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, i.e.

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.23}$$

- **Controlled-Not**. This is a two qubit gate, i.e. it has two input qubits called control and target state and two output qubits called in the same way. Its effect on the corresponding basis states can be described by

[6] See [8] for a comprehensive analysis of quantum gates and their properties.

Input		Output	
Control	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Other, for use important, quantum gates are based on linear optics and they are beamsplitters and polarizing beamsplitters. The theory of lossless beamsplitters was derived in [105, 45]. See also [62, 48] for a recent introduction.

- **Beamsplitter**. This gate is realized with a semi-reflective mirror. When light passes the mirror, part of the light is reflected and part is transmitted. We denote by R the reflectivity and by $T = 1 - R$ the transmittivity. A beamsplitter has as input two spatial modes and as output other two spatial modes. Their relation is

$$a^\dagger_{out} = \sqrt{T}a^\dagger_{in} + \sqrt{R}b^\dagger_{in} \tag{2.24a}$$

$$b^\dagger_{out} = -\sqrt{R}a^\dagger_{in} + \sqrt{T}a^\dagger_{in}. \tag{2.24b}$$

- **Polarizing beamsplitters** transmit completely light with a certain polarization and reflect all light of the opposite polarization.

$$\begin{aligned} a^\dagger_H &\to c^\dagger_H, \qquad & a^\dagger_V \to d^\dagger_V,\\ b^\dagger_H &\to d^\dagger_H, \qquad & b^\dagger_V \to c^\dagger_V. \end{aligned}$$

2.2.2 Quantum channels

In many situations we focus on the evolutions of subsystems. In this case it is possible to describe the evolution of the subsystem using the formalism of quantum channels [64]. Mathematically, a quantum channel $\mathcal{E}$ is a completely positive and trace preserving map (CPTPM). Completely positive means that for any density operator ρ, $\mathcal{E}(\rho)$ and $\mathbb{1} \otimes \mathcal{E}(\rho)$ are positive. Trace preserving means that $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\rho)$. The relevant quantum channels for this thesis are:

- **Depolarizing channel**. For any n-qubit density operator ρ,

$$\mathcal{E}(\rho) := p\rho + \frac{1-p}{2^n}\mathbb{1}, \tag{2.25}$$

  with $0 \leq p \leq 1$.

- **Quantum erasure channel** [23, 52]. Let us consider a three-dimensional Hilbert space, with basis $\{|0\rangle, |1\rangle, |2\rangle\}$ and let us consider a qubit ρ embedded in the subspace described by the vectors $|0\rangle, |1\rangle$. Then the quantum erasure channel is

$$\mathcal{E}(\rho) := p\rho + (1-p)|2\rangle\langle 2|, \tag{2.26}$$

  with $0 \leq p \leq 1$. This type of channel can be used for modeling losses in optical fibers. The state $|2\rangle$ is in this case the vacuum $|0_F\rangle$ and the states $|0\rangle$ and $|1\rangle$ are the states $|1_F\rangle$ of two different modes, e.g. vertical and horizontal polarization of a photon.

- **Depolarizing noise for a quantum gate** [40]. Given a quantum gate U acting on n-qubits, we model an imperfect realization of such a gate using the following quantum channel

$$\mathcal{E}_U(\rho) := pU\rho U^\dagger + \frac{1-p}{2^n}\mathbb{1}, \tag{2.27}$$

  with $0 \leq p \leq 1$.

2.3 Quantum measurements

A quantum measurement of a quantum state ρ is characterized by Kraus operators A_m, where the index m refers to the measurement outcome. Kraus operators satisfy the relation

$$\sum_m A_m^\dagger A_m = \mathbb{1}. \tag{2.28}$$

The probability to measure the outcome m is

$$p_m = \mathrm{tr}(A_m \rho A_m^\dagger). \tag{2.29}$$

The state after the measurement becomes

$$\rho_m := \frac{A_m \rho A_m^\dagger}{p_m}. \tag{2.30}$$

In many situations, when the measurement destroys the quantum state, the resulting quantum state is not relevant and therefore a more compact representation is convenient. This representation is given in terms of positive operator valued measure (POVM). A POVM is a collection of operators E_m such that $\sum_m E_m = \mathbb{1}$. The relation between a POVM and the Kraus operator representation of a measurement is given by the relation $E_m = A_m^\dagger A_m$. Therefore, the probability to measure the outcome m is given by $p_m = \mathrm{tr}(E_m \rho)$. If we add the additional requirement that $E_m E_{m'} = \delta_{m,m'} E_m$ then a POVM reduces to a Von Neumann (or projective) measurement.

With the formalism described above, we formulate the POVM of photon detectors. We consider first photon-number-resolving detectors (PNRD). Elements of a POVM of an ideal PNRD have the form

$$\Pi^{(n)} = |n_F\rangle\langle n_F|, \tag{2.31}$$

where $n = 0, 1, 2, ...$ is the number of incoming photons. More realistic detectors have a finite *detection efficiency* η_D, which is the probability that a detector clicks if a photon is entering in the detector. Such detectors are described by [62]

$$\Pi^{(n)}(\eta_D) := \eta_D^n \sum_{k=n}^{\infty} \binom{k}{n} (1-\eta_D)^{k-n} |k_F\rangle\langle k_F|. \tag{2.32}$$

Note that $\Pi^{(n)}(\eta_D = 1) = |n_F\rangle\langle n_F|$.

Threshold detectors cannot distinguish the photon number but can only distinguish between the vacuum and any non-vacuum state. The POVM in this case has only two elements, and they are

$$\Pi^{(\text{No click})} = \Pi^{(0)}, \tag{2.33a}$$

$$\Pi^{(\text{click})} = \sum_{n=1}^{\infty} \Pi^{(n)} = \mathbb{1} - \Pi^{(0)}. \tag{2.33b}$$

Other relevant measurements are

- Single qubit measurement in the basis i with $i = X, Y, Z$. The POVM is given by the eigenvectors of the Pauli matrix σ_i.

- Bell-state measurement. This is a projective measurement, where the four elements are the projectors on the Bell states.

2.4 Information theory

The purpose of this section is to give the main definitions of information theory that we will use in the following chapter. In sec. 2.4.1 we will introduce the concept of random variables and probability distributions. In sec. 2.4.2 we discuss the Shannon and Von Neumann entropy.

2.4.1 Random variables and probabilities

We consider experiments where the outcome depends on chance. The outcome of the experiment is denoted by X which is called a *random variable.* A random variable can take values in the set $\mathcal{X}$ which we call *alphabet.* We denote by $x \in \mathcal{X}$ a possible value, an *event*, that the random variable X can have. A probability function P_X is a rule which assigns to each event $x \in \mathcal{X}$ a non-negative real number such that $\sum_{x\in\mathcal{X}} P_X(x) = 1$ where the sum runs over all elements of $\mathcal{X}$. Note that in the following, when there is no possibility of ambiguity we will not indicate the subscript X in P_X. Moreover, in sums we will not explicitly write the set of values, we always assume all possible x. Therefore, for example, we will write $\sum_{x\in\mathcal{X}} P_X(x) = 1$ as $\sum_x P(x) = 1$. For each random variable X we define its expectation value as $< X >= \sum_x x\ P(x)$.

2.4.2 Entropies

Shannon entropy We give now the definition of the *Shannon entropy H* of a random variable [93]

$$H(X) := -\sum_x P(x) \log_2 P(x). \tag{2.34}$$

The Shannon entropy is measured in bits and it represents the average unpredictability of a random variable. Relevant properties of the Shannon entropy are

1. $0 \leq H(X) \leq \log_2 |\mathcal{X}|$, where $|\mathcal{X}|$ is the cardinality of the set $\mathcal{X}$.

2. $H(X) = 0$ iff $|\mathrm{supp}(P_X)| = 1$, where supp is the support.

The properties above justify the meaning of Shannon entropy. In fact, if a random variable is completely predictable, i.e. $|\mathit{supp}\ P_X| = 1$ then the entropy is zero. On the other side if the random variable is completely unpredictable, i.e. each event can happen with the same probability $\frac{1}{|\mathcal{X}|}$ then the Shannon entropy is maximized and gives the number of bits needed to represent the alphabet.

A relevant particular case of the Shannon entropy is the *binary Shannon entropy* which is the expression when the alphabet contains only two values and the first value is assumed with probability p and the second value with probability $1-p$. In this case the expression of the Shannon entropy becomes

$$h(p) := -p \log_2 p - (1-p) \log_2 (1-p). \tag{2.35}$$

Shannon conditional entropy In relation to error correction we define the *conditional entropy.* In this scenario we consider that we have two random variables X and Y and we define the uncertainty on X given the knowledge of Y as

$$H(X|Y) := -\sum_{x,y} P_{XY}(x,y) \log_2 P_{X|Y=y}(x). \tag{2.36}$$

Let us consider the binary symmetric channel [35] which is defined by the following relation

$$P(X=0|Y=0)=P(X=1|Y=1)=1-e \tag{2.37}$$

$$P(X=0|Y=1)=P(X=1|Y=0)=e \tag{2.38}$$

The probability e is the *bit error rate* and it represents the probability that the two random variables X and Y take different values. The conditional entropy in this case becomes $H(X|Y)=h(e)$ where $h(e)$ is the binary entropy defined above. When $e=0$ then $X=Y$ and the conditional entropy becomes 0 as the knowledge of Y specifies completely X. On the other side if $e=\frac{1}{2}$ the conditional entropy reaches the maximum as the knowledge of Y gives no information on X.

Von Neumann entropy We extend the definition of Shannon entropy to the case of quantum states. The von Neumann entropy [102] S of a quantum state ρ is defined as

$$S(\rho):=-\mathrm{tr}(\rho\log_2\rho). \tag{2.39}$$

If we write the spectral decomposition of ρ as $\rho=\sum_k \lambda_k|k\rangle\langle k|$, then the von Neumann entropy has the same form of the Shannon entropy, i.e. $S(\rho)=-\sum_k \lambda_k \log_2 \lambda_k$.

3 Entanglement-based quantum key distribution

The idea of Entanglement-based (EB) QKD is due to A. Ekert [42] who rediscovered QKD independently of Bennett and Brassard [16]. Informally speaking, the idea is that a source in the middle between Alice and Bob produces bipartite entangled states and each part of these states is sent to Alice and Bob respectively. In his paper Ekert suggests to relate the security to Bell inequalities [14], which can be used to certify entanglement.

The chapter is organized in this way: in sec. 3.1 we describe how an entanglement-based QKD protocol works and in particular we consider the BB84 and the six-state protocol. In sec. 3.2 we describe the structure of a security proof. In particular, we describe the assumptions, then we give the secret key fraction for an ideal implementation and we show how this last quantity changes if imperfections are present.

3.1 The protocol

In the following we present the entanglement-based version of the famous BB84 [16, 42, 17] and six-state protocol [29, 13]. Such protocols are divided in two parts: the quantum part and the classical post-processing. After the quantum part we describe all classical steps of the protocol which determine the amount of attack of the eavesdropper and to extract a secret key if possible.

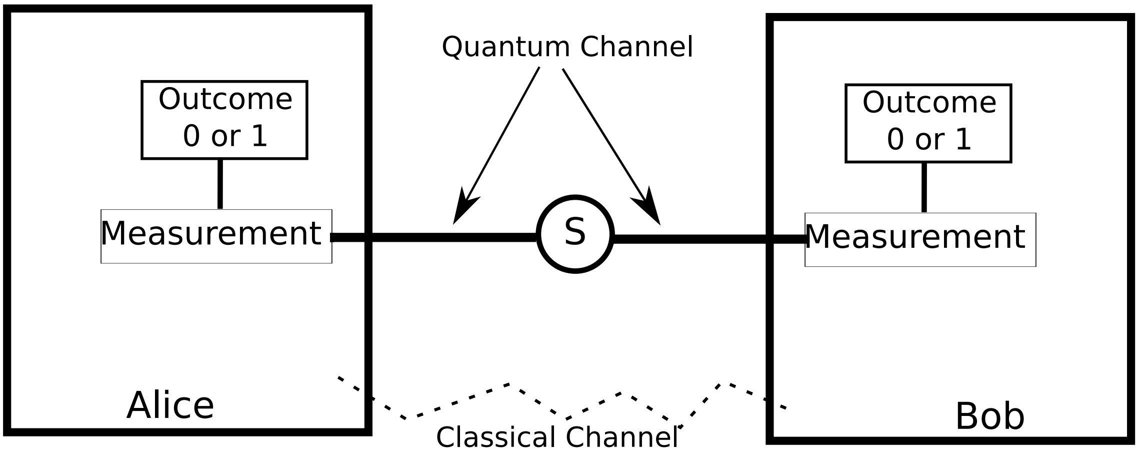


Figure 3.1: Set-up of a generic EB-QKD protocol. In the middle between Alice and Bob there is a source (circle with S inside) sending entangled photons to them through a quantum channel (solid line). The photons are measured in a randomly chosen basis and the outcome 0 or 1 is produced. The choice of the basis is done by trusted random number generators (not shown in the figure). The classical channel (zigzag line) is authenticated but public.

3.1.1 Quantum part

The first part of a QKD protocol involves the preparation and the transmission of quantum states.

The protocol works as follows (see fig. 3.1):

1. A source between Alice and Bob produces bipartite entangled pairs. One part of the pair is sent to Alice and the other one is sent to Bob. The distribution is done using the quantum channel.

2. Alice and Bob choose randomly and independently a measurement basis and they measure the respective part of the pair. The two protocols, BB84 and six-state differ in the number of measurement bases. For the BB84 there are two measurement bases $M_Z := \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and $M_X := \{|+\rangle\langle +|, |-\rangle\langle -|\}$ where $|\pm\rangle := \frac{|0\rangle \pm |1\rangle}{2}$. For the six-state protocol, in addition to M_Z and M_X we consider also $M_Y := \{|\tilde{+}\rangle\langle\tilde{+}|, |\tilde{-}\rangle\langle\tilde{-}|\}$ where $|\tilde{\pm}\rangle := \frac{|0\rangle \pm i|1\rangle}{2}$.

3. The outcome of each measurement is either 0 or 1, thus resulting in a binary string, the *raw key*, on both sides.

3.1.2 Classical post-processing

Once Alice and Bob have classical information consisting of the results of the measurements (the *raw key*) and the choice of the measurement bases, they exchange classical information which allows to estimate the amount of information obtained by Eve and consequently, if possible, to distill a secret key. A crucial assumption in order to make the following procedure work is that the classical channel between Alice and Bob is authenticated [33]. The protocol is the following [89]:

1. **Sifting**: Alice and Bob share information about the measurement bases and they discard all outcomes where they have used different bases.

2. **Parameter estimation**: Alice and Bob exchange a randomly chosen small amount of measurement outcomes which are used for estimating the amount of correlations. If the correlations are high enough they proceed and if the correlations are too weak then they stop.

3. **Error Correction**: [58, 43, 44] At this point Alice and Bob have two lists of outcomes each which are not exactly the same. In this step, they exchange information in order to correct the errors. At the end of this step they have equal keys.

4. **Privacy Amplification**: [22, 20, 85] Alice and Bob reduce the length of their string using classical extractors (hash functions [33]). The final result is the secret key.

3.2 Security analysis

EB-QKD has been shown to be secure by H.K. Lo and H.F. Chau in the year 1999 [68]. The authors considered that Alice and Bob share entangled pairs and that they have at disposal quantum computers able to perform quantum error correction. One year later, P.W. Shor and J. Preskill [95] have shown that the protocol considered in [68] is equivalent to BB84 outlined in sec. 3.1 . Anyway, real implementations of EB-QKD have been done with spontaneous parametric down conversion sources which produce also pulses containing many photons. In order to account for these experimental imperfections which could break the security of the protocol new security proofs and techniques have been developed. The final purpose of each security proof is to give a formula for the secret key fraction which contains all details of the imperfections of the implementation and also the maximal amount of information which could be obtained by an eavesdropper. In the following we will discuss the secret key fraction in the case of an ideal implementation without imperfections, then we will discuss how to include imperfections in the formula of the secret key fraction.

3.2.1 Secret key fraction for a perfect implementation

In this case the only noise affecting the measurement outcomes is attributed to Eve. The eavesdropper can perform many types of attacks [49, 89]. In this thesis we have considered the most general attack which is called *coherent attack*. In general Eve can apply any strategy allowed by the laws of quantum mechanics, in particular she can use ancillary states and apply the most general quantum operation between these states and the quantum states sent to Alice and Bob. Then she will keep the ancillary states and she will use them at any time even after the protocol is finished and the secret key is used. It is remarkably that the only quantity entering in the formula of the secret key fraction is the quantum bit error rate (QBER) which is for each measurement basis the fraction of discordant outcomes. We will denote the QBER as e_X, e_Y and e_Z for the QBERs in direction X, Y and Z.

It is possible to show [86, 89] that the state between Alice and Bob can be reduced to a Bell-diagonal state, i.e. a state of the form

$$\rho_{AB} = A|\phi^+\rangle_{AB}\langle\phi^+| + B|\phi^-\rangle_{AB}\langle\phi^-| + C|\psi^+\rangle_{AB}\langle\psi^+| + D|\psi^-\rangle_{AB}\langle\psi^-|, \tag{3.1}$$

with the probabilities A, B, C and D. The QBER along the directions X, Y and Z is [89]

$$e_X := B + D, \quad e_Z := C + D, \quad e_Y := B + C. \tag{3.2}$$

In the case of the BB84 protocol the asymptotic secret fraction is [38, 60, 63]

$$r_\infty^{BB84} = 1 - h(e_X) - h(e_Z), \tag{3.3}$$

where $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy (see sec. 2.4). This formula has a very simple interpretation [98]. Let's consider a protocol where all outcomes coming from the Z basis are used for producing the secret key and all outcomes coming from the X basis are used for measuring the amount of eavesdropping[1]. Then $h(e_Z)$ represents the fraction of information leaked to the eavesdropper during error correction (see sec. 2.4) and $h(e_X)$ is the amount of information which could be gained by Eve during the eavesdropping.

For the case of the six-state protocol the formula of the asymptotic secret key rate is slightly more complicated [38, 60, 63, 89]

$$r_\infty^{6S} := 1 - e_Z h\left(\frac{1 + (e_X - e_Y)/e_Z}{2}\right) - (1 - e_Z) h\left(\frac{1 - (e_X + e_Y + e_Z)/2}{1 - e_Z}\right) - h(e_Z). \tag{3.4}$$

This formula holds under the assumption that the basis Z is used for extracting a key, which will be chosen with a probability of almost one, and both Y and X are the bases used for parameter estimation.

3.2.2 Including imperfections

Realistic devices move away from ideal devices in many different ways. There are known imperfections which come from design principles, for example a spontaneous parametric down conversion source creates multiphoton states by design (see sec. 2.1.3). Known

[1] This protocol is equivalent to the original BB84 via [69]

imperfections can be characterized and considered in the security proofs. Unknown imperfections which come from errors in the implementation or tampering are not under control and therefore they cannot be easily corrected or accounted for in a security proof[2] The calculation of the secret key rate throughout the whole thesis has been performed assuming that Alice and Bob are able to characterize completely the device used for the quantum key distribution protocol. That means that they have complete control and knowledge of the devices in their labs. However, nothing is assumed about the set-up outside the labs which are controlled by the eavesdropper. The assumptions we considered above are by far the most commons and used in literature [89]. For additional details how to adapt the formula of the secret key rate see [12, 99, 47] and in the context of quantum repeaters see [7, 4].

[2] Modern techniques such as device-independent QKD [82] are able to deal with both type of errors. However, it is not easy to capture everything also in this general type of security proof and attacks are know which could permit an eavesdropper to learn the secret key [10, 9].

4 Quantum repeaters

In this chapter we will give basic information about quantum repeaters, what are the building blocks and what are their performances. In sec. 4.1 we show that losses in optical fibers are a major problem in quantum optical communication. In order to solve this problem, we will in sec. 4.2 describe the simplest quantum repeater set-up. Then in sec. 4.3 we will introduce all building blocks of a quantum repeater and in the successive section (sec. 4.4) we will describe the original quantum repeater protocol proposed in [28].

4.1 Losses in optical fibers

Although quantum key distribution may be realizable for any physical system, in practical cases photons are the unique reasonable choice. Photons are fairly easy to produce, to be transmitted and to be measured. The preferred means for transmitting photons are optical fibers and free-space [50]. In the following we will concentrate on optical fibers.

Optical fibers allow to transmit information from one place to another by transmitting photons. Optical fibers are flexible light pipes usually made of glass or plastic. See [56] for historical information and their todays use. See [11, 6] for an introduction to current implementations and applications, and [49, 89] for information regarding application in quantum key distribution and quantum communication. For the purpose of this thesis optical fibers are within good approximation to be considered lossy but noiseless. Optical losses are governed by the Beer-Lambert law [26, 83, 67]. Let P be the power of the light inserted in the optical fiber, then [6]

$$\frac{dP}{dz} = -\gamma P, \tag{4.1}$$

where z is a coordinate longitudinal to the optical fiber and γ is the *attenuation coefficient*. This coefficient depends on the material used for building the fiber, on the wavelength of the signals, on the shape of the signal, on the temperature and other atmospheric conditions as humidity. The solution of eq. (4.1) leads to the exponential attenuation:

$$P_{\text{out}} = P_{\text{in}} e^{-\gamma L}, \tag{4.2}$$

where L is the distance traveled by the light, P_{in} is the input power and P_{out} is the output power. It is customary to define the absorption coefficient α in dB/km [6],

$$\alpha := -\frac{10}{L} \log_{10} \left(\frac{P_{\text{out}}}{P_{\text{in}}} \right), \tag{4.3}$$

which implies

$$P_{\text{out}} = P_{\text{in}} 10^{-\frac{\alpha L}{10}}. \tag{4.4}$$

In case of single photons, losses remain the same, but instead of speaking of power decay we speak about *transmission probability* which is defined as

$$\eta_{\text{T}}(L) := 10^{-\frac{\alpha L}{10}}. \tag{4.5}$$

The values of losses depend mainly on the wavelength and it is minimal in the two *telecom windows* around 1330 nm for which $\alpha \approx 0.34$ dB/km and around 1550 nm for which $\alpha \approx 0.2$ dB/km.

L (km)	photons/s
10	$6.3 \cdot 10^9$
50	10^9
100	10^8
300	10^4
500	1
800	$10^{-6} \approx 3$ photons/month
1000	$10^{-10} \approx 1$ photon each 3800 years

Table 4.1: Rate of single photons at distance L. We use eq. (4.5) with $\alpha = 0.2$ dB/km. The source is supposed to produce photons with a rate of 10^{10} photons/s.

In tab. 4.1 we give the values of the rate when a source with a frequency of 10^{10} Hz is used. This is a completely futuristic source as current single photon sources are in the order of MHz [41]. As we see, after few hundreds of kilometers the rate is so low that communication becomes impractical. As we will see in the next section, quantum repeaters can solve the problem of photon losses.

4.2 Introduction to quantum repeaters

The purpose of this section is to give a general overview of a quantum repeater and how it works. Later in sec. 4.3 we will discuss with more details all ingredients and why they are really necessary. In sec. 4.4 we will present the original quantum repeater protocol.

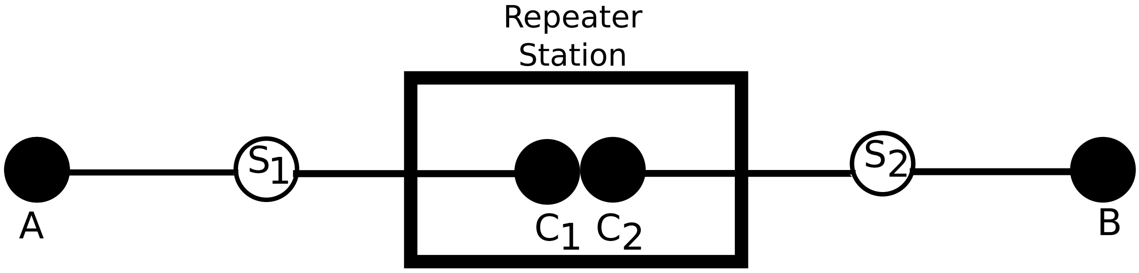


Figure 4.1: Set-up of a two-segment quantum repeater. The filled black circles are quantum memories. The circle with S_1 and S_2 inside are entanglement sources. The distance between Alice (Bob) and the repeater station is $\frac{L}{2}$.

In fig. 4.1 a simple quantum repeater with two segments is depicted. The source S_1 (S_2) produces entangled photons which are sent to the quantum memories A and C_1 (C_2 and B). Quantum memories store the information of the photons and acknowledge the arrival with a heralding signal. If a photon has been stored in the quantum memory A, then a heralding signal is sent to S_1 and C_1. If S_1 receives a heralding signal also from C_1 from the same entangled pair then the distribution is stopped and an entangled pair has been distributed between A and C_1. The same procedure is used on the segment on the right until an entangled pair has been acknowledged between C_2 and B. Now, entanglement swapping is performed on the elements C_1 and C_2 to connect the two entangled pairs. Then Alice and Bob apply accordingly to the result of the measurement a quantum operation on their quantum memories to transform the state to the desired entangled pair between Alice and Bob.

We now discuss the performance of this protocol. The situation depicted in fig. 4.1 should be compared to one unique entanglement based source in the middle between Alice and Bob (see fig. 3.1). In this case the probability that Alice and Bob receive pairs from the same entangled pair is given by $P_0^2 = \eta_T(L)$ where $P_0 := \eta_T(L/2)$ is the probability to distribute successfully a pair in a segment of length $L_0 := L/2$. Therefore, the number of pairs a source needs to produce on average is given by $< N >= P_0^{-2}$ and the average total time necessary for creating one entangled pair between Alice and Bob is given by $(\nu P_0^2)^{-1}$ where ν is the repetition frequency of the source measured in pairs per seconds. In the case of a quantum repeater depicted in fig. 4.1 the average number of pairs necessary for creating an entangled pair between Alice and Bob is given by [34, 24]

$$< N >= \frac{3 - 2P_0}{(2 - P_0)P_0}. \tag{4.6}$$

In order to make a fair comparison with direct communication it is necessary to include also times needed for heralding and to entanglement swapping. The communication time necessary for distributing one entangled pair is given by $\frac{T_0}{2}$ which is the time needed for a photon to go from a source (S_1 or S_2) to the quantum memory. The time for receiving the heralding is given by T_0 which is the time for a light signal to go from one quantum memory to the other one, i.e. from the repeater station to Alice or Bob or viceversa). After entanglement swapping has been performed, the result of the measurement takes still a time T_0, therefore the average total time for producing one entangled pair is given by

$$< T >:= T_0 \left(\frac{3}{2} < N > +1 \right). \tag{4.7}$$

A different aspect we need to consider is the quality of the resulting entangled pair. For concreteness, let us suppose that the created entangled state in each segment is a depolarized state with fidelity F_0 (see sec. (2.14)). This fidelity depends on the initial fidelity of the pair as generated by the source and on the noise introduced by the channel. After entanglement swapping, the fidelity of the obtained pair is

$$F_1 = \frac{1 - 2F_0 + 4F_0^2}{3}. \tag{4.8}$$

If $F_0 < 0.683$ then the resulting pair will become a separable state which could be prepared with classical communication and local operations. A possible solution is to increase the fidelity of the pairs before entanglement swapping. A possible protocol is entanglement distillation [21, 37] . The quantum repeater protocol changes in this way. First, many entangled pairs are created on each segment, then a specific combination of quantum gates and measurement is applied on each side in a way to obtain a resulting pair of higher fidelity. Then entanglement swapping between these two distilled pairs is performed. Depending on the initial fidelity F_0 it is possible to increase the number of pairs used for distillation in such a way the final pair after entanglement swapping is entangled.

As a conclusion, we have discussed the main ingredients of a quantum repeater protocol. Summarizing we need

1. quantum memories and heralded creation of entanglement,

2. entanglement swapping,

3. entanglement distillation.

In the following we will discuss these four ingredients, then we will discuss why all of them are necessary and what happens if one of them is not included. Finally, we will discuss several scheduling algorithms, which are methods for composing the elements above.

4.3 Ingredients for quantum repeaters

In this section we discuss all ingredients of a quantum repeater. For each ingredient we will give a brief description of how it is supposed to work, we will present the main imperfections and its characterization, then we will discuss what is the actual status of implementations.

4.3.1 Quantum memories and heralded creation of entanglement

Nowadays, the realization and the improvement of quantum memories represent a broad research area worldwide. Quoting a recent review [31] "a quantum memory is, in broad terms, a system that can store a quantum state to accomplish a certain task". Recent reviews of research in quantum memories include [73, 5, 54, 74, 96, 31].

For application to quantum repeaters many types of quantum memories could be used. There are quantum memories that herald the absorbition of photons [97, 25, 81] and quantum memories which are not intrinsic heralded. These are also know in literature as optical quantum memories [31] because their state can be prepared and manipulated using light. The most studied implementation of such quantum memories is based on atomic ensembles [39, 88]. Optical quantum memories, in their most common implementation, do not posses heralding and moreover, it is not straightforward to store an incoming photon. However, there are schemes similar to entanglement swapping which permit to entangle in an heralded way two of such quantum memories. See [39, 88] for additional details.

Relevant figure of merit relative to quantum memories are

- Heralding probability. This is the probability that heralding is acknowledged.
- Reading efficiency η_M. This is the probability that a stored photon is actually retrieved.
- Decoherence model $\Gamma_t(\rho)$. This is the quantum channel which describes how the stored quantum state evolves with the time. During the work of this thesis we have considered two types of decoherence model.
  1. Step function model [34]. The quantum state remains perfect for $t < \tau_C$ and then it becomes a completely mixed state for $t > \tau_C$, i.e.
  $$\Gamma_t(\rho) = \begin{cases} \rho & \text{if } t \leq \tau_C \\ \mathbb{1}/2 & \text{if } t > \tau_C, \end{cases} \tag{4.9}$$
  where the time τ_C is called *coherence time.*
  2. Depolarization model [84]. The quantum state degrades following an exponential law
  $$\Gamma_t(\rho) = e^{-\frac{t}{\tau_C}}\rho + (1 - e^{-\frac{t}{\tau_C}})\mathbb{1}, \tag{4.10}$$
  where τ_C is called coherence time.

4.3.2 Entanglement swapping

The next ingredient for a quantum repeater protocol is entanglement swapping [19, 59]. In the following we will describe how the protocol works, then we will discuss how it is often implemented and finally we will describe how imperfections affects the figure of merits of entanglement swapping. The idea of the protocol is that there are two separate entangled pairs which are joined by applying a suitable measurement between one part of each pair. More formally, let us consider two entangled quantum states ρ_{AC_1} and ρ_{C_2B} as depicted in fig. 4.1. The purpose of the protocol is to generate a new entangled state ρ_{AB} between Alice and Bob. Therefore in the beginning Alice and Bob are not entangled, at the end without actual communication between them they will be entangled. The actual communication is only between the repeater station and Alice and Bob. If $\rho_{AC_1} := |\phi^+\rangle_{AC_1}\langle\phi^+|$ and $\rho_{C_2B} := |\phi^+\rangle_{C_2B}\langle\phi^+|$ then it is enough to do a Bell measurement between the quantum memories C_1C_2, i.e. to perform the projective measurement consisting of the following four projectors $|\phi^\pm\rangle\langle\phi^\pm|$ and $|\psi^\pm\rangle\langle\psi^\pm|$. The result of the measurement is communicated to Alice and Bob who will apply an appropriate single-qubit rotation to their quantum systems. The final resulting state is $\rho_{AB} = |\phi^+\rangle_{AB}\langle\phi^+|$ which is a maximally entangled state.

We have seen that provided the two segments are Bell states, the final connected state is once again a Bell state. However, if the states ρ_{AC_1} and ρ_{C_2B} are not maximally entangled states, then the resulting state will be also a not maximally Bell state (see sec. 4.2). Let us consider a chain of $n+1$ entangled state, the purpose is to apply entanglement swapping n times in such a way to have a long distance entangled state. If all states are depolarized states of fidelity F_0, applying eq. (4.8) many times it is easy to show that the final fidelity is

$$F := \frac{1}{4} + \frac{3}{4}\left(\frac{4F-1}{3}\right)^n. \tag{4.11}$$

Therefore, we see that the fidelity decreases exponentially in n.

A Bell-state measurement between the quantum memories C_1C_2 can be implemented as follows. The quantum states C_1C_2 are first given as input to a CNOT gate (see sec. 2.2.1), then the control bit is subjected to a Hadamard gate (see sec. 2.2.1) and, finally, both quantum states are measured in the Z basis. A successful measurement needs that both detectors produce an outcome. If only one, or none, detector clicks than the result is inconclusive because we don't know which was the measured Bell-state. Therefore, for detectors with detection efficiency η_D as described in sec. 2.3 the BSM success probability is

$$P_{\text{BSM}} = \eta_D^2. \tag{4.12}$$

If the measurement is not done directly on the quantum memories, but instead photons are retrieved the success probability becomes

$$P_{\text{BSM}} = \frac{1}{2}(\eta_M\eta_D)^2. \tag{4.13}$$

The factor $\frac{1}{2}$ appears in the success probability because usually a BSM on photons is done with linear optics, and as shown in [32] the maximal success probability in this case is $\frac{1}{2}$. The advantage of entanglement swapping with linear optics is that even if it is probabilistic, the introduced noise is usually negligible.

4.3.3 Entanglement distillation

Entanglement distillation for mixed states has been proposed for the first time in [21]. Based on it, [37] proposed a similar protocol which permits to achieve higher success probability and final fidelity. These are examples of recursive protocols. The idea is the following. We start the protocol with 2^x entangled pairs. Couples of pairs are manipulated with a proper choice of quantum gates and measurements. Depending on the result of the measurement, it is possible to know with certainty that the remaining pair has a higher fidelity. In the other case, the round of distillation is considered failed and the protocol starts from the beginning. Therefore, as a result of the first round 2^{x-1} pairs are remained. The protocol is applied once again in the same way, and hence the name recursive, until the point that one final pair remains. A different type of protocols have been proposed in [28] and they are called pumping protocols. A complete explanation of such protocols is included in one of the papers attached to this thesis [27].

4.4 Original quantum repeater protocol

Now that we have presented all building blocks we can compose them for having a complete quantum repeater protocol. In this section we will first describe the original quantum repeater protocol presented in literature [28]. This protocol is also called *nested quantum repeater protocol* and it represents a prototype for most of the protocols developed till nowadays. In the following we will give a description of the protocol and we will discuss the scaling of the average number of pairs as a function of the parameters.

4.4.1 The protocol

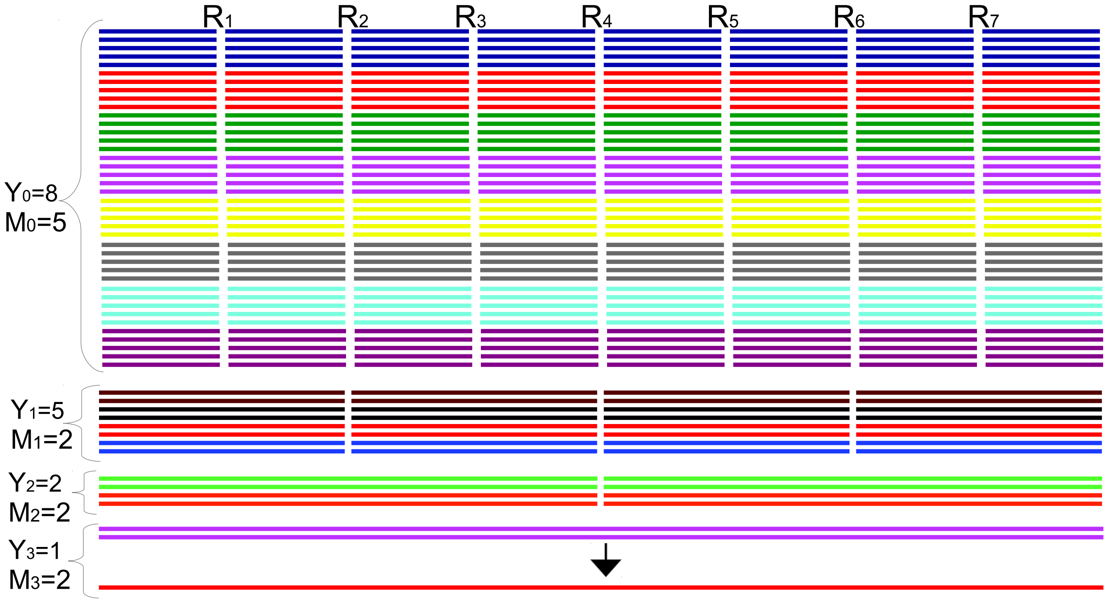


Figure 4.2: Nested quantum repeater scheme [28]. The index N is the nesting level and M is the number of quantum states used for distillation. The maximal nesting level is $N_{\text{MAX}} = 3$. Lines with the same colors are used for producing one entangled pair. The index R_i with $i = 1, ..., 2^{N_{\text{MAX}}} - 1$ represents an index for the repeater station. The red line on the bottom of the figure represents the final entangled pair between Alice and Bob.

In the following we will describe the steps of the protocol. In fig. 4.2 there is a representation of the protocol. The distance between Alice and Bob is divided in $2^{N_{\text{MAX}}}$ segments. Given that the distance between Alice and Bob is L the length of each segment is then $L_0 := L/2^{N_{\text{MAX}}}$. The index N is called nesting level and N_{MAX} is the maximal nesting level. The protocol works as follows:

1. In each segment $Y_0 \cdot M_0$ entangled pairs are created.
2. In each segment M_0 pairs are used for distillation, therefore in the end for each segment we obtain Y_0 final pairs.
3. Entanglement swapping is performed in the repeater stations R_1, R_3, R_5, R_7.

At the end of the third step we obtain quantum states which are shared at the distance $2L_0$. The three steps above are repeated until entangled pairs at distance L are produced. The last step is to perform distillation between pairs at distance L in such a way to obtain one final pair with high fidelity. The protocol is called *nested* because it is self-similar over distances which are doubling at each iteration.

Before to show that this protocol can outperform direct communication we wish to add additional details regarding the protocol.

- Distillation and eventually entanglement swapping are probabilistic. That means that when one of these two protocols fails, in the involved branch it is necessary to start from scratch from $N = 0$ before to be able to do entanglement swapping with another branch.
- After each operation it is necessary to communicate classical information regarding the outcome of the measurement and the fact that the measurement were successful.
- On parallel branches (column in fig. 4.2) operations can be performed in parallel, but before to join two branches with entanglement swapping it is necessary that the involved repeater stations got the information about successful distillation and previous entanglement swappings.
- It is not clear, at priori, which are the optimal values of N_{MAX}, M and Y. This depends on the particular application [27].

4.4.2 Performance

A complete and exact formula for the average time needed for creating entangled pairs on distance L is still not available. Instead of that, many exact formulas for special cases or approximate formulas for the general case are known. In the following we will consider few relevant cases for this thesis and we will give the formulas. In all formulas we will denote by P_0 the probability that a pair is created in a segment of length $L_0 := L/2^{N_{\text{MAX}}}$. The success probability of entanglement swapping is given by $P_{ES}^{(i)}$ where i is the nesting level. Note that these probabilities depend also on other parameters which are specific of each protocol.

Moreover, we need to define the speed of light. Typically, signals travel through optical fibers and the speed of light in this medium is about $c = 2 \cdot 10^6$ km/s [55]. We define also the *fundamental time* $T_0 := L_0/c$ which is the time light need to travel between the two extremes of an elementary segment.

- **Quantum repeater with no distillation and deterministic entanglement swapping** This is the simplest model of quantum repeater. Entanglement swapping never fails, and distillation is not used. Therefore, the only probabilistic process is entanglement creation in each elementary segment. The average time for creating entanglement in such a scheme is given by [24] [1]

$$< T >= \frac{3}{2} T_0 Z_{N_{\rm MAX}}(P_0) + L/2c, \tag{4.14}$$

with [24]

$$Z_N(P_0) := \sum_{j=1}^{2^N} \binom{2^N}{j} \frac{(-1)^{j+1}}{1-(1-P_0)^j} \tag{4.15}$$

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

- **Quantum repeater with no distillation and probabilistic entanglement swapping.** For this scheme an approximate formula for the average time has been derived in [88]. This formula is believed to be quite good for small value of P_0 [88] and it is

$$< T >= \frac{3}{2} T_0 \left(\frac{3}{2}\right)^{N_{\rm MAX}} \frac{1}{P_0 P_{ES}^{(1)} P_{ES}^{(2)} ... P_{ES}^{(N_{\rm MAX})}}. \tag{4.16}$$

One of the result of this thesis has been to generalize this formula to the following scenarios:

- **probabilistic entanglement swapping and distillation only in the 0th nesting level** See next chapter and [4].

- **probabilistic entanglement swapping and distillation in all nesting levels including also classical communication** See next chapter and [27].

4.4.3 Final shared state

In the previous section we have described what is the time for producing one entangled pair. However, for applications it is important to characterize also the final shared state between Alice and Bob. The final aim of this characterization is to tune the repeater parameters as the number of segments, the number of pairs used for distillation, the distillation protocol, the minimal coherence time of the quantum memories, etc in order to optimize some figure of merit. The usual figure of merit which has been optimized is the fidelity of the final pair. In this thesis we have studied the secret key rate which will present some peculiarity that we will explore in the next chapter.

[1] This formula does not match exactly the formula given in [24] for the following reason. In [24] entanglement is not created with a source in the middle but instead with a source on only one side. Therefore, the time for distributing one pair is give by T_0 and the time for getting the acknowledge signal is once again T_0. This explain the factor $2T_0$ present in [24]. Check sec. II.A.3 and fig. 2 of the paper [4] attached to this thesis for additional details about the distribution and the acknowledgment time.

5 Results

5.1 Introduction

The purpose of this section is to put together the elements presented in the previous two chapters and to present the result of this dissertation which can be divided in three categories:

- **Analysis of the performance and requirements of general purpose quantum repeater protocols for application to QKD**. The expression *general purpose* in this context means that the quantum repeater protocols are not specifically designed for application to QKD. Instead, the final entangled pair may be used for generic applications like distributed quantum computation and entanglement teleportation. In Ref. [4, 27] we have studied common quantum repeater protocols, namely the original quantum repeater protocol, the hybrid quantum repeater and quantum repeaters based on linear optics and entanglement swapping. We have calculate the secret key rate and characterized the minimal requirement. Regarding [4] we have assumed that distillation is only performed before to do any entanglement swapping. Then in [27] we have lifted this assumption and we have characterized different distillation protocols and general scheduling algorithms.

- **Analysis of two segment quantum repeaters protocol specifically minded for QKD**. Here we have shifted our focus on protocols which are more likely to be realized in the near future. We consider the simplest quantum repeater scenario where there is only one repeater station. Ref. [2, 1] belong to this category.

- **Finite-key analysis of the six-state protocol with realistic detectors**. In the previous two papers we have always calculated the asymptotic secret key rate. However, in realistic cases finite-key correction are going to play a relevant role. In Ref. [3] we consider entanglement-based QKD (without quantum repeaters) and we calculate the secret key rate with finite-size corrections when there are imperfections in the source and in the detectors.

5.2 Analysis of the performance and requirements of general purpose quantum repeater protocols for application to QKD

In order to characterize the performance of a quantum repeater protocol we have used as figure of merit the secret key rate which represents the number of bits per second and it is defined by

$$R_{\mathrm{QKD}} := R_{\mathrm{REP}} P_{\mathrm{click}} R_{\mathrm{sift}} r_{\infty}, \tag{5.1}$$

where R_{REP} is the repeater rate defined and discussed in sec. 4.4.2, the probability P_{click} has been defined in sec. 3.2.2 and it represents the probability that the QKD measurement is successful when the created entangled pair is measured. The sifting rate represents the probability that Alice and Bob choose the same measurement basis and for the whole thesis (except sec. 5.4) it will be chosen equal to one. The reason is that as proven in Ref. [70] in the asymptotic case Alice and Bob can choose one basis with probability almost one and the others with negligible probability. The secret fraction has been defined in sec. 3.2.1 for the BB84 and the six-state protocol.

In ref. [4] we studied the performance and the requirement of three quantum repeater protocols, the original quantum repeater [28], the hybrid quantum repeater [101, 66] and a quantum repeater based on linear optics and atomic ensembles. One challenging task of ref. [4] has been to set a unique notation, similar parameters and similar analysis techniques for different protocols which has been always studied individually. Section II of ref. [4] is therefore considered a good introduction to quantum repeater and QKD. In the following we will discuss for each type of quantum repeater the main results.

5.2.1 Original quantum repeater

The original quantum repeater has been proposed in [28]. The authors do not specify a specific implementation but they consider a generic implementation. The distributed entangled states are depolarized Bell states (eq. (2.14)) of initial fidelity F_0 and entanglement swapping is deterministic and the gates have depolarizing noise (see eq. (2.25)) with noise parameter (gate error) p_G. The probability that the entanglement swapping measurement is successful is given by $P_{ES} = \eta_D^2$ where η_D is the efficiency of photon number resolving detectors (see eq. (2.32)). For this type of quantum repeater we have considered protocols where distillation is done only in the beginning, i.e. before starting to perform entanglement swapping (see fig. 5.1).

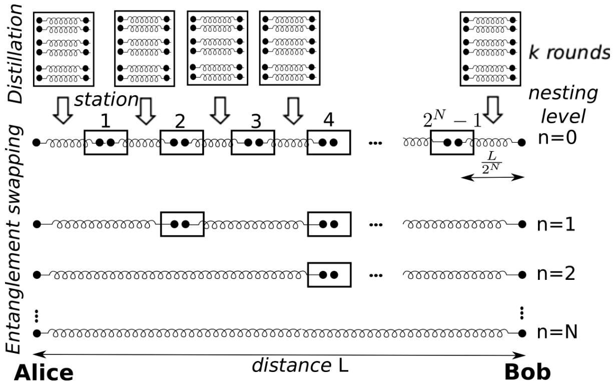


Figure 5.1: (Figure and caption from Ref. [4]) Scheme of a generic quantum repeater protocol. We adopt the nested protocol proposed in [28]. The distance between Alice and Bob is L, which is divided in 2^N segments, each having the length $L_0 := L/2^N$. The parameter n describes the different nesting 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.

The first quantities we have studied are the minimal initial fidelity F_0 and the maximal gate error p_G such that it is possible to extract a secret key. This has been done by studying the region where the secret fraction r_∞ becomes zero.

As shown in fig. 5.2 increasing the initial fidelity it is possible to use worse gates and vice versa. We see, moreover, that the initial distillation permits to use pairs with lower fidelity w.r.t. the case without distillation at the expense of better gates. After characterizing the minimal requirement, we have characterized what is the optimal number of distillation rounds. Optimal means that the secret key rate is maximized. In fact there are two competing effects. More rounds of distillation will decrease the QBER as the final pair

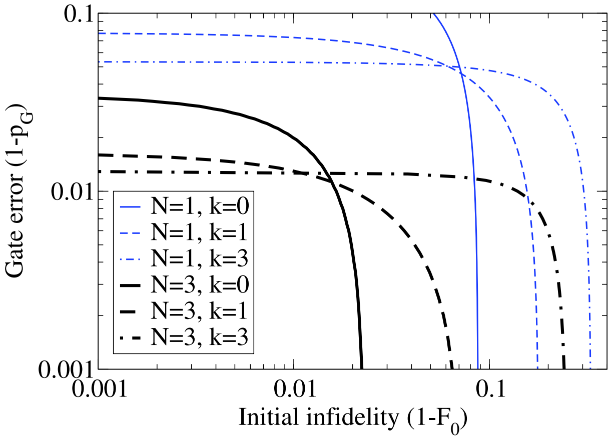


Figure 5.2: (Figure and caption from Ref. [4]) Original quantum repeater and the BB84-protocol: Maximal infidelity $(1 - F_0)$ as a function of gate error $(1 - p_G)$ permitting to extract a secret key for various maximal nesting levels N and numbers of distillation rounds k (Parameter: $L = 600$ km).

will have higher fidelity. The result is an increase of the secret fraction. On the other hand, more rounds of distillation will decrease the repeater rate as we need more pairs.

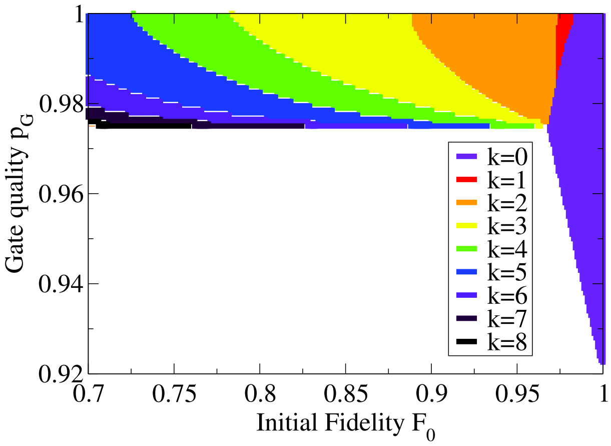


Figure 5.3: (Figure and caption from Ref. [4]) Original quantum repeater and the BB84-protocol: Number of distillation rounds k that maximizes the secret key rate as a function of gate quality p_G and initial fidelity F_0. In the white area, it is no longer possible to extract a secret key. (Parameters: $N = 2$, $L = 600$ km)

In fig. 5.3 we have the optimal number of rounds of distillation as a function of the gate quality and the initial fidelity. Interestingly, there is a not negligible region where no distillation is optimal. This is the region where both gates and pairs have high quality. Moreover, over a big range of initial fidelity we see that $k \leq 8$ is optimal.

Then, we have calculated the secret key rate as a function of the distance. For the plot in fig. 5.4 we have chosen initial fidelity $F_0 = 0.9$ and gate quality $p_G = 0.995$. Our result is that for perfect photon detectors $(\eta_d = 1)$ and for $L < 400$ km the nesting level $N = 3$ (i.e. $2^3 = 8$ segments) is optimal. Then $N = 4$ is optimal. Note that $N = 5$ will be never optimal because for our set-up it will always lead to a zero secret key rate. In case of more realistic detectors the situation is more complicated; for $L < 350$ km it is optimal to use $N = 2$ then till $L \approx 700$ km it is optimal to use $N = 3$ and for larger distances

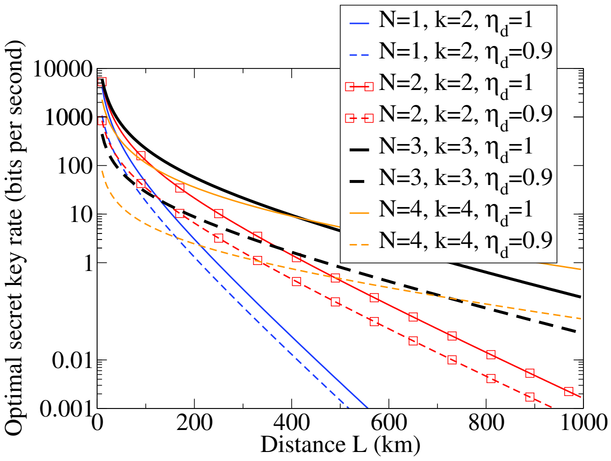


Figure 5.4: (Figure and caption from Ref. [4]) Original quantum repeater and the BB84-protocol: Optimal secret key rate versus distance for different nesting levels, with and without perfect detectors. For each maximal nesting level N, we have chosen the optimal number of distillation rounds k. A nesting level $N \geq 5$ no longer permits to obtain a non-zero secret key rate. (Parameters: $F_0 = 0.9$ and $p_g = 0.995$.)

$N = 4$ is optimal.

5.2.2 Hybrid quantum repeaters

Hybrid quantum repeaters have been proposed in [101, 66]. They are called hybrid because entanglement between two distant qubits is realized using a coherent state. Therefore, this scheme uses discrete and continuous variables.

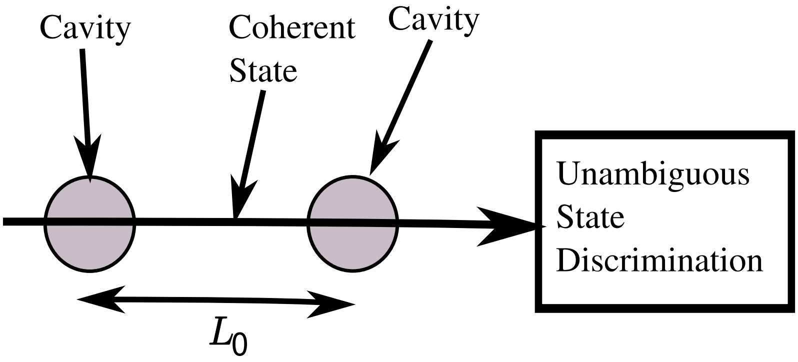


Figure 5.5: Conceptual scheme of heralded entanglement creation for an hybrid quantum repeater. The cavities are used as quantum memories.

Heralded entanglement creation works as follows. A coherent-state pulse interact for the first time with a cavity. The interaction can be described using a Jaynes-Cummings Hamiltonian in the limit of large detuning, i.e. $H_{int} = \hbar\chi Z a^\dagger a$, 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. After the interaction, the coherent state is sent through the lossy fiber and interacts once again with the other cavity. The resulting state is measured using an ambiguous discrimination measurement (USD) and in the case the state can be discriminated the resulting state of the two cavities is [24]

$$\rho_0 := F_0|\phi^+\rangle\langle\phi^+| + (1-F_0)|\phi^-\rangle\langle\phi^-|. \tag{5.2}$$

The success probability of creation of this state is given by [24]

$$P_0 = 1 - (2F_0 - 1)^{\frac{\eta_T(L_0)}{1-\eta_T(L_0)}}. \tag{5.3}$$

Note that as $F_0 \to 1$ then $P_0 \to 0$.

For the hybrid quantum repeater, analogously to the previous section we have studied a protocol were distillation is performed only in the beginning. This type of set-up was studied already in Ref. [24] but the used figure of merit was the final fidelity.

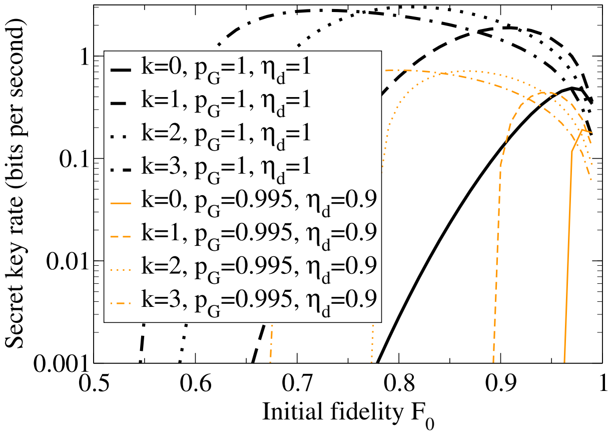


Figure 5.6: (Figure and caption from Ref. [4]) Hybrid quantum repeater with perfect quantum operations ($p_G = 1$) and perfect detectors ($\eta_d = 1$) (black lines) compared to imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_d = 0.9$) (orange lines): Secret key rate per second 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.

In fig. 5.6 we see how the secret key rate changes as a function of the initial fidelity for different numbers of rounds of distillation k, gate qualities p_G and detector efficiencies η_d. The result is that there is an optimal initial fidelity F_0. If a higher initial fidelity is used, the secret key rate will be lower. The reason is that even if the final pair will be with higher fidelity and therefore will produce a higher secret fraction due to eq. (5.3) the success probability will be lower and thus the repeater rate. We see, moreover, that increasing k the optimal fidelity decreases and at the same time the optimal secret key rate increases.

Then we have studied the secret key rate and as shown in fig. 5.7 we found that $N = 3$ (8 segments) and $k = 3$ is optimal through the whole range till $L \approx 950$ km.

5.2.3 Quantum repeaters based on linear optics and atomic ensembles

Duan, Lukin, Cirac and Zoller introduced in 2001 a quantum repeater protocol based on atomic ensembles and linear optics [39]. Since 2001 a big effort has been done in order to improve the protocol from the theoretical side and at the same time to implement it experimentally. Nowadays, all basic elements have been implemented, i.e. heralded creation of entanglement and entanglement swapping. See [88] for a recent review of experimental and theoretical results. However, according to [87] a quantum repeater that can outperform direct communication has not been developed yet. In Ref. [4] we have

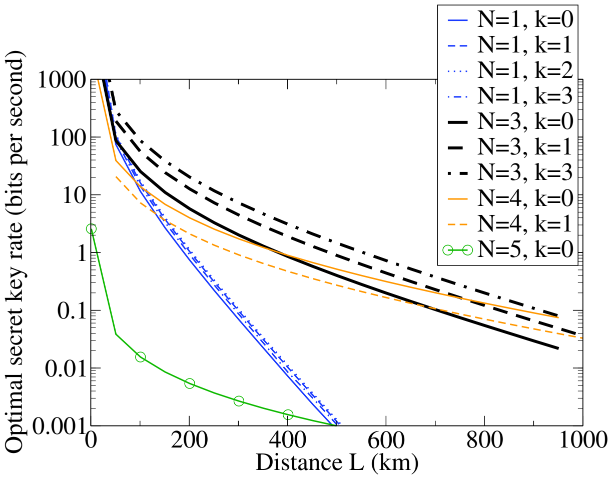


Figure 5.7: (Figure and caption from Ref. [4]) Hybrid quantum repeater with imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_d = 0.9$): Optimal secret key rate for the BB84-protocol as a function of the total distance L, for various numbers of segments 2^N and rounds of distillation k. For $N = 5$, it is not possible to obtain a secret key when distillation is applied.

studied the performance in relation to QKD of the most recent proposal [76] of quantum repeater based on atomic ensembles and linear optics. We refer to Sec.V of Ref. [4] for a complete explanation of the protocol and the parameters. For this protocol we have not treated distillation as this last one has not been studied in the original protocol [76] and it is not usually considered in protocols with atomic ensembles. The result is shown in fig. 5.8. We have compared the ideal scenario where everything is perfect and a realistic scenario where we used typical values of the imperfections. As a result we have shown that for $L > 400$ km is is optimal to have 16 segments in the case of imperfect set-up.

5.2.4 Study of more general scheduling algorithms

In the previous sections we have considered protocols where distillation may be performed only in the beginning before to start entanglement swapping. However, more general protocols are possible where distillation is performed in all nesting levels (see fig. 4.2). In [27] we have considered exactly this problem. First, we have considered two scheduling protocols: strategy α where distillation is performed in all nesting levels with the constraint that the number of rounds of distillation is always the same and strategy β where distillation is done before the first entanglement swapping. In contrast to [4] in [27] we consider the secret key rate per memory. This is necessary in order to make a fair comparison. Our result is summarized in fig. 5.9. We see that in most of the region it is optimal to perform distillation in all nesting levels. However, there is also a region where strategy β is optimal. This is the region where quantum gates are very good. Then we have also considered arbitrary complex scheduling algorithms where there are no restrictions. The results are described in Sec.IV.C of [27]. Notably, we found out that it is never optimal to do distillation in the beginning and in the end, i.e. at nesting levels 0 and N, where N is the maximal nesting level.

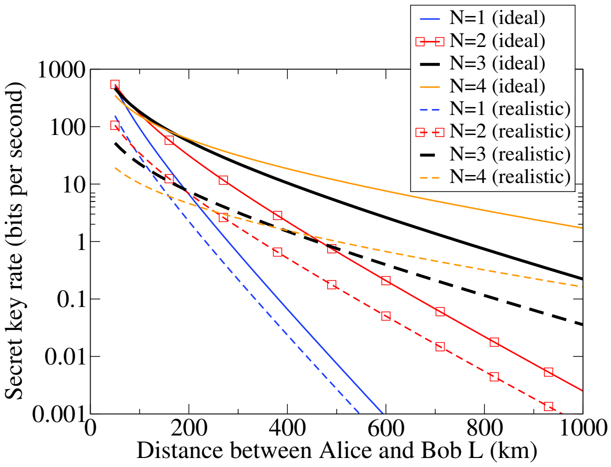


Figure 5.8: (Figure and caption from Ref. [4]) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the distance between Alice and Bob. The secret key rate has been obtained by maximizing over p and R. Ideal set-up (solid line) with parameters $\eta_m = \eta_d = q = 1, \gamma_{rep} = \infty$. More realistic set-up (dashed line) with parameters $\eta_m = 1$, $\eta_d = 0.9$, $q = 0.96$, $\gamma_{rep} = 50$ MHz. (See Ref. [4] for an explanation of the various parameters).

5.3 Analysis of two segment quantum repeaters protocol

5.3.1 Measurement-device independent QKD with quantum memories

Another part of the work of this thesis has involved quantum repeaters with two segments and one repeater station. Our results are in Refs. [2, 1]. This is the simplest set-up which could potentially outperform direct transmission. Our study starts from a work in Ref. [71]. There the authors describe a new quantum key distribution scheme where Alice and Bob have weak coherent pulse sources (see eq. (2.20)) which are used for approximating single photon sources. The two parties prepare photons in suitable quantum states for QKD and send them to a station in the middle which performs a *blind* Bell-state measurement. Correlations are created by performing suitable bit flips depending on the result of the BSM and the preparation basis. This protocol is called *measurement-device independent* because Alice and Bob do not perform any measurement but instead they move this task to the station in the middle which is controlled by the eavesdropper. We have called the measurement blind because as described in Ref. [71] the measurement is always performed even when the photons did not reach the measurement station. A posteriori, if both photons were not there then the measurement is considered failed and the corresponding bits are thrown away by Alice and Bob.

In Ref. [2] we have generalized the protocol to a set-up with quantum memories (see fig. 5.10). This permits to exploit the heralding of quantum memories and to perform the BSM only when both photons arrived to the measurement station that will be now called repeater station. Note, that a priori it is not clear if a quantum repeater with quantum memories will outperform the protocol without quantum memories. The reason is that from one side quantum memories will increase the repeater rate (see sec. 4.2) but from another side, due to memory decoherence, the QBER will increase giving as a result a decrease of the secret fraction. We have considered a delta function decoherence model (see eq. (4.9)). This model has been considered originally in [34] and it is convenient because it permitted to obtain analytical and closed formulas for the QBER and the repeater rate.

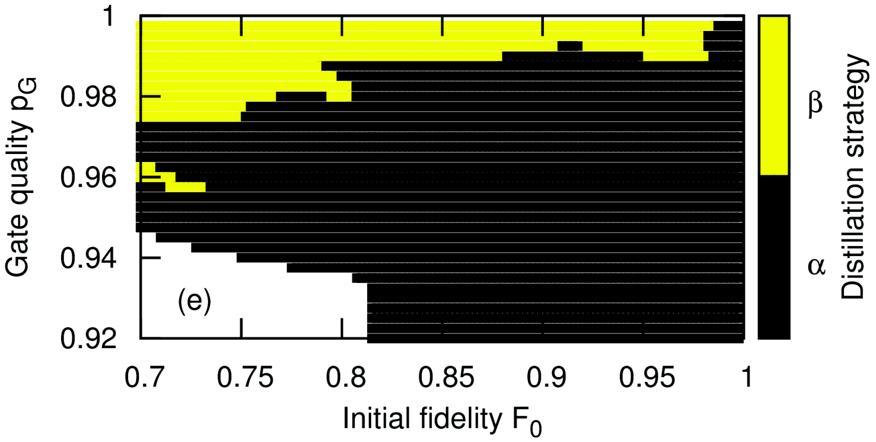


Figure 5.9: (Figure from Ref. [27]) Optimal scheduling algorithm for the original quantum repeater protocol.

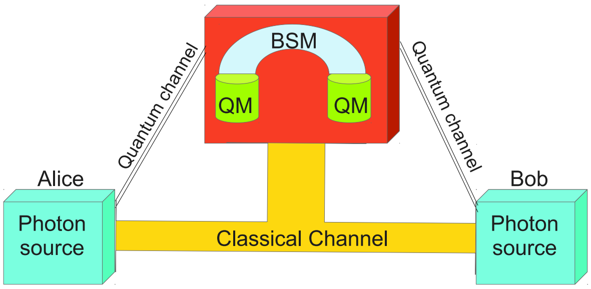


Figure 5.10: (Figure and caption adapted from Ref. [2]) Scheme of a measurement-device-independent quantum repeater. The difference w.r.t. Ref. [71] is that quantum memories are used. QM=quantum memories, BSM=Bell-state measurement. The two sources produce single-photon states or weak coherent pulses.

After we characterize the minimal coherence time permitting to have a non-zero secret key rate we have calculated how the secret key rate scales as a function of the coherence time. In fig. 5.11 we represent the secret key rate as a function of the ratio between τ and τ_{MIN}, where τ is the actual used fidelity and τ_{MIN} is the one permitting to extract a secret key. The result is that it is sufficient to have $\tau/\tau_{MIN} \approx 4$ as then the secret key rate reaches a flat region.

Then we have studied the secret key rate as a function of the distance for single-photon sources and WCP. As shown in fig. 5.12 we see that the protocol with the quantum memories and single-photon sources (denoted by MDI-QKD-REPEATER-SPS) greatly outperform the protocol without quantum memories even for decoherence times slightly better than the minimal ones. The analysis with weak coherent pulses is more complex because new attack strategies, namely photon splitting attacks, become possible. The reason is that a WCP is constituted by many, exactly equals, photons which can be spitted and saved by the eavesdropper without introducing any noise. In order to deal with this type of attacks, a protocol with *decoy states* has been created. Decoy states are WCP with a different average photon numbers. Using the techniques developed in [72, 75, 71] it is

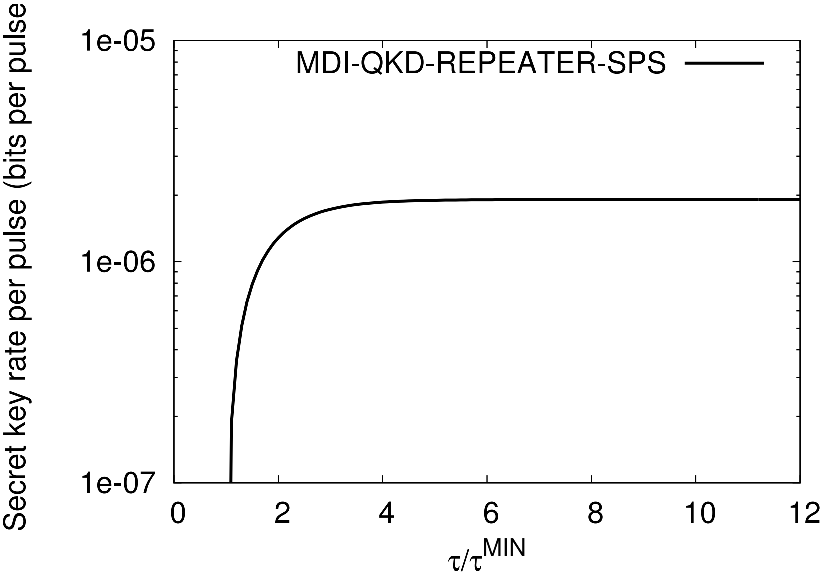


Figure 5.11: (Figure and caption from Ref. [2]) Secret key rate per pulse as function of τ/τ_{SPS}^{MIN}. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km, $L = 400$ km.

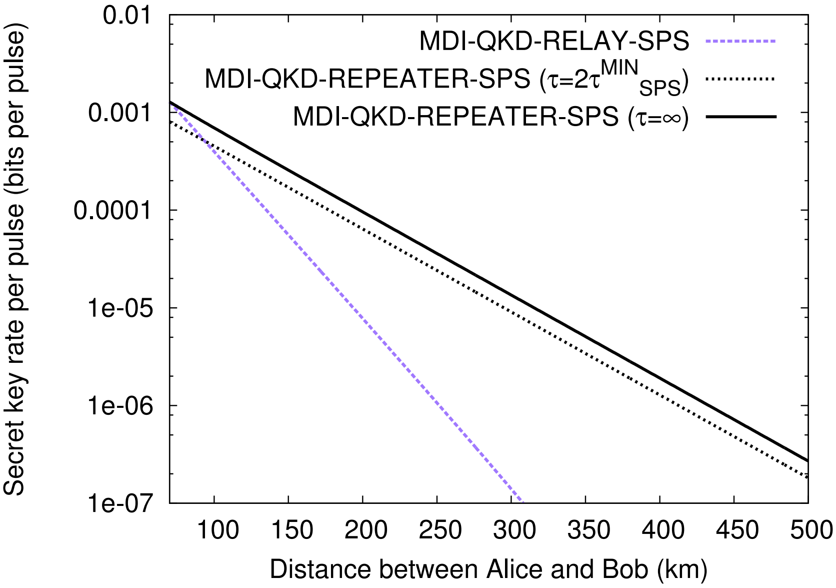


Figure 5.12: (Figure and caption from Ref. [2]) Secret key rate per pulse versus distance between Alice and Bob. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km.

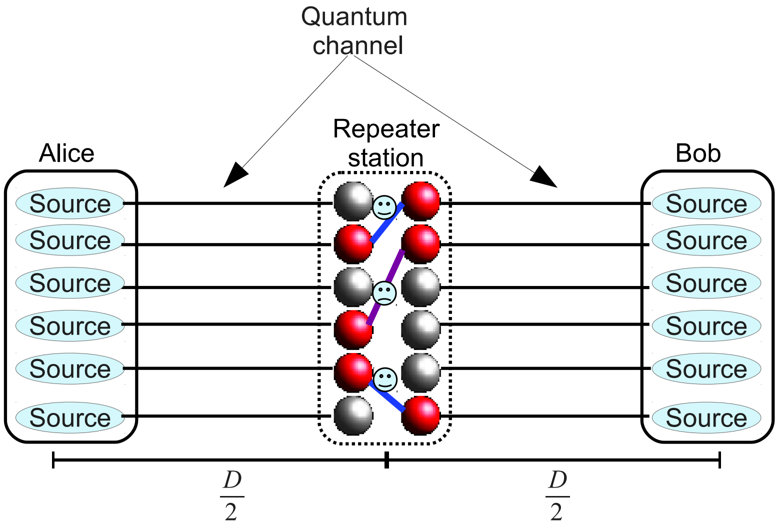


Figure 5.13: (Figure and caption from Ref. [1]) Alice and Bob are equipped with single-photon sources. Each source is connected through an optical fiber to a quantum memory in the repeater station. Red spheres represent filled quantum memories whereas gray spheres represent empty quantum memories. In this example the maximal connection length is one, therefore the connections indicated in blue are allowed and the magenta one is forbidden.

possible to evaluate the strength of the photon-number-splitting attack and consequently, to account for this additional information held by the eavesdropper in the formula of the secret key rate. In Ref. [2] we have performed all calculations evaluating the QBER and the optimal intensity of the decoy states such that the secret key rate is maximized. Accordingly to the result with single-photon sources we have found that imperfect quantum memories permit to outperform a protocol without quantum memories.

5.3.2 More general protocols: finite-range multiplexing

After the calculation of optimal secret key rate for the measurement-device independent protocol we have investigated how to increase the secret key rate by still using only one repeater station. We want to keep this constraint because this set-up is much less demanding than a full quantum repeater protocol with entanglement sources.

Therefore, we have considered the set-up shown in fig. 5.13. This is a generalization of the set-up of the previous section where in the repeater station there are two arrays of quantum memories. The arrays on the left is connected to Alice and the arrays on the right is connected to Bob. Let m be the number of quantum memories in one array. If the connections between the quantum memories are performed in parallel than the total secret key rate is m times the secret key rate calculate in the previous section. Actually, it is now possible to do better because it is possible to perform connection in diagonal between arbitrary quantum memories. This set-up has been introduced in Ref. [34] where the authors have shown that multiplexing permits to have a modest increase of the repeater rate and a significative decrease of the coherence time of the quantum memories. In Ref. [1] we have studied multiplexing in relation to quantum key distribution. We have generalized the original multiplexing considering finite-range connections. The reason is that long-range connections are difficult to perform. In Ref. [1] we have derived analytical

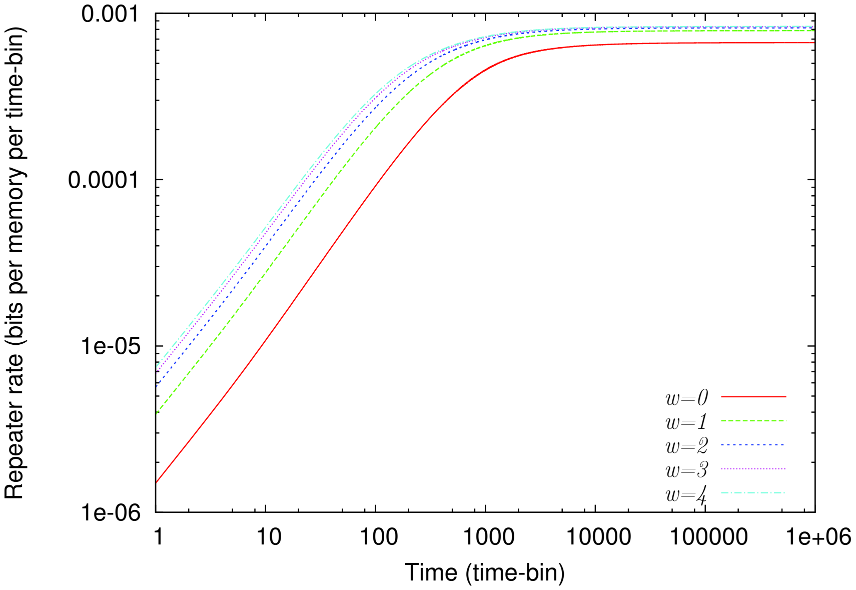


Figure 5.14: (Figure and caption from Ref. [1]) Repeater rate per memory as function of the time for $m = 5$ and various maximal connection length w. Parameters: $p = 0.001, P_{BSM} = 1$.

formulas for the repeater rate as function of the time from the beginning of the protocol. We have introduced an additional parameter w denoting the maximal connection length. The case $w = 0$ means that connection are performed only in parallel and $w = m - 1$ means that any connection is possible.

As shown in fig. 5.14 the repeater has a loading time till $t \approx 10^4$. After that the repeater rate has a practically flat behavior. Analyzing the dependence on the maximal connection length, we observe in the figure that the gap between $w = 0$ and $w = 1$ is almost the same than the gap between $w = 0$ and $w = 4$ which represents full-range multiplexing. This shows that in an experimental implementation in order to profit of multiplexing it is not necessary to have long-range connections. We have than studied the effect of imperfect quantum memories. In order to do that we have considered different matching algorithms depending on the arrival time of the photons in the quantum memories.

In fig. 5.15 we show three possible matching strategies. The number in a red sphere represents the arrival time and the blue edges represent the connection between the quantum memories. Moreover, the current time is also $t = 2$. In strategy 1 we perform connections such that the total time difference is minimized. In strategy 2 connections are performed in order to maximize the time differences and in strategy 0 connections are performed at random.

In Ref. [1] we have calculated the minimal coherence time permitting to extract a secret key and as shown in fig. 5.16 strategy 1 results to be optimal. We have than calculated the minimal coherence time as function of the maximal connection length and we have shown that $w = 1$ provides a great advantage on $w = 0$ and only a small disadvantage against full-range multiplexing. Finally, we have considered the secret key rate.

As shown in fig. 5.17 finite-range multiplexing with $w = 1$ leads to a similar improvement as with $w = 4$. The behavior of the secret key rate shows that there is still room of improvement. In fact a basic assumption for the calculation of the QBER has been that the maximal number of connection is performed. This maximize the repeater rate but not the secret key rate.

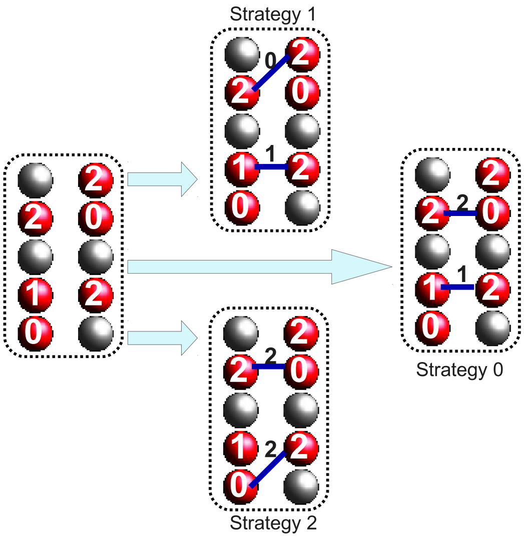


Figure 5.15: (Figure and caption from Ref. [1]) A red (gray) sphere indicates that the quantum memory is filled (empty). The number into the sphere represents the arrival time of the photons. On the left we have the situation at time 2_1 We consider $w = 1$. On the right three possible matching strategies are shown. Blue lines indicate the difference between the arrival times of the photons. It is possible to see the schemes on the right side as weighted bipartite graphs: red spheres are vertices and blue edges have indicated weights.

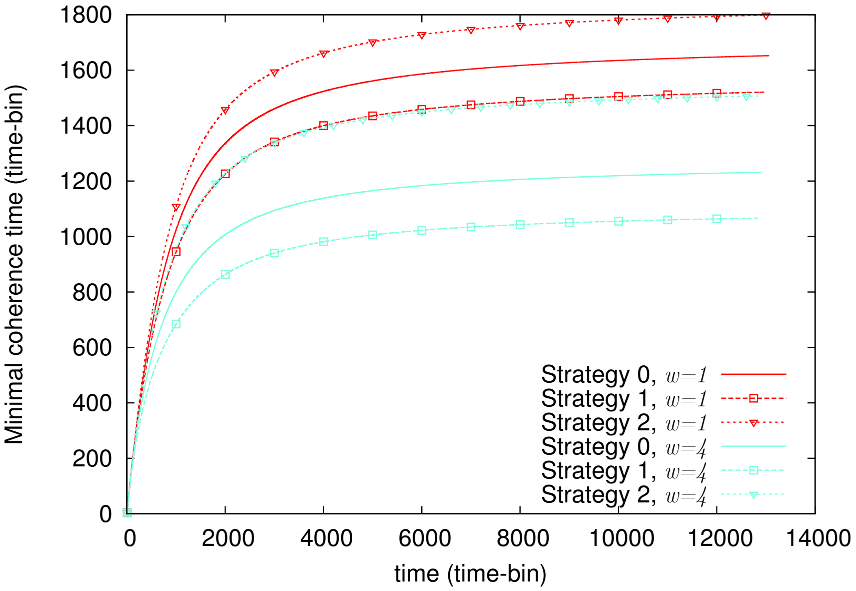


Figure 5.16: (Figure and caption from Ref. [1]) Minimal necessary coherence time τ as function of the time t for different strategies. Strategy 0 (solid lines), strategy 1 (dashed lines with squares), strategy 2 (dotted lines with reversed triangles). Parameters: $p = 0.001, m = 5, w = 1, 4$.

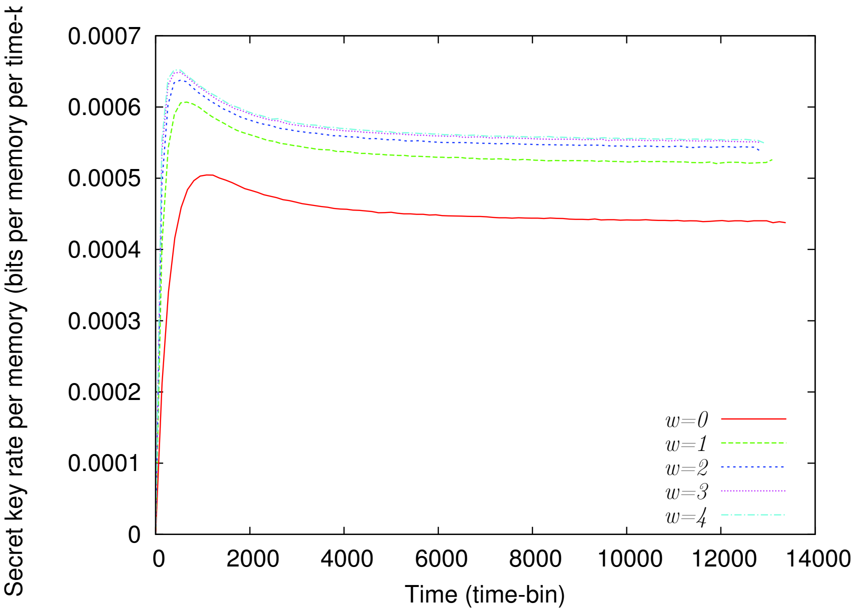


Figure 5.17: (Figure and caption from Ref. [1]) Secret key rate as function of the time t. for different maximal connection length. Parameters: $p = 0.001, m = 5$.

5.4 Finite-key analysis of the six-state protocol with realistic detectors

The paper in Ref. [3] can be considered a preparatory study to quantum repeaters and quantum key distribution. As we have discussed in sec. 3.2.2 the squashing model permits to adapt a security proof where quantum states are assumed to be qubits to a situation where quantum states are not qubits anymore because they can be absorbed by the channel or they can be composed of many photons. However, as proven in Ref. [12] the six-state protocol does not admit a squashing model. Therefore, for the six-state protocol it is not possible to use directly proofs where quantum states are assumed to be qubits. In Ref. [77] a workaround to this no-go theorem has been presented. The authors show that using photon number resolving detectors (see eq. (2.32)) it is possible to post-select only the events where one photon has been measured and then to extract a secret key using only these events. In Ref. [3] we study the performance of this technique when also finite-key corrections are applied. In contrast to the analysis performed in the previous sections, where the asymptotic secret key rate has been considered, we consider a well known achievable lower-bound to the finite secret key rate [90, 91] and we use it for calculating the optimal parameters which lead to the maximal secret key rate.

In fig. 5.18 we show the considered set-up. A SPDC source (see eq. (2.21)) is placed between Alice and Bob. The produced quantum states are measured by photon number resolving detectors which are represented in figure as a quantum non-demolition measurement determining the photon number followed by a standard QKD measurement.

In fig. 5.19 we show the result of the paper. We have the secret key rate as a function of the number of initial pulses produced by the source for different distances between Alice and Bob. The result has been that finite-size corrections are not negligible even for very large number of pulses.

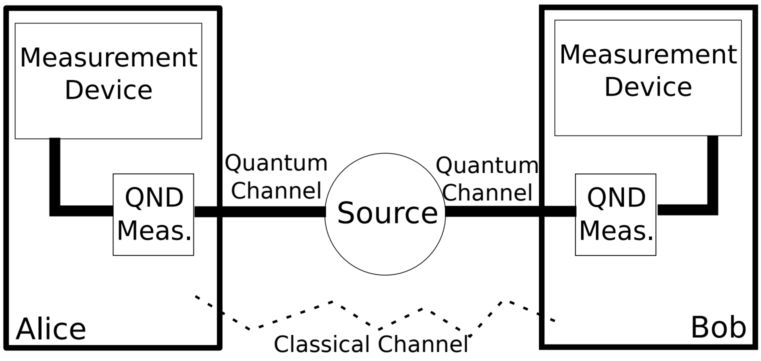


Figure 5.18: (Figure and caption from Ref. [3]) Set-up for QKD. The quantum channel is completely controlled by the eavesdropper. The classical channel is authenticated but otherwise tapped by the eavesdropper. The laboratories are by definition secure.

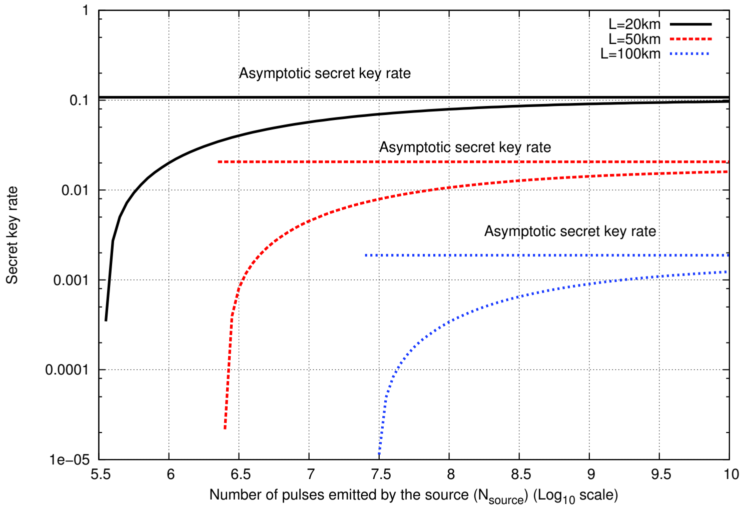


Figure 5.19: (Figure and caption from Ref. [3]) Secret key rate as a function of the number of pulses emitted by the source (N_{source}) for a perfect set-up ($\eta_D = 1$, $\eta_M = 0$). The absorption of the channel is $\alpha = 0.17$ dB/km. Security parameter $\varepsilon = 10^{-9}$, $\varepsilon_{\text{EC}} = 10^{-10}$,$f_{EC} = 1.2$. See Ref. [3] for an explanation of the parameters

6 Outlook

In this dissertation we have studied the performance of QKD in connection to quantum repeaters. The final aim is to have long distance QKD at continental and intercontinental distances. We started by characterizing the most famous quantum repeater protocols, namely the original quantum repeater protocol, the hybrid quantum repeater and the one based on linear optics and atomic ensembles. Each of these types of quantum repeaters has its own experimental and theoretical community. One challenge has been to find a common language for analysing all of them. The result of this effort has been summarized in [4]. One of the more interesting results is that with *not so demanding* technology it may be possible to have one bit/s at 600 km with all three protocols. A restriction of [4] has been that a specific protocol has been considered, which is the one where distillation is performed only in the beginning before starting with entanglement swapping. In [27] we have lifted this constraint and we have found the optimal entanglement distillation protocol and also the optimal scheduling strategy. It turns out that entanglement distillation helps to increase the final secret key rate.

All set-ups considered in [4] and [27] represent a theoretical study of technology that might be realized in the mid-term future. In [2] and [1] we have studied set-ups which are likely to be realized in the near-future. In [2] we generalize the measurement-device independent QKD by adding quantum memories. This represents a quantum repeater set-up with two segments and one repeater station. The advantage of this set-up w.r.t. a standard quantum repeater is that there is no need of entanglement source anymore and that Alice and Bob can use, already available, QKD sources. The result has been that the set-up studied by us permits to improve over a set-up without quantum memories also when quantum memories are imperfect. In [1] we have further generalized the set-up and we have considered the case when in the repeater station there are two arrays of quantum memories. Quantum memories can be connected using multiplexing and in our work we have studied the configuration where long-range connections cannot be performed because too demanding. Our finding was that it is enough to have short-range connections.

Finally, in [3] we give the basis for future research. In particular, we study a possible method permitting to use standard security proofs when there are imperfections in the source and in the detectors. We do this in the particular relevant case that finite-key corrections are considered. The result that we find is that finite-key corrections play a very relevant role in the security analysis.

The results of this dissertation have attracted noticeable attention and have started discussions and further analyses. For example the work published in [78] is based on [2] and it studies the effect of additional imperfections in the detectors and in the source.

Future development of this dissertation may include the analysis of secret key rates with finite-key corrections of the set-up considered in [4, 27, 2, 1]. This task is not completely trivial because there are three levels of optimization:

1. optimization of the security parameters as done in [3],
2. optimization of quantum device parameters, as intensities of the sources or repetition rates. Such analysis has been performed for example in [2, 1],

3. optimization of the quantum repeater protocol parameters like nesting levels, round of distillations and scheduling algorithms. Similar analyses have been performed in [4, 27].

Moreover, the scheme considered in [1] may be improved in order to find the optimal secret key rate. In fact, in our work we have maximized the repeater rate and then under this constraint we have maximized the QBER. As shown in [1] this strategy leads to suboptimal secret key rates. In order to increase it may be necessary to get rid of old pairs which are known from the beginning to not contribute to the secret key rate.

7 List of main results

- The optimization of the secret key rate is a completely different task with respect to the optimization of the final fidelity. The reason is that in the scenario of quantum key distribution there are two competing behaviors, namely, as the final fidelity increases the secret fraction increases and the raw key rate decreases.

- The original quantum repeater protocol, the hybrid quantum repeater and quantum repeaters based on atomic ensembles and linear optics can produce a secret key rate of few bits per second at a distance of about 600 km with typical value of the imperfections that may be achieved in the mid-term future. This is a positive result because it stimulates further research.

- Distillation permits to have higher secret key rates per memory.

- Imperfect quantum memories permit to improve the secret key rate in a measurement-device-independent quantum key distribution set-up. This is an important result because it simplifies the creation of two-segment quantum repeaters.

- Finite-range multiplexing in a set-up with only one repeater station permits to increase the secret key rate, to decrease the required decoherence time and to have most of the advantages of full-range multiplexing.

- In presence of imperfections in the source and in the detectors, finite-size corrections to the secret key rate become even more important w.r.t. scenarios where devices are considered perfect.

Bibliography

[1] S. Abruzzo, H. Kampermann, and D. Bruß. Finite-range multiplexing enhances quantum key distribution via quantum repeaters. *ArXiv: 1309.1106*, 2013.

[2] S. Abruzzo, H. Kampermann, and D. Bruß. Measurement-device-independent quantum key distribution with quantum memories. *ArXiv: 1306.3095*, 2013.

[3] S. Abruzzo, M. Mertz, H. Kampermann, and D. Bruss. Finite-key analysis of the six-state protocol with photon number resolution detectors. In *Security+ Defence*, pages 818917–818917. International Society for Optics and Photonics, 2011.

[4] Silvestre Abruzzo, Sylvia Bratzik, Nadja K. Bernardes, Hermann Kampermann, Peter van Loock, and Dagmar Bruß. Quantum repeaters and quantum key distribution: Analysis of secret-key rates. *Phys. Rev. A*, 87:052315, May 2013.

[5] M Afzelius, T Chaneliére, RL Cone, S Kröll, SA Moiseev, M Sellars, et al. Photon-echo quantum memory in solid state systems. *Laser & Photonics Reviews*, 4(2):244–267, 2010.

[6] Govind P. Agrawal. *Fiber-optic communication systems.* 2007.

[7] J. Amirloo, M. Razavi, and A. Hamed Majedi. Quantum key distribution over probabilistic quantum repeaters. *Phys. Rev. A*, 82(3):032304, September 2010.

[8] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.

[9] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A*, 86:062326, Dec 2012.

[10] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110:010503, Jan 2013.

[11] R.J. Bates. *Optical switching and networking handbook.* McGraw-Hill telecommunications. McGraw-Hill, 2001.

[12] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101(9):093601, Aug 2008.

[13] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59(6):4238–4248, Jun 1999.

[14] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38:447–452, Jul 1966.

[15] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[16] C.H. Bennett, G. Brassard, et al. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India, 1984.

[17] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557–559, 1992.

[18] C.H. Bennett and P.W. Shor. Quantum information theory. *Information Theory, IEEE Transactions on*, 44(6):2724–2742, 1998.

[19] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[20] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, November 1995.

[21] Charles H Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A Smolin, and William K Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76(5):722, January 1996.

[22] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

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

[24] Nadja K. Bernardes, Ludmiła Praxmeyer, and Peter van Loock. Rate analysis for a hybrid quantum repeater. *Phys. Rev. A*, 83(1):012323, Jan 2011.

[25] J. Bochmann, M. Mücke, C. Guhl, S. Ritter, G. Rempe, and D. L. Moehring. Lossless state detection of single neutral atoms. *Phys. Rev. Lett.*, 104:203601, May 2010.

[26] P. Bouguer. *Essai d'optique sur la gradation de la lumière.* 1729.

[27] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß. Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate. *Phys. Rev. A*, 87:062335, Jun 2013.

[28] H. -J Briegel, W. Dür, J. I Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81(26):5932–5935, December 1998.

[29] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, 1998.

[30] D. Bruss and G. Leuchs. *Lectures on quantum information.* Physics Textbook. Wiley-VCH, 2007.

[31] F. Bussieres, N. Sangouard, M. Afzelius, H. de Riedmatten, C. Simon, and W. Tittel. Prospective applications of optical quantum memories. *ArXiv e-prints*, June 2013.

[32] John Calsamiglia and Norbert Lütkenhaus. Maximum efficiency of a linear-optical bell-state analyzer. *Applied Physics B: Lasers and Optics*, 72(1):67–71, 2001.

[33] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143 – 154, 1979.

[34] O. Collins, S. Jenkins, A. Kuzmich, and T. Kennedy. Multiplexed Memory-Insensitive Quantum Repeaters. *Physical Review Letters*, 98(6):060502, February 2007.

[35] T.M. Cover and J.A. Thomas. *Elements of Information Theory.* Wiley, 2012.

[36] I. Csiszar and J. Korner. *Information theory: coding theorems for discrete memoryless systems.* Academic Press, Inc. Orlando, FL, USA, 1982.

[37] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Physical Review Letters*, 77(13):2818, 1996.

[38] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Royal Society of London Proceedings Series A*, 461:207–235, January 2005.

[39] L. -M Duan, M. D Lukin, J. I Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413–418, November 2001.

[40] W. Dür, H. -J Briegel, J. I Cirac, and P. Zoller. Quantum repeaters based on entanglement purification. *Phys. Rev. A*, 59(1):169–181, January 1999.

[41] MD Eisaman, J. Fan, A. Migdall, and SV Polyakov. Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82:071101, 2011.

[42] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[43] D. Elkouss, A. Leverrier, R. Alleaume, and J.J. Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, pages 1879–1883, 2009.

[44] D. Elkouss, J. Martinez, D. Lancho, and V. Martin. Rate compatible protocol for information reconciliation: An application to qkd. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1–5, 2010.

[45] H. Fearn and R. Loudon. Theory of two-photon interference. *J. Opt. Soc. Am. B*, 6(5):917–927, May 1989.

[46] V. Fock. Konfigurationsraum und zweite Quantelung. *Zeitschrift fur Physik*, 75:622–647, September 1932.

[47] Chi-Hang Fred Fung, H. F. Chau, and Hoi-Kwong Lo. Universal squash model for optical communications using linear optics and threshold detectors. *Phys. Rev. A*, 84:020303, Aug 2011.

[48] A. Furusawa and P. van Loock. *Quantum Teleportation and Entanglement.* Wiley, 2011.

[49] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.

[50] Nicolas Gisin and Rob Thew. Quantum communication. *Nature Photonics*, 1(3):165–171, 2007.

[51] Roy J. Glauber. Coherent and incoherent states of the radiation field. *Phys. Rev.*, 131:2766–2788, Sep 1963.

[52] M. Grassl, Th. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Phys. Rev. A*, 56:33–38, Jul 1997.

[53] D.M. Greenberger, K. Hentschel, and F. Weinert. *Compendium of Quantum Physics: Concepts, Experiments, History and Philosophy.* Springer, 2009.

[54] Klemens Hammerer, Anders S. Sørensen, and Eugene S. Polzik. Quantum interface between light and atomic ensembles. *Rev. Mod. Phys.*, 82:1041–1093, Apr 2010.

[55] E. Hecht. *Optics.* Pearson Education, 2008.

[56] J. Hecht. *City of Light: The Story of Fiber Optics.* Oxford University Press paperback. Oxford University Press, 2004.

[57] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1–2):1 – 8, 1996.

[58] W.C. Huffman and V. Pless. *Fundamentals of Error-correcting Codes.* Cambridge University Press, 2003.

[59] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "event-ready-detectors" bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, Dec 1993.

[60] Robert Koenig, Ueli Maurer, and Renato Renner. On the power of quantum memory. *IEEE Trans. Inf. Th., vol. 51, no. 7 (2005).*

[61] Pieter Kok and Samuel L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61:042304, Mar 2000.

[62] Pieter Kok and Brendan W. Lovett. *Introduction to optical quantum information processing.* Cambridge University Press, Cambridge, 2010.

[63] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501, Aug 2005.

[64] K. Kraus, A. Böhm, J. D. Dollard, and W. H. Wootters, editors. *States, Effects, and Operations Fundamental Notions of Quantum Theory*, volume 190 of *Lecture Notes in Physics, Berlin Springer Verlag*, 1983.

[65] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337–4341, Dec 1995.

[66] T D Ladd, P van Loock, K. Nemoto, W J Munro, and Y. Yamamoto. Hybrid quantum repeater based on dispersive CQED interactions between matter qubits and bright coherent light. *New Journal of Physics*, 8(9):184, 2006.

[67] J.H. Lambert and E. Anding. *Lamberts Photometrie: (Photometria, sive De mensura et gradibus luminis, colorum et umbrae) (1760)*. Number v. 1-2 in Ostwalds Klassiker der exakten Wissenschaften. W. Engelmann, 1892.

[68] H.K. Lo and H.F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050, 1999.

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

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

[71] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[72] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[73] M. D. Lukin. *Colloquium* : Trapping and manipulating photon states in atomic ensembles. *Rev. Mod. Phys.*, 75:457–472, Apr 2003.

[74] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature Photonics*, 3(12):706–714, 2009.

[75] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[76] Ji říMinář, Hugues de Riedmatten, and Nicolas Sangouard. Quantum repeaters based on heralded qubit amplifiers. *Phys. Rev. A*, 85:032313, Mar 2012.

[77] T. Moroder, M. Curty, and N. Lütkenhaus. Detector decoy quantum key distribution. *New Journal of Physics*, 11:045008, 2009.

[78] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus. Memory-assisted measurement-device-independent quantum key distribution. *ArXiv e-prints*, September 2013.

[79] K.A. Peacock. *The Quantum Revolution: A Historical Perspective*. Greenwood guides to great ideas in science. Greenwood Press, 2008.

[80] A. Peres. *Quantum theory: concepts and methods*. Springer, 1995.

[81] Nicolas Piro, Felix Rohde, Carsten Schuck, Marc Almendros, Jan Huwer, Joyee Ghosh, Albrecht Haase, Markus Hennrich, Francois Dubin, and Jürgen Eschner. Heralded single-photon absorption by a single atom. *Nature Physics*, 7(1):17–20, 2010.

[82] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[83] J.C. Poggendorff and Physikalische Gesellschaft zu Berlin. *Annalen der Physik*. J.A. Barth, 1852.

[84] M. Razavi, M. Piani, and N. Lütkenhaus. Quantum repeaters with imperfect memories: Cost and scalability. *Phys. Rev. A*, 80(3):032301, September 2009.

[85] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference (TCC)*, volume 3378, pages 407–425. Springer, 2005.

[86] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zurich, 2008.

[87] N. Sangouard. Quantum networks: A future without long memories? *Nature Photonics*, 6:722–724, November 2012.

[88] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83(1):33, March 2011.

[89] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301–1350, Sep 2009.

[90] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, 2008.

[91] Valerio Scarani and Renato Renner. Security bounds for quantum cryptography with finite resources. *Proceedings of TQC2008, Lecture Notes in Computer Science 5106 (Springer Verlag, Berlin), pp. 83-95 (2008)*, 06 2008.

[92] Benjamin Schumacher. Quantum coding. *Phys. Rev. A*, 51:2738–2747, Apr 1995.

[93] C. E. Shannon. A mathematical theory of communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, 5(1):3–55, 2001.

[94] CE Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[95] P.W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

[96] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young. Quantum memories. *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics*, 58:1–22, 2010. 10.1140/epjd/e2010-00103-y.

[97] H. Tanji, S. Ghosh, J. Simon, B. Bloom, and V. Vuletić. Heralded single-magnon quantum memory for photon polarization states. *Phys. Rev. Lett.*, 103(4):43601, 2009.

[98] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, Mar 2011.

[99] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78:032302, Sep 2008.

[100] Alan M Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London mathematical society*, 42(2):230–265, 1936.

[101] P. van Loock, T. D Ladd, K. Sanaka, F. Yamaguchi, Kae Nemoto, W. J Munro, and Y. Yamamoto. Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.*, 96(24):240501, June 2006.

[102] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik*. "Die" Grundlehren der mathematischen Wissenschaften / "Die" Grundlehren der mathematischen Wissenschaften. Springer, 1996.

[103] Reinhard F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989.

[104] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[105] A. Zeilinger. General properties of lossless beam splitters in interferometry. *American Journal of Physics*, 49:882–883, 1981.

Finite-key analysis of the six-state protocol with photon-number-resolution detectors.
S. Abruzzo, M. Mertz, H. Kampermann, and D. Bruß.
Proc. SPIE, 8189:818917, 2011.

Journal: Proc. SPIE 8189, Optics and Photonics for Counterterrorism and Crime Fighting VII; Optical Materials in Defence Systems Technology VIII; and Quantum-Physics-based Information Security, 818917 (October 19, 2011);
Contribution: first author, idea to perform the analysis, scientific work and preparation of the manuscript.
Percentage of my work: 95%.

Finite-key analysis of the six-state protocol with photon-number-resolution detectors

Silvestre Abruzzo,* Markus Mertz, Hermann Kampermann, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany

(Dated: November 14, 2011)

The six-state protocol is a discrete-variable protocol for quantum key distribution, that permits to tolerate a noisier channel than the BB84 protocol. In this work we provide a lower bound on the maximum achievable key rate of a practical implementation of the entanglement-based version of the six-state protocol. Regarding the experimental set-up we consider that the source is untrusted and the photon-number statistics is measured using photon-number-resolving detectors. We provide the formula for the key rate for a finite initial number of resources. As an illustration of the considered formalism, we calculate the key rate for the setting where the source produces entangled photon pairs via parametric down-conversion and the losses in the channel depend on the distance. As a result we find that the finite-key corrections for the considered scenario are not negligible and they should be considered in any practical analysis.

I. INTRODUCTION

Quantum Key Distribution (QKD) was proposed for the first time in 1984 by Bennett and Brassard[4](BB84 protocol) and it is a method for permitting two parties, usually called Alice and Bob, to share a secret bit-string that might be used as a key for cryptographic applications. The most prominent application is encryption with the one-time pad[25], where Alice sums bitwise the message and the key for obtaining the cypher-text. The cypher-text is then sent to Bob, who recovers the original text by using the knowledge of the key. Note that the encrypted text is sent publicly on the channel and therefore it is readable by any eavesdropper who is tapping the channel. The security of this scheme relies on the fact, that from the eavesdropper's point of view the distribution of all possible cypher-texts is uniform[24]. This last requirement implies that the key is chosen at random using a uniform distribution on the set of all possible keys. This is the point where QKD enters the game. In fact, using the laws of quantum mechanics, it is possible to create a bit-string with the guarantee that it is (almost) random from an eavesdropper's point of view[21]. In this paper we consider the entanglement-based version of the six-state protocol[3, 5, 7, 10]. It has been realized that, due to the use of a tomographic measurement, the six-state protocol is more robust against channel imperfections than the BB84 protocol. The six-state protocol was implemented experimentally, e.g. by Kwiat's group[13]. However, in the meantime the security analysis of this protocol has become more and more complete. In 2001, H.K. Lo[14] proved security of the protocol against the most general type of attacks and some years later R. Renner et al.[9, 12, 19] proved the security of the six-state protocol using information-theoretical arguments. Finite-key effects were considered for the first time by V. Scarani and R. Renner[22, 23] and by T. Meyer et al.[16]. It turns out that there is an initial regime where BB84 is advantageous over the six-state protocol and then there exists a second regime where the six-state protocol leads to higher secret key rates. The reason is the sifting procedure. More precisely, in the standard six-state protocol all measurement bases are chosen with the same probability and as a consequence, $\frac{2}{3}$ of the measurement outcomes are discarded due to this sifting. In the standard BB84 protocol the fraction of discarded outcomes is $\frac{1}{2}$. However, in the year 2005, it was proven by H.K. Lo and M. Ardehali[15] that it is possible to choose one basis with high probability and the other two (one for the BB84) with a negligible probability without jeopardizing the security of the protocol. In the asymptotic case, using this biased scheme, the sifting ratio approaches one and therefore the six-state protocol permits to give a higher secret key rate. However, when finite-key corrections are considered, for small block sizes it is not possible to choose with an arbitrary large bias the measurement basis and therefore the sifting advantage of the BB84 protocol leads to higher key rates. Note that recent papers considering the finite-key analysis studying the six-state protocol[1, 6, 22, 23] do not consider a realistic implementation with imperfections in the source, the channel and the detectors. The security proof becomes more involved due to the fact that a realistic source does have multi-photon pulses, which need special care. A common receipt is given by the squashing model[2], which permits to analyze the security of multi-photon sources using single photons and a special post-processing of the outcomes. However, it was proven that an active measurement set-up for the six-state protocol does not permit to use the squashing model[2]. A squashing model for the passive measurement set-up exists[2], but up to now only in the case of perfect detectors. However, another technique permitting to overcome the need of squashing model has

* abruzzo@thphy.uni-duesseldorf.de

been developed by T. Moroder et al.[17]. The main observation is, that if we had perfect photon-number-resolution detectors (PNRD), then we would be able to avoid the problem of multi-photon pulses by post-selecting only single-photon pulses. In their paper the authors developed an experimentally feasible technique permitting to acquire the statistics of a PNRD. In this paper we want to extend their analysis considering finite-key corrections. In order to state clearly our result, we will consider an ideal set-up, where we perform a Quantum Non-Demolition (QND) measurement permitting to detect error-free the number of photons present in an incoming pulse. We will use a standard measurement set-up, which has detectors with finite efficiency. Note that, although the set-up we consider may be idealized, it permits to provide a lower bound for the performance of the six-state protocol in presence of a realistic scenario. Finally, we will consider a specific example, i.e. we will calculate the secret key rate in the finite case for a spontaneous parametric down-conversion of type-II (SPDC) source.

The paper is organized as follows. In section II we describe the set-up followed by a presentation of the QKD protocol. In section III we present the security analysis and the formula for the secret key rate. In section IV we calculate the optimal secret key rate for a SPDC source. Finally, in section V we conclude this analysis.

II. THE ENTANGLED VERSION OF THE SIX-STATE PROTOCOL

In the first part of this section we present the set-up used by Alice and Bob. The second part considers an outline of the QKD protocol.

A. Set-up (see Fig. 1)

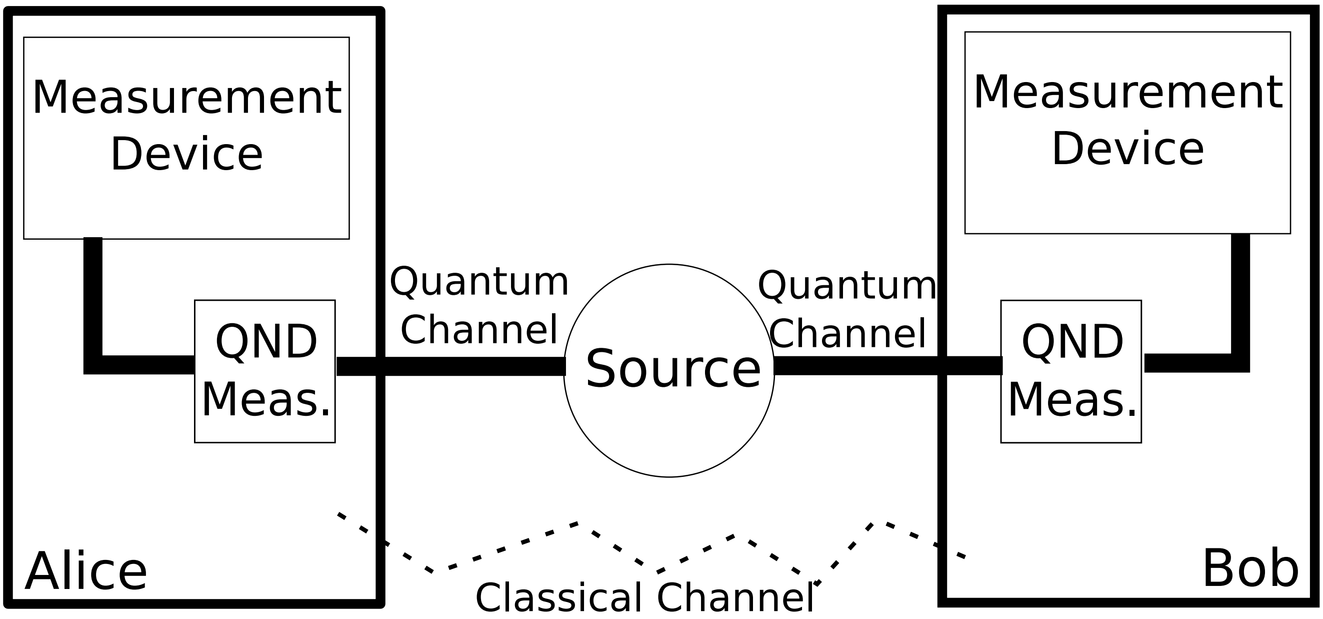


FIG. 1. Set-up for QKD. The quantum channel is completely controlled by the eavesdropper. The classical channel is authenticated but otherwise tapped by the eavesdropper. The laboratories are by definition secure.

- **Source.** An arbitrary source is placed in the middle of Alice and Bob. The source sends an n-photon pulse to Alice and an m-photon pulse to Bob.

- **Quantum Channel.** We consider that the channel is lossy but otherwise error-free. We suppose that the signals are encoded in the source, such that they do not experience any decoherence in the channel.

- **Classical Channel.** The classical channel is authenticated.

- **Alice's (Bob's) laboratory.** We assume that the laboratories are trusted. Alice (Bob) performs a QND measurement for measuring the number of photons contained in the incoming pulse. The POVM of the QND measurement is composed of two elements $\{|1\rangle\langle 1|, \mathbb{1} - |1\rangle\langle 1|\}$, where $\{|n\rangle\}$ is the Fock-basis. After the QND measurement, the pulse passes a standard QKD-measurement set-up, where one measurement basis is chosen at random out of the X-, Y- and Z-direction. Note that regarding the detectors, we assume that they have finite efficiency η_D and negligible background noise. Moreover, we consider a misalignment[17, 21] in the detectors. Each time that a single photon arrives at the detection device, it is measured correctly with probability $1 - \eta_M$.

B. QKD protocol

1. **Entanglement generation and distribution.** A source generates entangled pairs which are distributed through the quantum channel to Alice and Bob.

2. **Measurement.** Alice and Bob choose at random and independently the measurement basis and to perform the measurement on the incoming pulse. We consider a biased choice of the bases, i.e., the basis Z is chosen with probability $p_Z \geq \frac{1}{3}$ and the other two bases are chosen with the same probability $p_X = p_Y$. The result of the measurements is recorded in a vector of the form $(t^A, b_0^A, b_1^A, p^A, basis^A)$, where $b_i^A = 0$ indicates that the detector for the classical value i on Alice side did not experience a click, otherwise $b_i^A = 1$. The entry p^A contains the result of the QND measurement, in particular $p^A = 1$ when a 1-photon pulse is measured and $p^A = 0$ otherwise. The last entry contains a label for the measurement basis. The first entry t^A is a tag permitting to distinguish the measurements, e.g., the time of occurrence of the measurement.

3. **Vacuum sifting.** During this sifting we remove the non-measurement results. This step is performed locally and without communication between Alice and Bob. Let i=A,B. When $p^i = 1$, it is still possible that $b_0^i + b_1^i = 0$, i.e., none of the detectors has clicked. This can happen due to the finite efficiency of the detectors. We can eliminate these events safely, incorporating the efficiency of the detectors in the efficiency of the channel. During this step Alice (Bob) calculate the value of $b_0^i + b_1^i$ and set $p^i = 0$ every time that $b_0^i + b_1^i = 0$.

4. **Pulse sifting.** We use the output of the QND measurement for conditioning the type of bits used for the key. Alice and Bob communicate via the classical channel the value of p^A and p^B for each measurement and discard all measurements with $p^A \times p^B \neq 1$[17]. Note that this post-processing is possible only due to the fact, that the QND measurement is perfect and that we are considering entanglement-based QKD. If one of the two assumptions above is dropped, then security loopholes will arise[21].

5. **Bases sifting.** Alice and Bob exchange information regarding the measurement bases and discard the outcomes coming from different bases.

6. **Parameter estimation.** Alice and Bob take a random sample from each basis and use this sample for estimating the Quantum Bit Error Rate (QBER) for each basis. We denote with e_{X,m_X} the fraction of erroneous bits in the sample of length m_X. We choose[6] $m_X = m_Y = m_Z := Np_X^2$, where N is the number of bits after the pulse sifting. The QBERs along the Y and Z bases are defined analogously. Note that the worst-case QBER can be estimated with the fluctuations due to the finiteness of the sample.

7. **Error correction.** During this step Alice and Bob apply a one-way error correction protocol and correct their strings. As result they will exchange leak_{EC} bits on the channel.

8. **Error verification.** In realistic implementations it is possible that at the end of the error correction protocol, Alice and Bob do not have perfectly correlated bits. In order to acquire confidence regarding the remaining errors, they apply a two-universal hash function on their strings and they communicate the result of the function on the channel. This step costs $\log_2(\frac{2}{\varepsilon_{\text{EC}}})$ bits. If the resulting hash tag is the same, then the two strings are the same with probability $1 - \varepsilon_{\text{EC}}$. If the hashing produces a different outcome, Alice and Bob may perform more error correction followed by another error verification.

9. **Privacy amplification.** Alice and Bob apply a two-universal hash function in order to shrink their string. The resulting string is called the key.
   In the next section we will discuss a bound on the achievable key length ℓ as a function of a security parameter ε.

III. FINITE SECRET KEY RATE

The secret key rate is the relevant figure of merit for describing the performance of a QKD protocol. First of all, we are going to state the definition of security.

Definition III.1. [18, 20] Let ρ_{KE} be the classical-quantum-state describing the classical key K of length ℓ, distilled at the end of a QKD protocol, correlated with the quantum states of the eavesdropper ρ_E. The state ρ_{KE} is said to be ε-secure if

$$\min_{\rho_{E'}} \frac{1}{2} \|\rho_{KE} - \frac{1}{2^\ell} \mathbb{1} \otimes \rho_{E'}\|_1 \leq \varepsilon, \tag{1}$$

where $\rho_{E'}$ is the quantum state of an eavesdropper not correlated with the key.

The definition states that from the eavesdropper's (Eve) point of view the classical key K is indistinguishable from a random and uniform key with probability $1-\epsilon$. Note that the used definition of security is composable, i.e. if we have two protocols characterized by two different probabilities of failure, then, after a concatenation of these protocols, the probability of failure of the global protocol will be bounded by the sum of the single probabilities of failure.

In the following we derive a formula for the ε-secure key length ℓ. We consider that Eve has complete control over the quantum channel and the source. Moreover, we consider the *uncalibrated scenario*[21], where the finite efficiency of the detectors are also attributed to Eve. Let p_{11} be the probability that Alice and Bob receive a single photon. Then, starting with N_{source} initial pulses, the steps $1-4$ of the QKD protocol (see Fig. 1) decrease the number of signals to $N_{\text{source}} p_{11}$. Afterwards, the bases-sifting and the PE lead to $N_{\text{source}} p_{11} \left(p_Z^2 - p_X^2\right)$ resulting bits. For PE $3p_X^2$ signals are used to estimate the QBER. The fluctuations due to finite statistics have been analyzed in [6, 8, 22, 23] . Note that differently to [6] we do not consider one symmetrized QBER. Instead we treat the QBER for each direction separately.

Let e_{i,m_i} be the measured QBER in direction $i = X, Y, Z$, then with probability $1-\varepsilon_{PE}$ the real QBER e_i is such that[6, 8, 22, 23]

$$e_i \leq e_{i,m_i} + 2\zeta\left(\varepsilon_{PE}, m_i\right) \tag{2}$$

with

$$\zeta(\varepsilon_{PE}, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{PE}}\right) + 2\ln(m+1)}{8m}}. \tag{3}$$

For the error correction protocol the total number of bits exchanged during the procedure is an upper bound on the information leaked to the eavesdropper about the final key. For the simulations, we will use [8, 23]

$$\text{leak}_{\text{EC}} := f_{\text{EC}} n h(e), \tag{4}$$

where $f_{\text{EC}} \geq 1$ depends on the used EC protocol, $h(e)$ is the binary Shannon entropy, i.e., $h(e) = -e\log e - (1-e)\log(1-e)$ and e is the QBER. This definition comes from the fact that $nh(e)$ represents the asymptotic number of bits used by a perfect error correction protocol. The coefficient f_{EC} represents a deviation of the real protocol from the asymptotic one.

Regarding privacy amplification many bounds on the achievable secret key length are placed at the disposal in the literature[1, 6, 22, 23]. Note that the bounds given in [1, 6] are tighter than the bound given in [22, 23] . However, they require that the channel is symmetric. Although it is possible to transform any channel in a symmetric one, we consider the bound provided in [22, 23] to take the analysis simple and more general.

The following result summarizes the preceding considerations and provides a formula for the achievable secret key length. It is important to emphasize, that the following theorem holds only due to our special set-up with the QND measurement and the particular post-processing, which selects only the pulses containing one photon.

Theorem III.2 ([22, 23])**.** *Let N_{source} being the number of measurements performed by Alice and Bob. Let p_{11} be the fraction of attempts resulting in a single-photon pulse entering Alice's and Bob's laboratories. The number of bits allocated for extracting a key is $n := N_{\text{source}} p_{11}(p_Z^2 - p_X^2)$. If Alice and Bob distill a key of length*

$$\ell \leq \max_{\overline{\varepsilon}, \varepsilon_{PE}, \varepsilon_{PA}, p_X, p_{11}} \left[n(S_\zeta(X|E) - f_{\text{EC}} h(e_Z)) - 2\log_2 \frac{1}{\varepsilon_{PA}} - \log_2 \frac{2}{\varepsilon_{EC}} \right], \tag{5}$$

then it is ε-secure, with $0 \leq \bar{\varepsilon} + \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{PE} \leq \varepsilon$. The quantity $S_\zeta(X|E)$ is given by [21–23]

$$S_\zeta(X|E) := 1 - e_Z h\left(\frac{1 + (e_X - e_Y)/e_Z}{2}\right) - (1 - e_Z) h\left(\frac{1 - (e_X + e_Y + e_Z)/2}{1 - e_Z}\right) - 5\sqrt{\log_2\left(\frac{2}{\bar{\varepsilon}}\right)\frac{1}{n}}. \tag{6}$$

The entropy $S_\zeta(X|E)$ is calculated with the QBER inferred during the parameter estimation protocol (see Eq. (2)). We would like to point out that the theorem above is a standard theorem, the unique difference is that we are not using all signals for extracting the key but only the signals coming as single-photon pulse.

The asymptotic formula for the secret key rate can be recovered as a special case of the theorem above for $n \to \infty$ and $\varepsilon \to 0$.

IV. CASE STUDY: SPDC SOURCE

In this section we will calculate the achievable secret key length for a pumped type-II down-conversion source[11]. The produced state by this source can be written as

$$|\phi\rangle_{AB} := \sum_{n=0}^{\infty} \sqrt{p_n}\, |\phi_n\rangle_{AB}\,, \tag{7}$$

where

$$p_n := \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}, \tag{8}$$

and

$$|\phi_n\rangle_{AB} := \sum_{m=0}^{n} \frac{(-1)^m}{\sqrt{n+1}} |n-m, m\rangle_A |m, n-m\rangle_B\,. \tag{9}$$

The state above is written along one fixed direction, e.g. the Z-direction. The meaning of the notation $|l_H, l_V\rangle_A$ is that on Alice side, a pulse with $l_H + l_V$ photons is coming and $l_H(l_V)$ have horizontal (vertical) polarization.

The quantity 2λ represents the mean photon pair number per pulse.

In the following we calculate the quantities that enter the formula of the secret key rate (Eq. (5)). First of all, we express the probability that Alice and Bob receive only one photon. Then we calculate the QBER produced by the incoming pulse and finally, we find the optimal mean photon pair number per pulse, i.e. the one which maximize the secret key rate.

A. Calculation of p_{11}

We denote with η_A the total transmittivity of Alice's set-up. It is given by $\eta_A := \eta_D \eta_C(L/2)$, where η_D is the efficiency of Alice's detectors and L is the distance between Alice and Bob. We consider a lossy, but otherwise perfect channel with attenuation coefficient $\alpha = 0.17$ dB/km, such that the transmission probability of a photon is given by $\eta_C(L) := 10^{-\frac{\alpha L}{10}}$.

Analogously we define the total efficiency on Bob's set-up, denoted by η_B. When an n-photon pulse is produced, during its travel on the channel and during the detection, some photons could be absorbed. The following formula gives the probability that an n-photon pulse becomes a 1-photon pulse,

$$W_n := p_n n^2 (1 - \eta_A)^{n-1} (1 - \eta_B)^{n-1} \eta_A \eta_B. \tag{10}$$

The factor n^2 is a combinatorial factor coming from our ignorance which photon was absorbed. The total probability that both, Alice and Bob, receive one photon is given by

$$p_{11} := \sum_{n=1}^{\infty} W_n. \tag{11}$$

B. Calculation of the QBER

In the six-state protocol measurements are performed along three orthogonal directions in the Bloch sphere, and, as explained above, three QBERs are involved. The Hamiltonian of the parametric down-conversion process is invariant under rotations from the X- to Y-, Y- to Z- and Z- to X-basis. Therefore, the state in Eq. (7) remains invariant in form under these transformations and hence the QBER is the same in all directions, i.e., there is only one QBER to consider, e.g., for the Z-direction. There are two contributions to the QBER. The first one comes from the misalignment and the second one is due to the fact, that the entering state is not maximally entangled. Let e_n be the QBER generated by $|\phi_n\rangle$ when misalignment is not considered. Then the total QBER is given by

$$e_{PDC} := \frac{\sum_{n=1}^{\infty}(e_M(1-e_n)+(1-e_M)e_n)W_n}{p_{11}}, \tag{12}$$

where $e_M := 2\eta_M(1-\eta_M)$ and η_M is the misalignment-error probability. The first term of e_{PDC} accounts for the fact, that even if the incoming state did not produce a QBER, due to the misalignment there would be an error. The second contribution comes from the error generated by the incoming photons. Note that terms of the form $e_M e_n$ are not considered, because the simultaneous appearance of these two errors will produce correlated outcomes. The quantity e_n can be calculated with the help of Eq. (9). This state is the superposition of $n+1$ states. The first and the last term in the summation, with $m=0$ or $m=n$ will produce a correlated outcome. On the contrary the remaining $n-1$ elements in the summation will produce an error with probability $\frac{1}{2}$. Therefore we get

$$e_n = \frac{(n+1)-2}{2(n+1)} = \frac{1}{2}\left(1-\frac{2}{n+1}\right). \tag{13}$$

From the formula above it is possible to verify that $e_1 = 0$, which is consistent with the fact that $|\phi_1\rangle$ is a maximally entangled state.

The common free parameter in the QBER e_{PDC} and in p_{11} is the mean number of photons per pulse 2λ.

Therefore, in the following we will calculate the optimal λ permitting to maximize the secret key rate.

As shown in Fig. 2, in order to have a low QBER e_{PDC} it is necessary to have λ small. For short distances, e.g. $L = 20$km it is possible to choose $\lambda < 20$ and at the same time be able to extract a key. The reason is that the multi-photon pulses arrives to Alice and Bob without an appreciable degradation and therefore, we are able to filter those contribution to the QBER during the pulse sifting. However, the situation changes when the distance between Alice and Bob increases. We see that the mean number of photons per pulse has to be much smaller than 1 in order to decrease the multi-photon contribution to the QBER. From Fig. 2 we see that for $L \geq 100$km we have to choose $\lambda < 1$ in order to have a QBER smaller than the maximal QBER tolerated by the six-state protocol.

C. Asymptotic secret key rate

The secret key rate in the asymptotic case characterizes the maximal achievable secret key rate in case of perfect error correction, no uncertainty in the estimation of the QBER and perfect security ($\epsilon = 0$). The formula is given by

$$r_\infty := \lim_{\substack{n\to\infty \\ \varepsilon\to 0}} \frac{l}{N_{\text{source}}} = \max_{\lambda}\left[p_{11}\left((1-e_{PDC})\left(1-h\left(\frac{1-3e_{PDC}/2}{1-e_{PDC}}\right)\right)-h\left(e_{PDC}\right)\right)\right]. \tag{14}$$

In Fig. 3 the secret key rate is shown as a function of the distance for two different experimental set-ups. A comparison between an idealized scenario ($\eta_D = 1, \eta_M = 0$) and a more realistic one ($\eta_D = 0.1, \eta_M = 0.03$) shows that the secret key rate decreases of at least 2 orders of magnitude. Regarding the optimal mean of photon-number per pulse, as shown in Fig. 4, the difference is of the order of 1. The optimized function is non-linear and the used optimization algorithm may only permit to find a local optimum.

Finally, we would like to point out, that a similar analysis of the asymptotic case was performed by Moroder et al.[17] with a source placed in an asymmetric position, i.e., closer to Bob than to Alice.

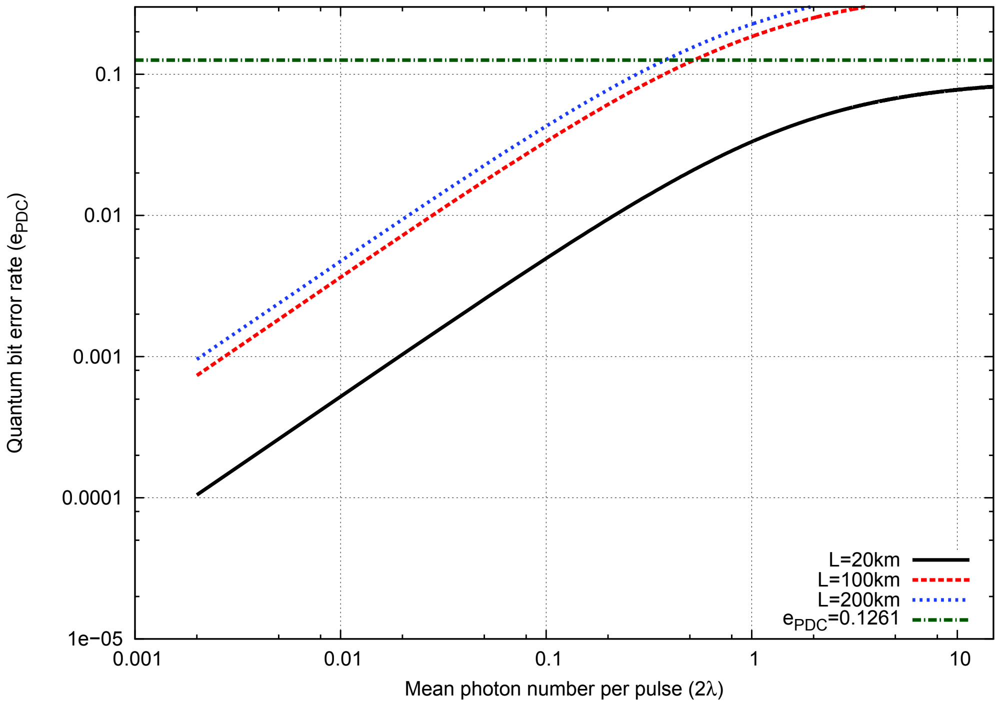


FIG. 2. (Color online) Value of e_{PDC} (Eq. (12)) as a function of the probability that both, Alice and Bob, receive one photon as a function of the mean number of photons produced by the source for various distances. The horizontal line represents the maximal QBER tolerated by the six-state protocol. The absorption of the channel is $\alpha = 0.17$ dB/km and Alice and Bob use perfect detectors $\eta_D = 1, \eta_M = 0$.

D. Finite-key analysis

In a practical execution of a QKD protocol, the initial number of resources is always finite, therefore we need to take into account corrections to the asymptotic secret key rate. The formula for the secret key rate is

$$r := \frac{\ell}{N_{\text{source}}} = \underset{\overline{\varepsilon},\varepsilon_{\text{PE}},\varepsilon_{\text{PA}},p_X,\lambda}{max} \left[p_{11}(p_Z^2 - p_X^2) \left((1-e_{PDC}) \left(1 - h\left(\frac{1-3e_{PDC}/2}{1-e_{PDC}} \right) \right) - f_{\text{EC}} h(e_Z) \right) \right. \tag{15}$$

$$\left. -2\log_2 \frac{1}{\varepsilon_{\text{PA}}} - \log_2 \frac{2}{\varepsilon_{\text{EC}}} - 5\sqrt{\log_2\left(\frac{2}{\overline{\varepsilon}}\right)} \right] . \tag{16}$$

The calculations are done in such a way, that we optimize over all free parameters: the mean number of photons per pulse (λ), the probability to measure along the Z basis (p_Z), the failure probability for the parameter estimation (ε_{PE}), for privacy amplification (ε_{PA}) and the smoothing parameter ($\overline{\varepsilon}$).

For extracting a key it is necessary to have a block bigger than a specific length. As shown in Fig. 5, even for short distances the source has to emit at least 10^5 pulses with in mean $\lambda \approx 0.1$ photons per pulse for extracting a key of 1 bit. However, if we consider detector inefficiencies and misalignment errors, the requirements will become much more stringent. In particular, we need at least 10^9 pulses for extracting a key.

The second quantity we want to analyze is the secret key rate (Eq. (5)). As shown in Fig. 6, for a perfect set-up ($\eta_D = 1$, $\eta_M = 0$) the finite secret key rate differs significantly from the asymptotic secret key rate. In particular, for all distances considered in Fig. 6, the secret key rate differs of at least 10% ($N_{\text{source}} = 10^{10}$, $L = 20$ km) from the asymptotic key rate. However, for more realistic initial number of pulses, the difference is bigger, e.g for $L = 100$ km and $N_{\text{source}} = 10^8$, the difference between the asymptotic secret key rate and the one with finite-key corrections is of one order of magnitude. In case of imperfections we will have similar plots but with a worse secret key rate. However, the qualitative behavior of the plot remains similar to Fig. 6.

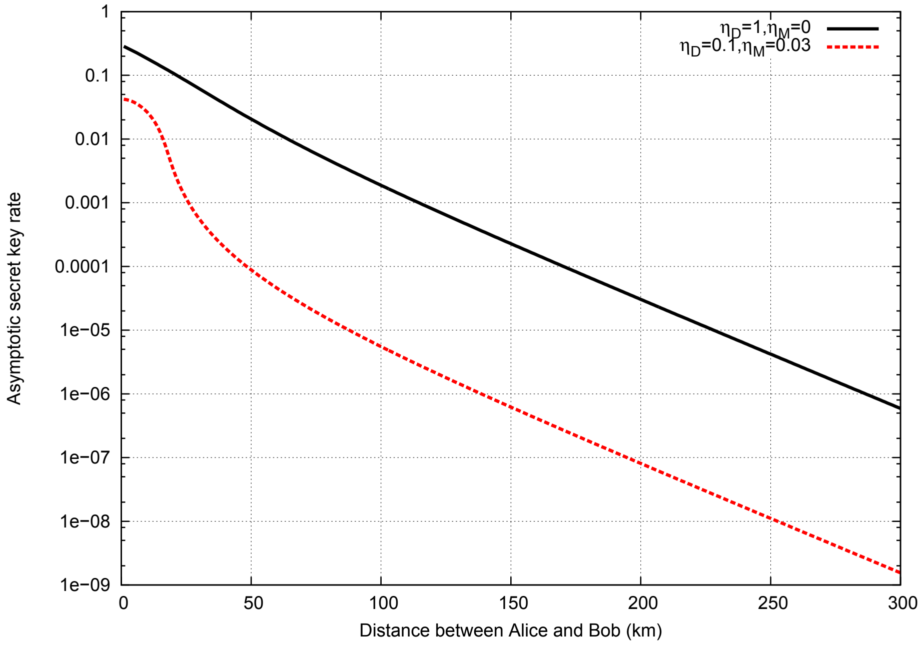


FIG. 3. (Color online) Asymptotic secret key rate (Eq. (14)). The absorption of the channel is $\alpha = 0.17$ dB/km.

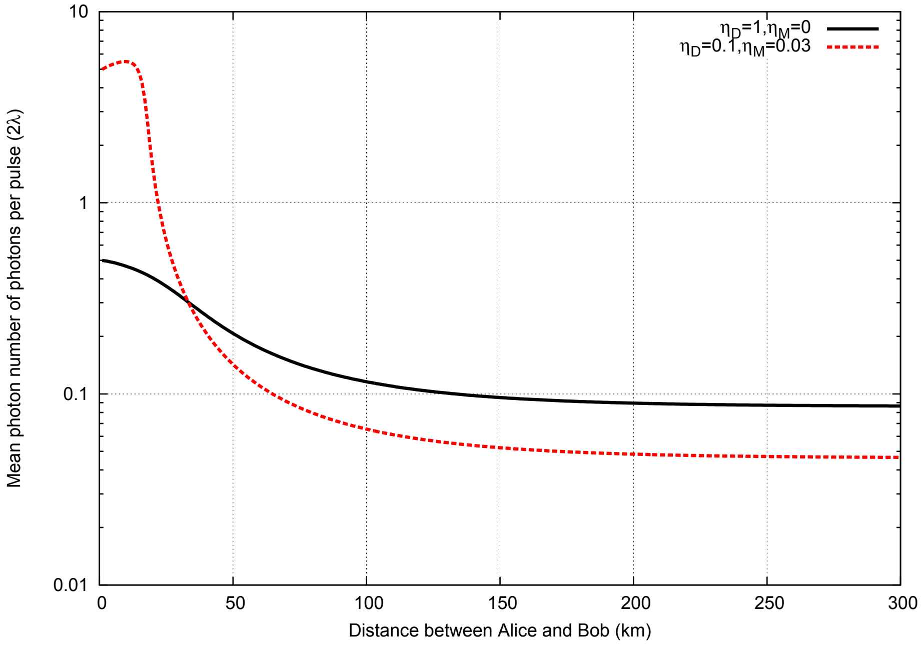


FIG. 4. (Color online) Optimal mean of photon-number per pulse. The absorption of the channel is $\alpha = 0.17$ dB/km.

V. CONCLUSION

In this paper we did a step towards the analysis of a realistic implementation of the entanglement-based version of the six-state protocol. We considered that the standard QKD measurement is preceded by a QND measurement permitting to know the number of photons entering in the source. This special set-up with a post-processing which

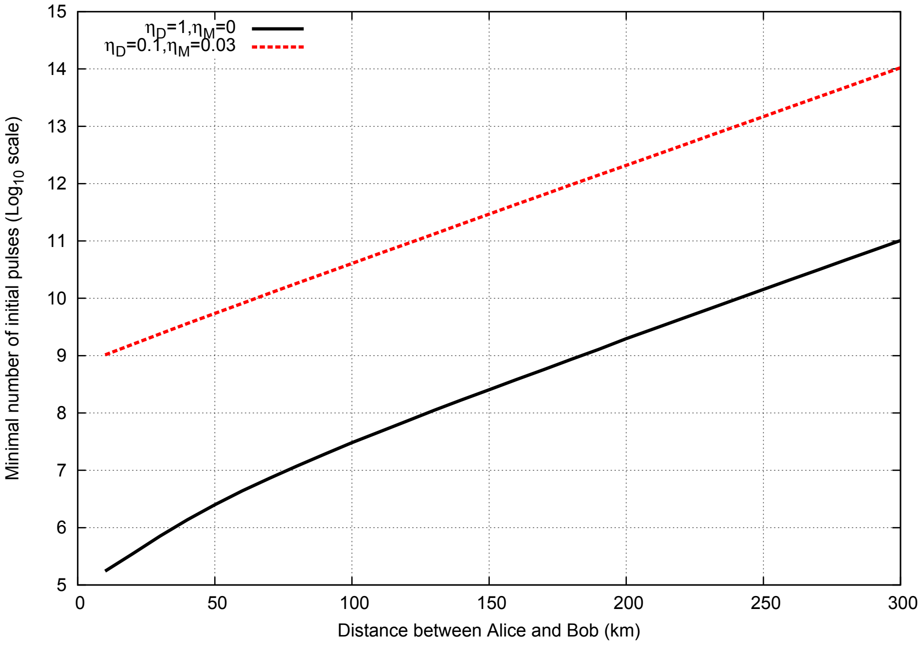


FIG. 5. (Color online) Minimal number of initial pulses permitting to extract a key of 1 bit as a function of the length L for a perfect set-up ($\eta_D = 1$, $\eta_M = 0$). The absorption of the channel is $\alpha = 0.17$ dB/km. Security parameter $\varepsilon = 10^{-9}$, $\varepsilon_{\mathrm{EC}} = 10^{-10}$, $f_{EC} = 1.2$.

considers only signals coming from a single-photon source permits to evaluate secret key rates for the six-state protocol. We studied the case of an arbitrary large number of initial pulses as well as of a finite key. As result we found that in realistic implementations with finite-efficiency detectors and misalignment, the minimal number of pulses for being able to extract a key is around 10^9 pulses at the distance of a few kilometers. Note that this is a very stringent requirement. In fact, considering an ordinary source, which emits pulses at the rate of 10 MHz, at the distance of 20 km between Alice and Bob, the time needed for extracting a key of 1 bit will be of the order of 100 seconds. Using the asymptotic key formula, in the same time, it could be possible to obtain a key of length 10^6 bits, which would be unfortunately completely insecure. Therefore, we emphasize once again that finite-key corrections are necessary for a realistic and correct security analysis.

Regarding future work, we underline that more realistic experimental imperfections should be taken into account in order to characterize the performance of the six-state protocol. In a future work, we want to consider the encoding of the quantum bits on the quantum channel and to study the effects of decoherence. This is a problematic issue which limits practical implementations of the six-state protocol and needs a careful analysis.

ACKNOWLEDGMENTS

We would like to thank Sylvia Bratzik and Tobias Moroder for valuable and enlightening discussions. We acknowledge partial financial support by Deutsche Forschungsgemeinschaft (DFG) and by BMBF (project QuOReP).

[1] Abruzzo, S., Kampermann, H., Mertz, M., and Bruß, D. (2011). Quantum key distribution with finite resources: Secret key rates via rényi entropies. *Physical Review A*, 84(3):032321.

[2] Beaudry, N. J., Moroder, T., and Lütkenhaus, N. (2008). Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101(9):093601.

[3] Bechmann-Pasquinucci, H. and Gisin, N. (1999). Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59(6):4238–4248.

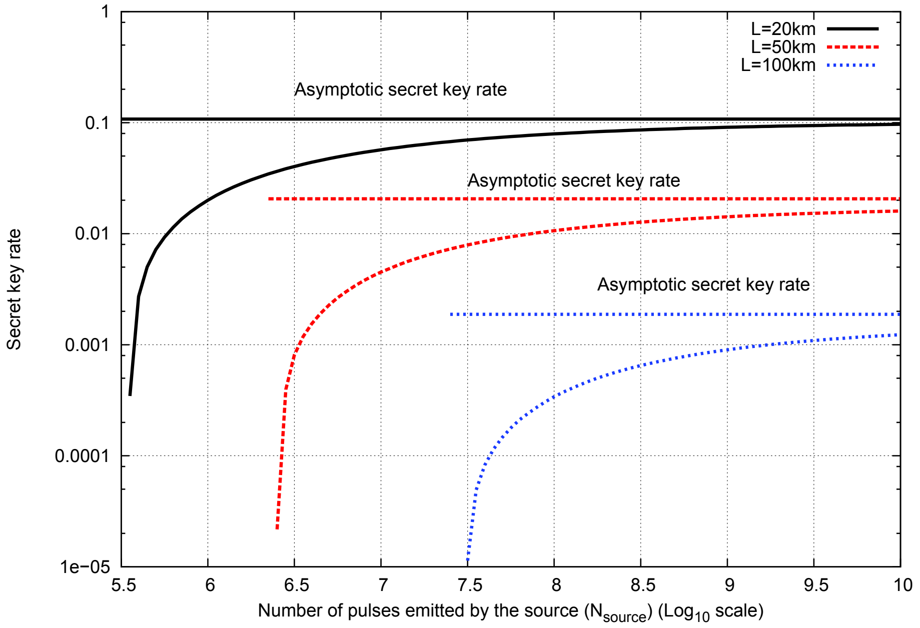


FIG. 6. (Color online) Secret key rate as a function of the number of pulses emitted by the source (N_{source}) for a perfect set-up ($\eta_D = 1$, $\eta_M = 0$). The absorption of the channel is $\alpha = 0.17$ dB/km. Security parameter $\varepsilon = 10^{-9}$, $\varepsilon_{\text{EC}} = 10^{-10}$,$f_{EC} = 1.2$.

[4] Bennett, C. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175. Bangalore, India.

[5] Bennett, C., Brassard, G., and Mermin, N. (1992). Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557–559.

[6] Bratzik, S., Mertz, M., Kampermann, H., and Bruß, D. (2011). Min-entropy and quantum key distribution: Nonzero key rates for "small" numbers of signals. *Phys. Rev. A*, 83(2):022330.

[7] Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021.

[8] Cai, R. Y. Q. and Scarani, V. (2009). Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024.

[9] Christandl, M., Renner, R., and Ekert, A. (2004). A generic security proof for quantum key distribution. *Arxiv preprint quant-ph/0402131*.

[10] Ekert, A. (1991). Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663.

[11] Kok, P. and Braunstein, S. L. (2000). Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61(4):042304.

[12] Kraus, B., Gisin, N., and Renner, R. (2005). Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95(8):080501.

[13] Kwiat, P., Enzer, D. G., Hadley, P. G., and Peterson, C. G. (2001). Experimental six-state quantum cryptography. In *International Conference on Quantum Information*, page FQIPB4. Optical Society of America.

[14] Lo, H. (2001). Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Information and Computation*, 1(2):81–94.

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

[16] Meyer, T., Kampermann, H., Kleinmann, M., and Bruß, D. (2006). Finite key analysis for symmetric attacks in quantum key distribution. *Phys. Rev. A*, 74(4):042340.

[17] Moroder, T., Curty, M., and Lütkenhaus, N. (2009). Detector decoy quantum key distribution. *New Journal of Physics*, 11(4):045008.

[18] Müller-Quade, J. and Renner, R. (2009). Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006.

[19] Renner, R., Gisin, N., and Kraus, B. (2005). Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332.

[20] Renner, R. and König, R. (2005). Universally composable privacy amplification against quantum adversaries. In Kilian, J., editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer Berlin / Heidelberg.

[21] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301–1350.

[22] Scarani, V. and Renner, R. (2008a). Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100(20):200501.

[23] Scarani, V. and Renner, R. (2008b). Security bounds for quantum cryptography with finite resources. In Kawano, Y. and Mosca, M., editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 5106 of *Lecture Notes in Computer Science*, pages 83–95. Springer Berlin / Heidelberg.

[24] Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715.

[25] Vernam, G. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *American Institute of Electrical Engineers, Transactions of the*, 45:295–301.

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

Journal: Physical Review A
Impact Factor 2012: 3.042
Contribution: first author, organization of the manuscript and writing of most of it. I conducted the theoretical analysis and the calculations for the original quantum repeater and the quantum repeater with atomic ensembles. I did not performed the calculations when distillation is present with the exeption of fig. 6.
Percentage of my work: 60%.

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, Universitätsstr. 1, 40225 Düsseldorf, Germany*
[2]*Optical Quantum Information Theory Group, Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany*
[3]*Institute of Theoretical Physics I, Universität Erlangen-Nürnberg, Staudtstr. 7/B2, 91058 Erlangen, Germany*
[4]*Institute of Physics, Johannes-Gutenberg Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany*

(Dated: April 12, 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 *et al.* , the so-called hybrid quantum repeater using optical coherent states dispersively interacting with atomic spin qubits, and the DLCZ-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 non-zero 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.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.67.-a, 03.67.Bg, 42.50.Ex

I. INTRODUCTION

Quantum communication is one of the most exciting and well developed areas of quantum information. Quantum key distribution (QKD) is a sub-field, 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 set-up, 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 non-zero 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 manuscript 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], section IV analyzes the hybrid quantum repeater [13], and finally, in section V, we investigate quantum repeaters with atomic ensembles [12]. The conclusion will be given in section VI, and more details on the calculations will be presented in the appendix.

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.

[*] abruzzo@thphy.uni-duesseldorf.de

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). 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*.

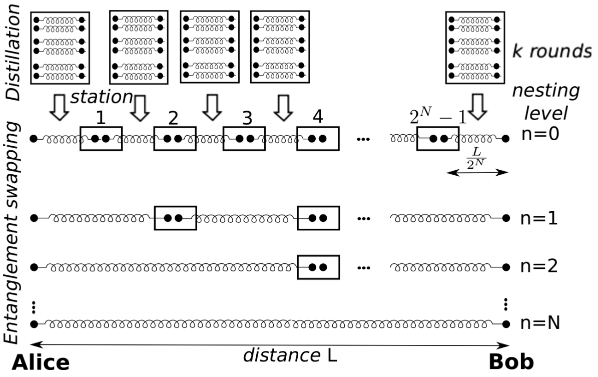


FIG. 1. Scheme of a generic quantum repeater protocol. We adopt the nested protocol proposed in [7]. The distance between Alice and Bob is L, which is divided in 2^N segments, each having the length $L_0 := L/2^N$. The parameter n describes the different nesting levels, and the value N represents the 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.

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 set-up 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 form of single- or multi-photon 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 will also be 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 sub-exponential, 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 post-processing, 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 will consider photon-number resolving detectors (PNRD) which can be described by a positive-operator valued measure (POVM) with elements [27]

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

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 e.g. described in [28]. In our analysis, we will characterize them using the gate quality which will be denoted by p_G (see Eq. (19) and Eq. (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 read-out. We discuss the role of η_m only for the quantum repeater with atomic ensembles (see section 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 multi-qubit 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), each performed on two qubits at the same repeater station, and projective measurements with post-selection.

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 i-th distillation round by $P_D[i]$.

We study entanglement distillation for the original quantum repeater protocol (section III) and the hybrid quantum repeater (section IV). For the quantum repeater with atomic ensembles (section 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 post-processing.

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 n-th 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 reference 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*

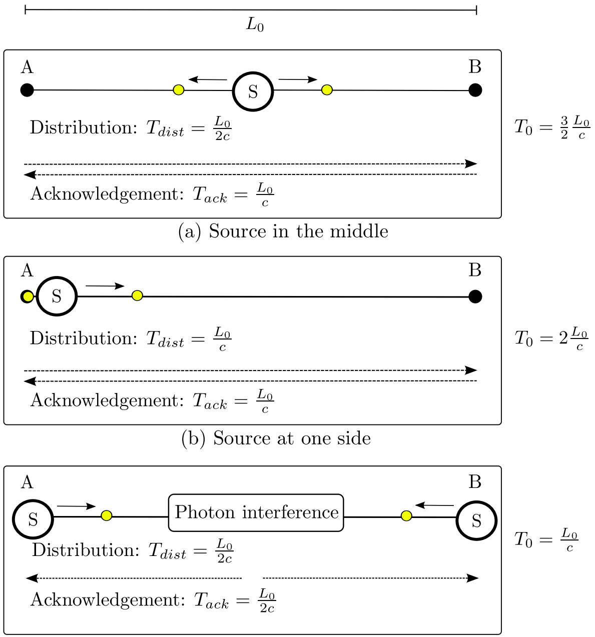
In order to evaluate the performance of a quantum repeater protocol it is necessary to assess how many entangled pairs across distance L can be generated per second.

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:

$$T_0 := \frac{\beta L_0}{c}, \qquad (3)$$

where $c = 2 \cdot 10^5$ 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 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 set-ups 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


L_0
A
B
S
Distribution: $T_{dist} = \frac{L_0}{2c}$
Acknowledgement: $T_{ack} = \frac{L_0}{c}$
$T_0 = \frac{3}{2}\frac{L_0}{c}$
Distribution: $T_{dist} = \frac{L_0}{c}$
Acknowledgement: $T_{ack} = \frac{L_0}{c}$
$T_0 = 2\frac{L_0}{c}$
Photon interference
Distribution: $T_{dist} = \frac{L_0}{2c}$
Acknowledgement: $T_{ack} = \frac{L_0}{2c}$
$T_0 = \frac{L_0}{c}$

(a) Source in the middle

(b) Source at one side

(c) Source at both sides

FIG. 2. 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]).

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]

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

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

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

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

We remind the reader that $P_D[i]$ is the success probability in the i-th 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 $P_0 << 1$, we find an upper bound on the entanglement generation rate:

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

with $a \leq \frac{2}{3} P_{L_0}[k] Z_1(P_{L_0}[k])$. Our derivation is given in App. A. For the plots we bound a according to the occuring 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.

B. Quantum key distribution (QKD)

The QKD protocol

In Fig. 3 a general quantum key distribution set-up 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 figure 3). The QKD protocol itself starts with Alice and Bob performing measurements on their shared, long-distance entangled pairs (see figure 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 post-processing 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].

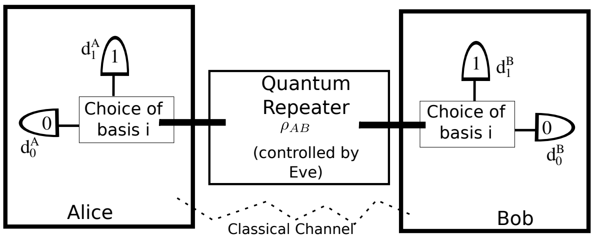


FIG. 3. Scheme of quantum key distribution. The state ρ_{AB} is produced using a quantum repeater. Alice and Bob locally rotate this state in a measurement basis and then they perform the measurement. The detectors are denoted by $d_0^A, d_1^A, d_0^B, d_1^B$ and to each detector click a classical outcome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

1. *The quantum bit error rate (QBER)*

In order to evaluate the performance of a QKD protocol, it is necessary to determine the quantum bit error rate. 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 modelled by means of four detectors (two on Alice's side and two on Bob's side, see figure 3) where to each detector click a classical binary outcome is assigned. Particular care is necessary when multi-photon states are measured [41, 42]. In the following, we give the definition of the QBER for the case of photon-number-resolving detectors 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

$$P_{jklm}^{(i)} := \mathrm{tr}\left(\Pi_{d_0^A}^{(j)}\Pi_{d_1^A}^{(k)}\Pi_{d_0^B}^{(l)}\Pi_{d_1^B}^{(m)}\rho_{AB}^{(i)}\right), \tag{9}$$

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 $\rho_{AB}^{(i)}$ 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]

$$P_{\text{click}}^{(i)} := P_{1010}^{(i)} + P_{0101}^{(i)} + P_{0110}^{(i)} + P_{1001}^{(i)}. \tag{10}$$

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

$$P_{\text{err}}^{(i)} := P_{0110}^{(i)} + P_{1001}^{(i)}. \tag{11}$$

Thus, the fraction of discordant bits, i.e., the quantum bit error rate for measurement basis i is [20]

$$e_i := \frac{P_{\text{err}}^{(i)}}{P_{\text{click}}^{(i)}}. \tag{12}$$

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 $P_{\text{click}}^{(i)} = \eta_{\text{d}}^2$ and $P_{\text{err}}^{(i)} \propto \eta_{\text{d}}^2$.

If we assume a genuine two-qubit system[1] like in the original quantum repeater proposal (see section III) or the hybrid quantum repeater (see section 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]

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

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

2. *The secret key rate*

The figure of merit representing the performance of quantum key distribution 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 will 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

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

where the sifting rate R_{sift} is the fraction of measurements performed in the same basis by Alice and Bob Throughout the whole paper we will use $R_{\text{sift}} = 1$ 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 will 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

[1] Note that the states of the DLCZ-type quantum repeaters (see section 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.

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 quantum bit error rate (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 only achievable for ideal implementations 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]

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

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 will 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 set-up. 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 set-up

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.,

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

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].

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

[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.

upon two qubits B and C can be modeled by

$$O_{BC}(\rho_{BC}) = p_G O_{BC}^{\mathrm{ideal}}(\rho_{BC}) + \frac{1-p_G}{4}\mathbf{1}_{BC}, \qquad (19)$$

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.

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 App. B 2, 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).

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 will 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.

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,

$$\begin{aligned} R_{\mathrm{QKD}}^{\mathrm{O}} =& R_{\mathrm{REP}}(L_0, N, k, F_0, p_G, \eta_{\mathrm{d}}) P_{\mathrm{click}}(\eta_{\mathrm{d}}) \\ & \times R_{\mathrm{sift}} r_\infty(N, k, F_0, p_G), \end{aligned} \qquad (20)$$

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 non-zero 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 non-zero 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 non-zero 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.

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 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.

Minimally required parameters In this paragraph, we will discuss the minimal requirements that are necessary to be able to extract a secret key, i.e., we will specify the parameter region where the secret fraction is non-zero. 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 App. B 2), and then we swap the distilled state $2^N - 1$ times (see the formulas in B 1). At the end, a generic Bell diagonal state is obtained. Using Eq. (13) one can then

[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 two-fold 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.

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

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.

calculate the QBER, which is sufficient to calculate the secret fraction.

Table I and Tab. 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).

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.

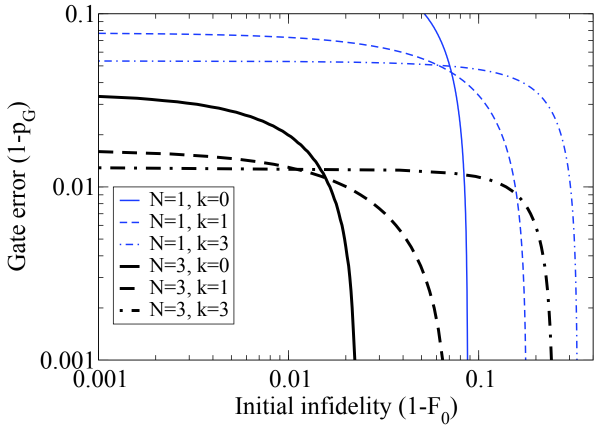


FIG. 4. (Color online) Original quantum repeater and the BB84-protocol: Maximal infidelity $(1-F_0)$ as a function of gate error $(1-p_G)$ permitting to extract a secret key for various maximal nesting levels N and numbers of distillation rounds k (Parameter: L = 600 km).

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

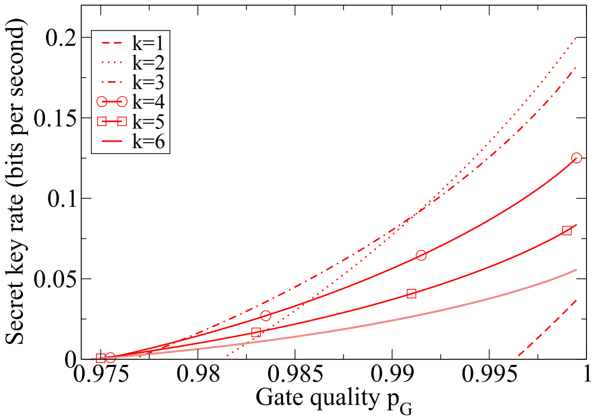


FIG. 5. (Color online) Original quantum repeater and the BB84-protocol: Secret key rate Eq. (20) versus gate quality p_G for different rounds of distillation k. The case $k = 0$ leads to a vanishing secret key rate. (Parameters: $F_0 = 0.9$, $N = 2$, L = 600 km)

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 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 permit to increase the secret key rate sufficiently much 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 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 $N = 5$.

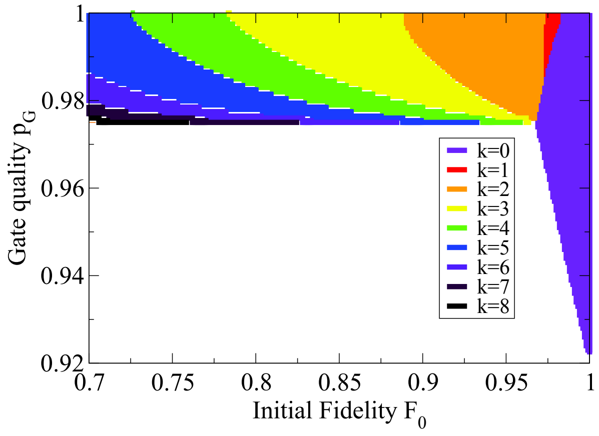


FIG. 6. (Color online) Original quantum repeater and the BB84-protocol: Number of distillation rounds k that maximizes the secret key rate as a function of gate quality p_G and initial fidelity F_0. In the white area, it is no longer possible to extract a secret key. (Parameters: $N = 2$, $L = 600$ km)

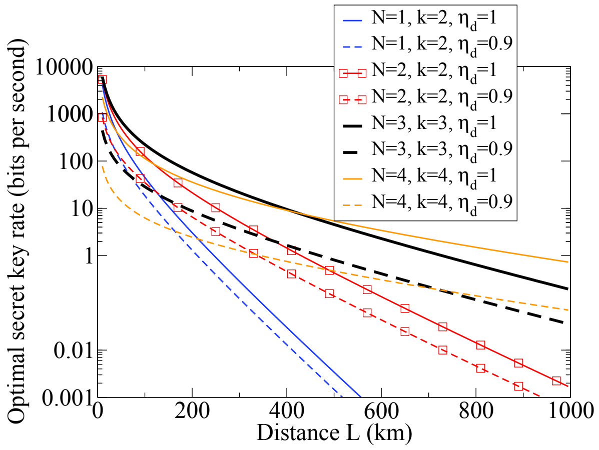


FIG. 7. (Color online) Original quantum repeater and the BB84-protocol: Optimal secret key rate Eq. (20) versus distance for different nesting levels, with and without perfect detectors. For each maximal nesting level N, we have chosen the optimal number of distillation rounds k. A nesting level $N \geq 5$ no longer permits to obtain a non-zero secret key rate. (Parameters: $F_0 = 0.9$ and $p_g = 0.995$.)

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

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

using Eq. (14) with the repeater rate $R_{\rm REP}$ given by Eq. (8). The term $\eta_{\rm d}^{2k}$ arises from the two-fold detections for the distillation, and similarly, $\eta_{\rm d}^{2N}$ comes from the entanglement swapping and $\eta_{\rm d}^{2}$ from the QKD measurements.

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 App. 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 will 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 shall 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 set-up

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 $U_{int}\left[|\alpha\rangle(|0\rangle + |1\rangle)/\sqrt{2}\right] = \left(\left|\alpha e^{-i\theta/2}\right\rangle|0\rangle + \left|\alpha e^{i\theta/2}\right\rangle|1\rangle\right)/\sqrt{2}$, 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 opti-

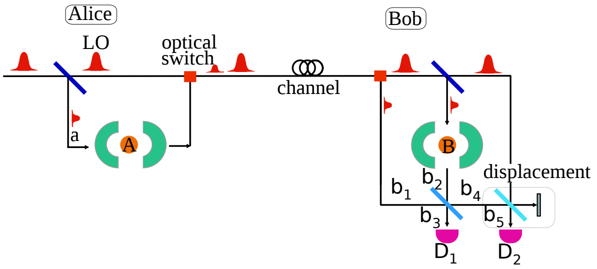


FIG. 8. (Color online) Schematic diagram for the entanglement generation by means of a USD measurement following [55]. The two quantum memories A and B are separated by a distance L_0. The part on the left side (an intermediate Alice) prepares a pulse in a coherent state $|\alpha\rangle_a$ (the subscript 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 $\left|\sqrt{\eta_t}\alpha\right\rangle_{b_1}$ and produces from the LO through beam splitting a second probe pulse $\left|\sqrt{\eta_t}\alpha\right\rangle_{b_2}$ 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 η_t (L_0) has been defined in Eq. (1).

cal elements and photon detectors are used for the unambiguous discrimination of the phase-rotated coherent states. Different from [55], however, we use imperfect photon-number-resolving detectors (PNRD), as described by Eq. (2), instead of threshold detectors. By performing such a USD measurement on the probe state, as illustrated in Fig. 8, the following entangled state can be conditionally prepared,

$$\rho_0 := F_0 \left|\phi^+\right\rangle\left\langle\phi^+\right| + (1-F_0)\left|\phi^-\right\rangle\left\langle\phi^-\right|, \tag{22}$$

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 section II A 2). Our derivation of the fidelity F_0 can be found in App. C 1. Note that the form of this state is different from the state considered in section 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, photon-number-resolving detectors. We explain our derivation of Eq. (23) in App. C 1[7].

Entanglement swapping

A two-qubit gate is essential to perform entanglement swapping and entanglement distillation. In the HQR a controlled-Z (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,

$$\begin{aligned} O_{BC}(\rho_{BC}) =& O_{BC}^{ideal}\Big(p_c^2(x)\rho_{BC} + \\ & p_c(x)(1-p_c(x))(Z^B\rho_{BC}Z^B + Z^C\rho_{BC}Z^C) \\ & +(1-p_c(x))^2 Z^B Z^C \rho_{BC} Z^C Z^B\Big), \end{aligned} \tag{24}$$

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 App. C 2.

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

[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 unambiguous state discrimination, 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].

[8] Note that this error model is considering a CZ gate operation. For a CNOT gate, Z errors can be transformed into X errors.

Bell diagonal state. The effect of gate errors in the distillation step is derived in App. C 3.[9]

B. Performance in the presence of imperfections

In the following, we will 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 hybrid quantum repeater 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 section 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 hybrid quantum repeater. 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 section 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 set-up adopted for these measurements, it should be multiplied by the square of the detector efficiency.

k N	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

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.

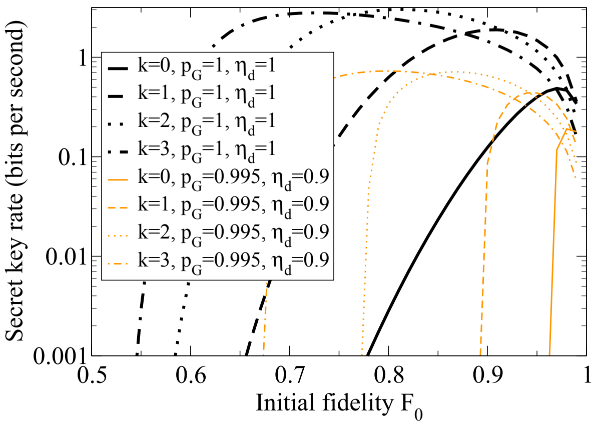


FIG. 9. (Color online) Hybrid quantum repeater with perfect quantum operations ($p_G = 1$) and perfect detectors ($\eta_d = 1$) (black lines) compared to imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_d = 0.9$) (orange lines): Secret key rate per second Eq. (26) as a function 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 hybrid quantum repeater 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 permit 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 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

[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).

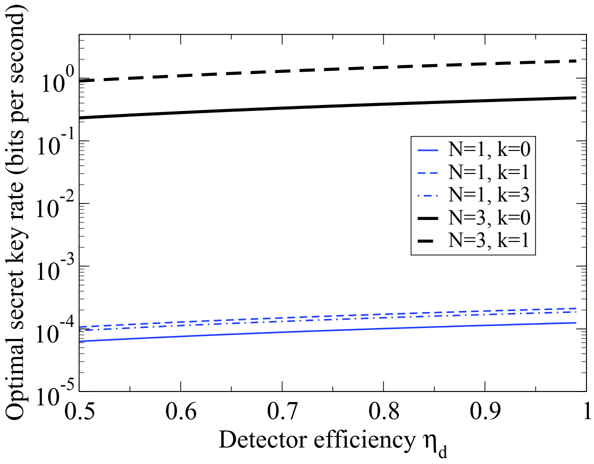


FIG. 10. (Color online) Hybrid quantum repeater with perfect gates ($p_G = 1$): The optimal secret key rate Eq. (26) for the BB84-protocol in terms of the detector efficiency η_d for the distance $L = 600$ km with various numbers of segments 2^N and rounds of distillation k.

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 hybrid quantum repeater, 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. 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 9 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 A. 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 non-zero 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.

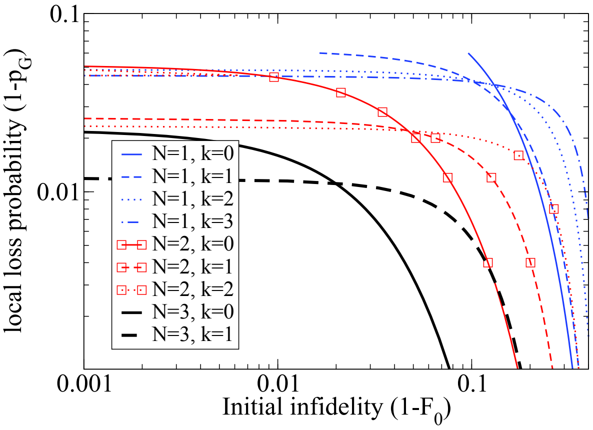


FIG. 11. (Color online) Hybrid quantum repeater with distillation and imperfections: Maximally allowed infidelity $(1 - F_0)$ as a function of the local loss probability $(1 - p_G)$ for various maximal numbers of segments 2^N and rounds of distillation k (distance: $L = 600$ km). Above the curves it is no longer possible to extract a secret key. The lines with $k = 0$ correspond to entanglement swapping without distillation.

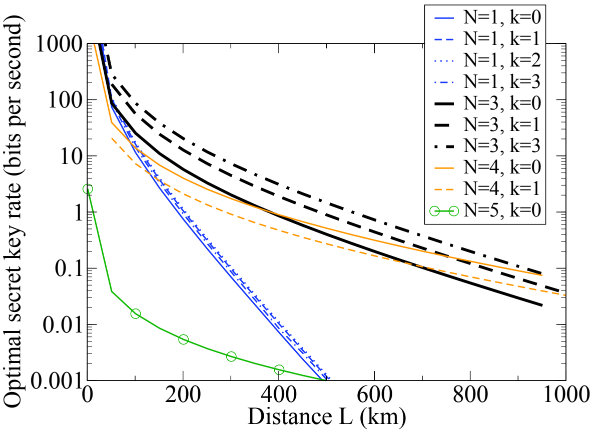


FIG. 12. (Color online) Hybrid quantum repeater with imperfect quantum operations ($p_G = 0.995$) and imperfect detectors ($\eta_d = 0.9$): Optimal secret key rate Eq. (26) for the BB84-protocol as a function of the total distance L, for various numbers of segments 2^N and rounds of distillation k. For $N = 5$, it is not possible to obtain a secret key when distillation is applied.

In figure 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, for example, for $N = 3$ and $N = 4$ at a distance of around 750 km.

V. QUANTUM REPEATERS BASED ON ATOMIC ENSEMBLES

The probably most influential proposal for a practical realization of quantum repeaters was made in [12] and it is known as the Duan-Lukin-Cirac-Zoller (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 set-up

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 [62] and [23])[11]

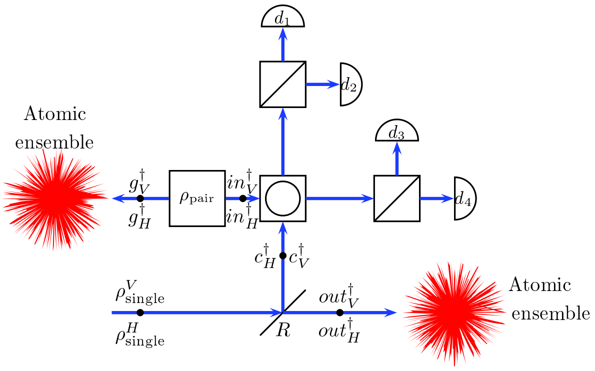


FIG. 13. Quantum repeater based on atomic ensembles: Set-up for creation of on-demand entanglement (see also [23]). The whole set-up is situated at one physical location. A pair source produces the state ρ_{pair}. One part of the pair (the mode g) is stored in an atomic ensemble and the other part (mode *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 ±45° (square with a circle inside), two polarizing beam splitters in the rectilinear basis (square with a diagonal line inside), and four detectors.

$$\rho_{\text{pair}} := (1-p)\sum_{m=0}^{\infty} \frac{2^m p^m}{(m!)^2(m+1)} (B^\dagger)^m \,|0\rangle\langle 0|\, B^m, \qquad (27)$$

where $B^\dagger := (g_H^\dagger in_H^\dagger + g_V^\dagger in_V^\dagger)/\sqrt{2}$. The operator $g_i^\dagger$ ($in_i^\dagger$) 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

$$\rho^i_{\text{single}} := (1-q)\,|0\rangle\langle 0| + q a_i^\dagger \,|0\rangle\langle 0|\, a_i, \qquad (28)$$

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.

On-demand entanglement source

The protocol that produces local entangled pairs works as follows (see Fig. 13 and [23] for additional details):

[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 post-processing [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 $m \leq 2$. 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.

1. The state $\rho_{\text{pair}} \otimes \rho^{H}_{\text{single}} \otimes \rho^{V}_{\text{single}}$ 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 $a_i \rightarrow \sqrt{R}\, c_i + \sqrt{1-R}\, out_i$.

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,

$$
\begin{aligned}
c_H &\rightarrow \frac{d_3 + d_4 + d_2 - d_1}{2},\\
c_V &\rightarrow \frac{d_3 + d_4 - d_2 + d_1}{2},\\
in_H &\rightarrow \frac{d_2 + d_1 + d_3 - d_4}{2},\\
in_V &\rightarrow \frac{d_2 + d_1 - d_3 + d_4}{2},
\end{aligned}
$$

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 quantum memories *out* and g.The probability of a successful measurement is given by

$$
P^s_0(p, q, R, \eta_{\text{d}}) = 4\text{tr}\left(\Pi^{(1)}_{d_1}(\eta_{\text{d}})\Pi^{(0)}_{d_2}(\eta_{\text{d}})\Pi^{(1)}_{d_3}(\eta_{\text{d}})\Pi^{(0)}_{d_4}(\eta_{\text{d}})\rho'_{g,out,d_1,d_2,d_3,d_4}\right), \tag{29}
$$

where $\rho'_{g,out,d_1,d_2,d_3,d_4}$ 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

$$
\rho^s_0(p, q, R, \eta_{\text{d}}) = \frac{4}{P^s_0}\text{tr}_{d_1,d_2,d_3,d_4}\left(\Pi^{(1)}_{d_1}(\eta_{\text{d}})\Pi^{(0)}_{d_2}(\eta_{\text{d}})\Pi^{(1)}_{d_3}(\eta_{\text{d}})\Pi^{(0)}_{d_4}(\eta_{\text{d}})\rho'_{g,out,d_1,d_2,d_3,d_4}\right). \tag{30}
$$

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 $\rho^s_0 = |\phi^+\rangle\langle\phi^+|$ which can be obtained with probability $P^s_0 = pR(1-R)$. In the realistic case, however, additional higher-order excitations are present. In [23], the explicit form of ρ^s_0 and P^s_0 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] permits 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.

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 shall 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^s_0. 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

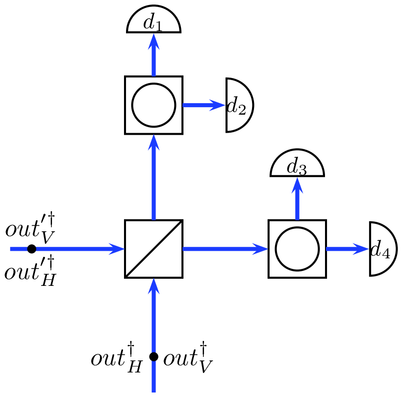


FIG. 14. Quantum repeater based on atomic ensembles: Set-up used for entanglement distribution (swapping) (see [23] for additional details). The modes *out* and *out'* are released from two quantum memories separated by distance L_0 (or located at the same station for the case of swapping) and sent into 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.

of the modes are as follows:

$$out_H \to \frac{d_3 + d_4}{\sqrt{2}}, \quad out_V \to \frac{d_1 - d_2}{\sqrt{2}},$$
$$out'_H \to \frac{d_1 + d_2}{\sqrt{2}}, \quad out'_V \to \frac{d_3 - d_4}{\sqrt{2}},$$

where $d_1,\ d_2,\ d_3,\ d_4$ 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

$$P_0(p,q,R,\eta_\mathrm{d},\eta_\mathrm{mtd}) = 4\mathrm{tr}\left(\Pi^{(1)}_{d_1}(\eta_{mtd})\Pi^{(0)}_{d_2}(\eta_{mtd})\Pi^{(1)}_{d_3}(\eta_{mtd})\Pi^{(0)}_{d_4}(\eta_{mtd})\rho'_{g,g',d_1,d_2,d_3,d_4}\right), \tag{31}$$

where $\rho'_{g,g',d_1,d_2,d_3,d_4}$ is the total state obtained at the end of step (ii) and $\eta_{mtd} := \eta_m\eta_t\left(\frac{L_0}{2}\right)\eta_\mathrm{d}$, 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

$$\rho_{0,g,g'} = \frac{4}{P_0}\mathrm{tr}_{d_1,d_2,d_3,d_4}\left(\Pi^{(1)}_{d_1}(\eta_{mtd})\Pi^{(0)}_{d_2}(\eta_{mtd})\Pi^{(1)}_{d_3}(\eta_{mtd})\Pi^{(0)}_{d_4}(\eta_{mtd})\rho'_{g,g',d_1,d_2,d_3,d_4}\right). \tag{32}$$

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

$$P^{(n)}_{ES}(p,q,R,\eta_\mathrm{d},\eta_\mathrm{mtd}) = 4\mathrm{tr}\left(\Pi^{(1)}_{d_1}(\eta_{md})\Pi^{(0)}_{d_2}(\eta_{md})\Pi^{(1)}_{d_3}(\eta_{md})\Pi^{(0)}_{d_4}(\eta_{md})\rho'_{n-1,g,g',d_1,d_2,d_3,d_4}\right), \tag{33}$$

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

$$\rho_{k,g,g'} = \frac{4}{P^{(i)}_{ES}}\mathrm{tr}_{d_1,d_2,d_3,d_4}\left(\Pi^{(1)}_{d_1}(\eta_{md})\Pi^{(0)}_{d_2}(\eta_{md})\Pi^{(1)}_{d_3}(\eta_{md})\Pi^{(0)}_{d_4}(\eta_{md})\rho'_{k-1,g,g',d_1,d_2,d_3,d_4}\right). \tag{34}$$

The state $\rho_{n,g,g'}$ is the state that will be used for quantum key distribution 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] it 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_0^s 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 2 and inserting η_{md} for the detector efficiency.

The final secret key rate then reads

$$R_{\mathrm{QKD}}^{\mathrm{AE}} = R_{\mathrm{REP}}(L_0, p, N, \eta_{\mathrm{d}}, \eta_m, \gamma_{\mathrm{rep}}, q) P_{\mathrm{click}}(L_0, p, N, \eta_{\mathrm{d}}, \eta_m, q) R_{\mathrm{sift}} r_{\infty}^{\mathrm{BB84}}(L_0, p, N, \eta_{\mathrm{d}}, \eta_m, q), \tag{35}$$

where R_{REP} is given by Eq. (8) with $\beta = 1$ for the communication time (see Fig. 2c). 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.

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_0^s, 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 $T_0^s = \frac{1}{\gamma_{\mathrm{rep}} P_0^s}$ [23]. The formula for the repeater rate in this case corresponds to Eq. (8) with $T_0 \to T_0 + T_0^s$. As shown in Fig. 16, when $\eta_{\mathrm{d}} = 1$ the secret key rate is constant for $\gamma_{rep} > 10^7$, however, for realistic detectors with $\eta_{\mathrm{d}} = 0.9$, 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 will employ $\gamma_{rep} = 50$ MHz.

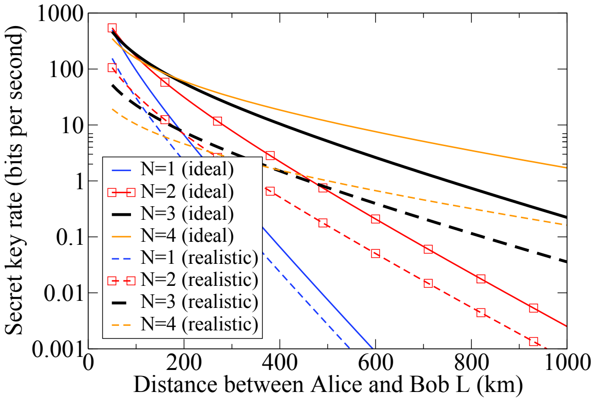


FIG. 15. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the distance between Alice and Bob. The secret key rate has been obtained by maximizing over p and R. Ideal set-up (solid line) with parameters $\eta_m = \eta_{\mathrm{d}} = q = 1, \gamma_{rep} = \infty$. More realistic set-up (dashed line) with parameters $\eta_m = 1$, $\eta_{\mathrm{d}} = 0.9$, $q = 0.96$, $\gamma_{rep} = 50$ MHz.

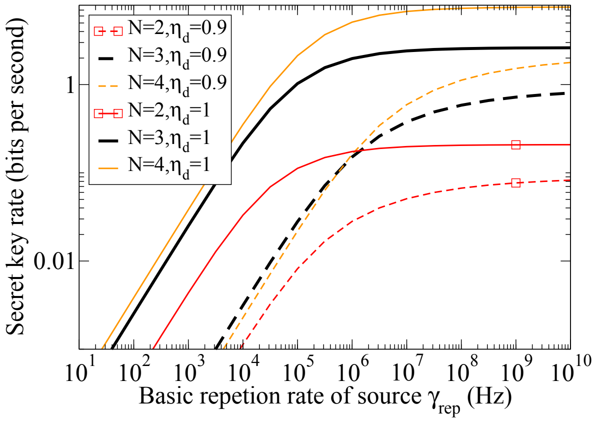


FIG. 16. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the basic repetition rate of the source γ_{rep}. The secret key rate has been obtained by maximizing over p and R. (Parameters: $\eta_{\mathrm{d}} = \eta_m = q = 1$).

A consequence of imperfect detectors is that multi-photon 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 permit 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 to [25], intrinsic quantum memory efficiencies above 80% have been realized [65]; however, total efficiencies where coupling losses are included are much lower.

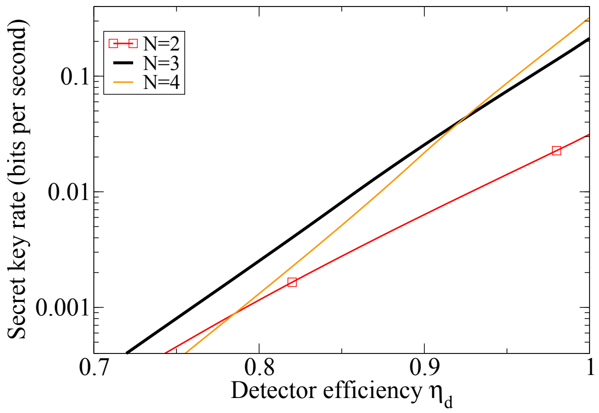


FIG. 17. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the efficiency of the detectors $\eta_{\rm d}$. The secret key rate has been obtained by maximizing over p and R. (Parameters: $\eta_m = q = 1$, $\gamma_{\rm rep} = 50$ MHz, $L = 600$ km).

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 set-up 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 $N = 4$, the secret key rate scales proportionally to $\eta_{\rm d}^2\eta_{\rm d}^2\eta_{\rm d}^{2\cdot 4}\eta_{\rm d}^2$ (local creation, distribution, entanglement swapping, and QKD measurement). For $\eta_{\rm d} = 0.9$, 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.

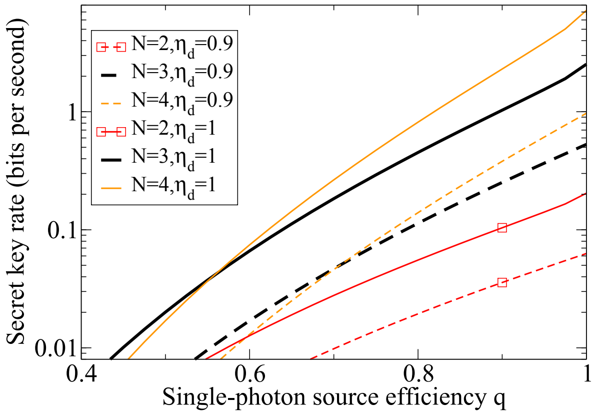


FIG. 18. (Color online) Quantum repeaters based on atomic ensembles: Optimal secret key rate per second versus the probability to emit a single photon. The secret key rate has been obtained by maximizing over p and R. (Parameters: $\eta_m = 1, \gamma_{rep} = 50$ MHz, $L = 600$ km).

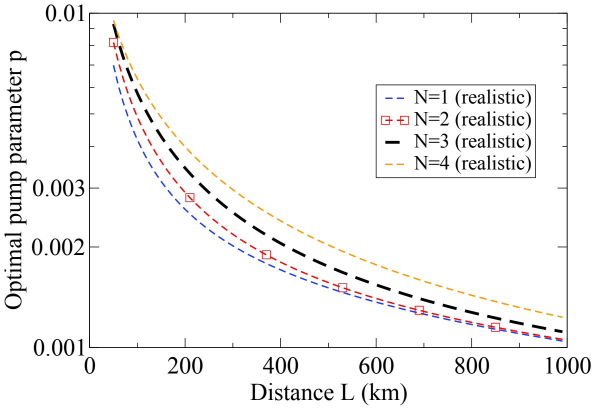


FIG. 19. (Color online) Quantum repeaters based on atomic ensembles: Optimal value of p versus the distance between Alice and Bob. The corresponding secret key rate is shown in Fig. 15. (Parameters: $\eta_m = 1, \eta_D = 0.9, q = 0.96, \gamma_{rep} = 50$ MHz, $L = 600$ km)

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 (QKD) 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

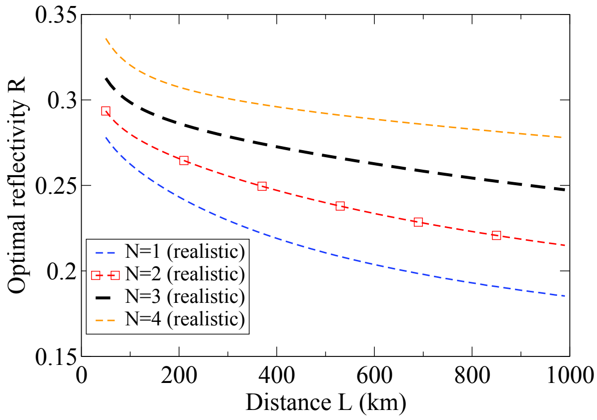


FIG. 20. (Color online) Quantum repeaters based on atomic ensembles: Optimal value of the reflectivity R versus the distance between Alice and Bob. The corresponding secret key rate is shown in Fig. 15. (Parameters: $\eta_m = 1$, $\eta_D = 0.9$, $q = 0.96$, $\gamma_{rep} = 50$ MHz)

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 hybrid quantum repeater, 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 non-trivial, 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 allows 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 hybrid quantum repeater. This protocol permits 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 photon-number resolving detectors, 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 permits to have high secret key rates in a set-up 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 two-fold 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 set-up. 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 hybrid quantum repeater 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 quantum key distribution, 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 in 2011 and 2012. 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 A 2 which describes the generation rate of entangled pairs per time unit T_0 with probabilistic entanglement swapping and distillation, i.e.,

$$R_{\rm REP}^{\rm prob} = \frac{1}{T_0}\left(\frac{2}{3a}\right)^{N+k} P_0 P_{ES}^{(1)} P_{ES}^{(2)} ... P_{ES}^{(N)} \prod_{i=1}^{k} P_D[i]. \qquad \text{(A1)}$$

In [25] the formula has been derived only for the case without distillation and there it reads as follows,

$$R_{\rm REP}^{\rm prob} = \frac{1}{T_0}\left(\frac{2}{3}\right)^{N} P_0 P_{ES}^{(1)} P_{ES}^{(2)} ... P_{ES}^{(N)}, \qquad \text{(A2)}$$

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 $Z_1(x) = \frac{3-2x}{x(2-x)} \geq \frac{3}{2x}a$, we can rewrite $P_{L_0}[k]$:

$$\begin{aligned} P_{L_0}[k] &= \frac{P_D[k]}{Z_1(P_{L_0}[k-1])} \leq \frac{2}{3a} P_D[k] P_{L_0}[k-1] \\ &= \frac{2}{3a} P_D[k] \frac{P_D[k-1]}{Z_1(P_{L_0}[k-2])} \\ &\leq ... \leq \left(\frac{2}{3a}\right)^{k} P_0 \prod_{i=1}^{k} P_D[i], \end{aligned} \qquad \text{(A3)}$$

where in the last line $P_{L_0}[k]$ is a recursive formula. For deriving Eq. (A1), we replace in Eq. (A2) P_0 by 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 $P_{L_0}[k] \leq 0.037$ and $a \leq 0.994$.

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.

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.

Formulas in the presence of imperfections

We consider a set-up 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 $d_1 = \text{click}, d_2 = \text{noclick} \Rightarrow |H\rangle = \left|1_{d_1}, 0_{d_2}\right\rangle$ and $d_1 = \text{noclick}, d_2 = \text{click} \Rightarrow |V\rangle = \left|0_{d_1}, 1_{d_2}\right\rangle$ 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 $|H\rangle$ ($|V\rangle$):

$$\Pi_H := \gamma |H\rangle \langle H| + (1-\gamma) |V\rangle \langle V|, \qquad \text{(B1)}$$

$$\Pi_V := \gamma |V\rangle \langle V| + (1-\gamma) |H\rangle \langle H|, \qquad \text{(B2)}$$

with

$$\gamma := \frac{\eta_{\rm d} + p_{\rm dark}(1-\eta_{\rm d})}{\eta_{\rm d} + 2p_{\rm dark}(1-\eta_{\rm d})}, \qquad \text{(B3)}$$

[12] Note that this step is different from [7], where the single-qubit rotations were explicitly included.

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.

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]:

$$\begin{aligned}
A' &= \frac{1-p_G}{4} + p_G\left[\gamma^2(A^2+B^2+C^2+D^2) + 2(1-\gamma)^2(AD+BC) + 2\gamma(1-\gamma)(A+D)(C+B)\right],\\
B' &= \frac{1-p_G}{4} + p_G\left[2\gamma^2(AB+CD) + 2(1-\gamma)^2(AC+BD) + \gamma(1-\gamma)(A^2+B^2+C^2+D^2+2AD+2BC)\right],\\
C' &= \frac{1-p_G}{4} + p_G\left[2\gamma^2(AC+BD) + 2(1-\gamma)^2(AB+CD) + \gamma(1-\gamma)(A^2+B^2+C^2+D^2+2AD+2BC)\right],\\
D' &= \frac{1-p_G}{4} + p_G\left[2\gamma^2(AD+BC) + (1-\gamma)^2(A^2+B^2+C^2+D^2) + 2\gamma(1-\gamma)(A+D)(B+C)\right],
\end{aligned} \tag{B4}$$

and the probability to obtain the state above is equal to

$$P_{ES}(\eta_{\mathrm{d}}, p_{\mathrm{dark}}) := ((1-p_{\mathrm{dark}})(\eta_{\mathrm{d}} + 2p_{\mathrm{dark}}(1-\eta_{\mathrm{d}})))^2\,, \tag{B5}$$

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 $p_{\mathrm{dark}} < 10^{-5}$, 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_{dark} represents the probability that in the involved time window the detector gets a dark count.

2. Distillation

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 the following:

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.

Formulas in the presence of imperfections

Given a Bell diagonal state with the following coefficients

$$\rho_{ab} = A\left|\phi^+\right\rangle\left\langle\phi^+\right| + B\left|\phi^-\right\rangle\left\langle\phi^-\right| + C\left|\psi^+\right\rangle\left\langle\psi^+\right| + D\left|\psi^-\right\rangle\left\langle\psi^-\right|, \tag{B6}$$

the coefficients transform according to the following map [30]:

$$A' = \frac{1}{P_D}\left(A^2 + D^2\right), \tag{B7}$$

$$B' = \frac{1}{P_D}(2AD)\,, \tag{B8}$$

$$C' = \frac{1}{P_D}\left(B^2 + C^2\right), \tag{B9}$$

$$D' = \frac{1}{P_D}(2BC)\,, \tag{B10}$$

[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 no click

$$E^{(\mathrm{noclick})} = (1-p_{\mathrm{dark}})\,|0\rangle\langle 0| + (1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}})\,|1\rangle\langle 1|\,.$$

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:

$$\begin{aligned}
&E_a^{(\mathrm{click})} \otimes E_b^{(\mathrm{noclick})}\\
&= (1-(1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}}))\,(1-p_{\mathrm{dark}})\,|1_a, 0_b\rangle\langle 1_a, 0_b|\\
&+ p_{\mathrm{dark}}(1-p_{\mathrm{dark}})(1-\eta_{\mathrm{d}})\,|0_a, 1_b\rangle\langle 0_a, 1_b|\,.
\end{aligned}$$

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.

[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 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]:

$$P_D[k] = \frac{1}{2}\left\{1 + p_G^2 (-1 + 2A_{k-1} + 2D_{k-1})^2\right\}. \tag{B12}$$

with

$$\begin{aligned}
A' &= \left[1 + p_G^2 \left((A - B - C + D)(3A + B + C + 3D) + 4(A - D)^2\right)\right]/(8P_D),\\
B' &= \left[1 - p_G^2 \left(A^2 + 2A(B + C - 7D) + (B + C + D)^2\right)\right]/(8P_D),\\
C' &= \left[1 + p_G^2 \left(4(B - C)^2 - (A - B - C + D)(A + 3(B + C) + D)\right)\right]/(8P_D),\\
D' &= \left[1 - p_G^2 \left(A^2 + 2A(B + C + D) + B^2 + 2B(D - 7C) + (C + D)^2\right)\right]/(8P_D).
\end{aligned}$$

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]

$$\begin{aligned}
\rho_{AB,b_3,b_5} = \; & p\left\{\left[|0\rangle_{b_3} (|00\rangle_{AB} |\beta\rangle_{b_5} + |11\rangle_{AB} |-\beta\rangle_{b_5})/2 + |0\rangle_{b_5} (|01\rangle_{AB} |-\beta\rangle_{b_3} + |10\rangle_{AB} |\beta\rangle_{b_3})/2\right] \times H.c.\right\} +\\
& (1 - p)\left\{\left[|0\rangle_{b_3} (|00\rangle_{AB} |\beta\rangle_{b_5} - |11\rangle_{AB} |-\beta\rangle_{b_5})/2 + |0\rangle_{b_5} (|01\rangle_{AB} |-\beta\rangle_{b_3} - |10\rangle_{AB} |\beta\rangle_{b_3})/2\right] \times H.c.\right\},
\end{aligned} \tag{C1}$$

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 figure 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

$$\rho_{AB} = \frac{\mathrm{tr}_{b_3 b_5}(\Pi^{(0)}_{b_3}\Pi^{(n)}_{b_5}\rho_{AB,b_3,b_5})}{\mathrm{tr}(\Pi^{(0)}_{b_3}\Pi^{(n)}_{b_5}\rho_{AB,b_3,b_5})}, \tag{C2}$$

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

$$\rho = F_0 \left|\phi^+\right\rangle\left\langle\phi^+\right| + (1 - F_0)\left|\phi^-\right\rangle\left\langle\phi^-\right|,$$

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

$$P_0 = \sum_{n=1}^{\infty} \mathrm{tr}(\Pi^{(0)}_{b_3}\Pi^{(n)}_{b_5}\rho_{AB,b_3,b_5} + \Pi^{(0)}_{b_5}\Pi^{(n)}_{b_3}\rho_{AB,b_3,b_5}). \tag{C4}$$

Combining Eq. (C1) and Eq. (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:

$$
\begin{aligned}
A' &= 2BC + 2AD + 2[-2BC + A(B + C - 2D) + (B + C)D]p_G + (A - B - C + D)^2 p_G^2,\\
B' &= 2AC + 2BD + [A^2 + (B + C)^2 - 4BD + D^2 + 2A(-2C + D)]p_G - (A - B - C + D)^2 p_G^2,\\
C' &= 2AB + 2CD + [A^2 + (B + C)^2 - 4CD + D^2 + 2A(-2B + D)]p_G - (A - B - C + D)^2 p_G^2,\\
D' &= A^2 + B^2 + C^2 + D^2 - 2[A^2 + B^2 + C^2 - A(B + C) - (B + C)D + D^2]p_G + (A - B - C + D)^2 p_G^2.
\end{aligned} \tag{C5}
$$

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

$$
\begin{aligned}
A' &= \frac{1}{P_D}\Big(D^2 + A^2[1 + 2(-1 + p_G)p_G]^2 - 2A(-1 + p_G)p_G[C + 2D + 2(B - C - 2D)p_G + 2(-B + C + 2D)p_G^2]\\
&\quad -2D(-1 + p_G)p_G\{-2D - 2(C + D)(-1 + p_G)p_G + B[1 + 2(-1 + p_G)p_G]\}\Big),\\
B' &= \frac{1}{P_D}\Big[-2\big(D(-1 + p_G)p_G(C + D + 2Bp_G - 2Cp_G - 2Dp_G - 2Bp_G^2 + 2Cp_G^2 + 2Dp_G^2)A^2 p_G(-1 + 3p_G - 4p_G^2 + 2p_G^3)\\
&\quad -A\{D(1 - 2p_G + 2p_G^2)^2 - (-1 + p_G)p_G[-2C(-1 + p_G)p_G + B(1 - 2p_G + 2p_G^2)]\}\big)\Big],\\
C' &= \frac{1}{P_D}\Big(B^2(1 - 2p_G + 2p_G^2)^2 - 2B(-1 + p_G)p_G[-2A(-1 + p_G)p_G + D(1 - 2p_G + 2p_G^2) + C(2 - 4p_G + 4p_G^2)]\\
&\quad +C\{C(1 - 2p_G + 2p_G^2)^2 - 2(-1 + p_G)p_G[-2D(-1 + p_G)p_G + A(1 - 2p_G + 2p_G^2)]\}\Big),\\
D' &= \frac{1}{P_D}\Big\{-2(C(-1 + p_G)p_G(C + D + 2Ap_G - 2Cp_G - 2Dp_G - 2Ap_G^2 + 2Cp_G^2 + 2Dp_G^2) + B^2 p_G(-1 + 3p_G - 4p_G^2 + 2p_G^3)\\
&\quad -B\{C(1 - 2p_G + 2p_G^2)^2 - (-1 + p_G)p_G[-2D(-1 + p_G)p_G + A(1 - 2p_G + 2p_G^2)]\})\Big\},
\end{aligned} \tag{C6}
$$

P_D is the distillation probability of success and is given by

$$
\begin{aligned}
P_D =&(B + C)^2 + (A + D)^2 - 2(A - B - C + D)^2 p_G\\
&+2(A - B - C + D)^2 p_G^2.
\end{aligned} \tag{C7}
$$

For the case of $p_G = 1$, Eq. (C6) and Eq. (C7) are in accordance with [30].

[1] A. 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. Optic. **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 **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)* (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 e-prints (2012), arXiv:1210.8042 [quant-ph].

[22] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, Phys. Rev. A **76**, 050301 (2007), arXiv:0706.1924 [quant-ph].

[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. Tatarskiĭ, *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. Langford, and M. Nielsen, Physical Review A **71**, 062310 (2005).

[29] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young, The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics **58**, 1 (2010), 10.1140/epjd/e2010-00103-y.

[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. Horne, and A. 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*, Vol. 175 (Bangalore, India, 1984).

[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] C.-H. F. 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. Collins, S. Jenkins, A. Kuzmich, and T. Kennedy, Physical Review Letters **98**, 060502 (2007).

[47] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Theory of Cryptography*, Lecture Notes in Computer Science, Vol. 3378, edited by J. Kilian (Springer Berlin / Heidelberg, 2005) pp. 386–406.

[48] R. Renner and R. König, in *Theory of Cryptography Conference (TCC)*, Vol. 3378 (Springer, 2005) 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, Inc., 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. 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, in *AIP Conference Proceedings*, Vol. 1110 (2009) p. 155.

[59] J. Fiurasek and N. J. Cerf, ArXiv e-prints (2012), arXiv:1205.6933 [quant-ph].

[60] N. Walk, T. Symul, P. K. Lam, and T. C. Ralph, ArXiv e-prints (2012), arXiv:1206.0936 [quant-ph].

[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, Nature 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, Proceedings of the National Academy of Sciences **104**, 17291 (2007).

[69] R. Van Meter, T. Ladd, W. Munro, and K. Nemoto, Networking, IEEE/ACM Transactions on **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. V. 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**, 169–181 (1999).

[74] W. Dür, *Quantum communication over long distances using quantum repeaters*, Diplomarbeit, Leopold-Franzens-Universität Innsbruck, Innsbruck (1998).

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

Journal: Physical Review A
Impact Factor 2012: 3.042
Contribution: second author. I gave key ideas for the creation of the formulas for the repeater rate, suggested to perform the analysis in sec. IV.C, help with numerical calculations.
Percentage of my work: 5%.

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

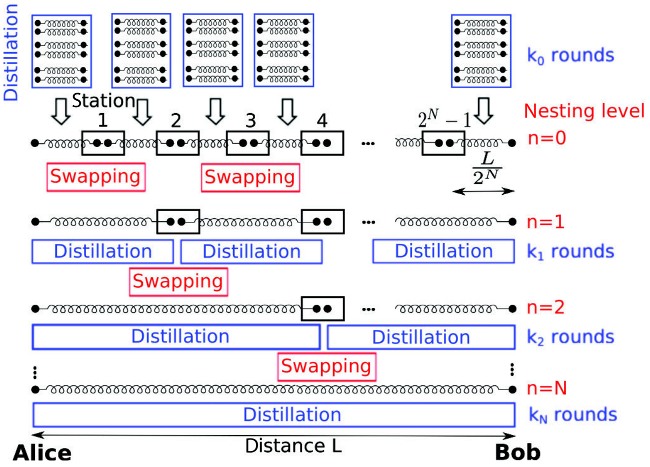


FIG. 1. (Color online) A generic quantum repeater protocol with nested distillation (see text).

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.

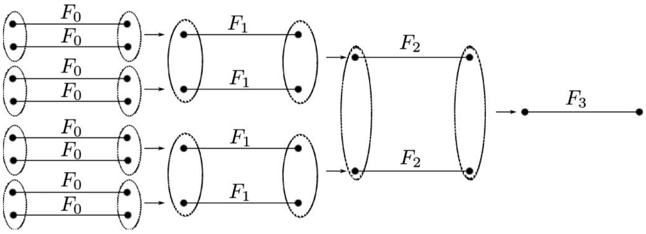


FIG. 2. Recurrence protocol: The *Deutsch et al.* protocol (figure adapted from Ref. [3]). The fidelity F_k is the fidelity in the kth distillation round.

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.

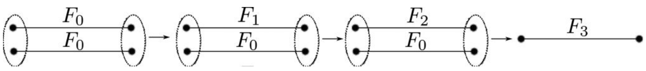


FIG. 3. Entanglement pumping: *Dür et al.* protocol (figure adapted from Ref. [3]).

[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.

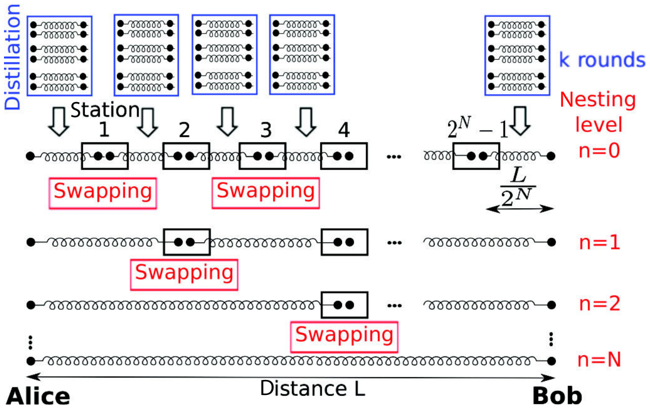


FIG. 4. (Color online) *Distillation strategy* β: distillation only in the beginning.

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 C1, 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,

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

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],

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

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

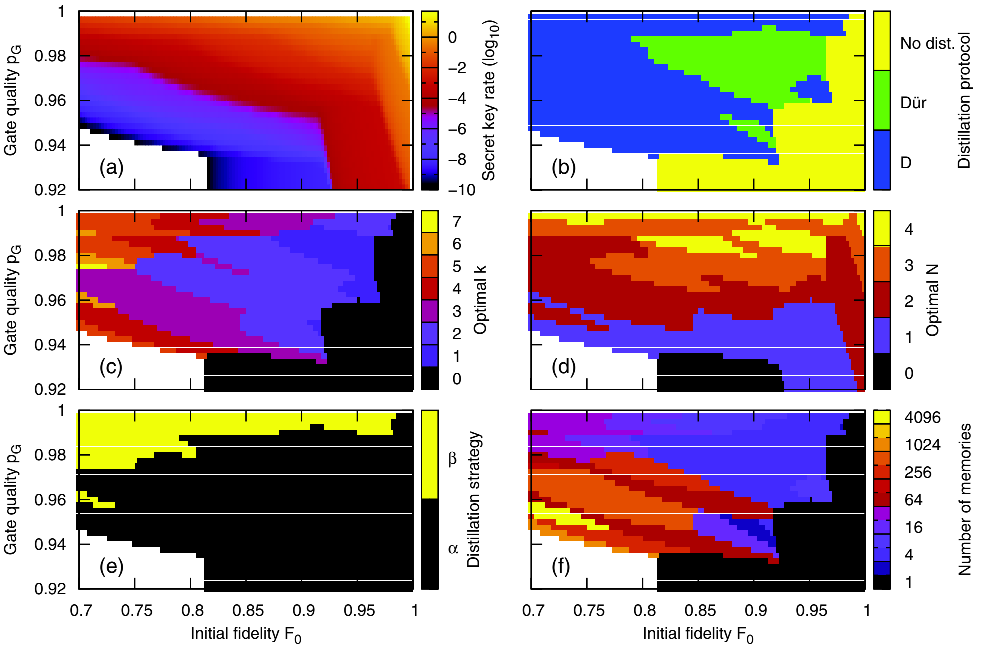


FIG. 5. (Color online) (a) Optimal secret key rate per memory per second (bits per second) [Eq. (4)] for the distance $L = 600$ km. The smallest secret key rate still depicted is chosen to be 10^{-10} secret bits per second per memory. In the white region, an extraction of a nonzero secret key rate is 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

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

where the set $|\{k_i\colon k_i = 0\}|$ 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

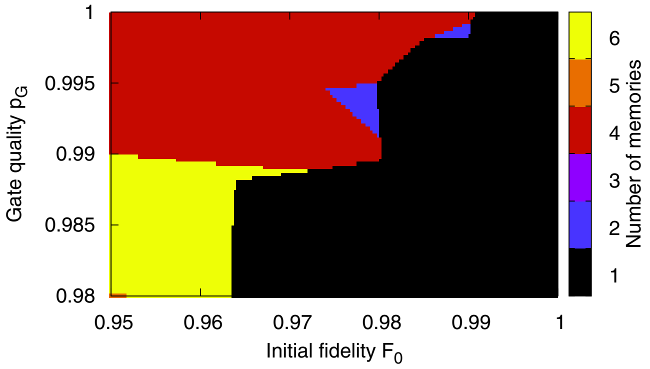


FIG. 6. (Color online) Expanded region from Fig. 5(f): Number of memories that lead to the optimal secret key rate per second per memory [see Eq. (4), $L = 600$ km].

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

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

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 $P_{\text{ES}}(n)$ in the equations for the repeater rate [Eqs. (6) and (9)] by

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

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

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.

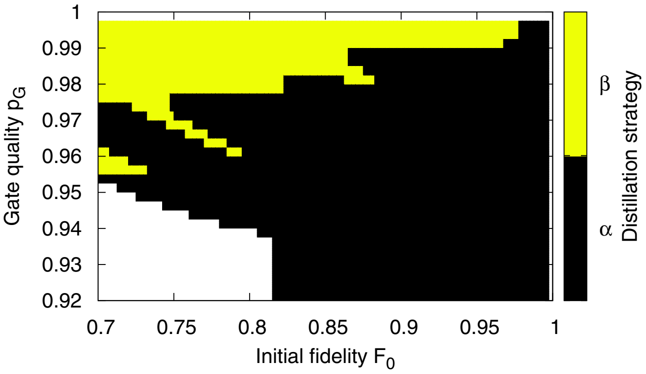


FIG. 7. (Color online) Distillation strategies with imperfect detectors: strategy α (nested distillation strategy) and strategy β (distillation only before the first entanglement swapping) that lead to the optimal secret key rate per memory per second [Eq. (4), $L = 600$ km and $\eta_d = 0.9$].

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 $\vec{k} = (2,0,0,0)$ 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.

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)

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., $m K_m = r_\infty R_{\text{Rep}}$. 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 $\vec{k}_M = (k_0,\dots,k_N)$ 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 $R_{\text{Rep,NC}}$ where we only consider the classical communication for entanglement distribution. Then, we compare the optimal secret key rates using the repeater rate without ($R_{\text{Rep,NC}}$) 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])

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

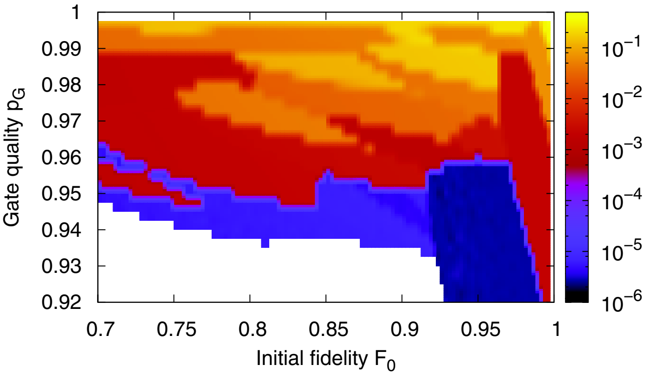


FIG. 8. (Color online) The relative change [Eq. (20)] in the optimal secret key rate per memory per second [Eq. (4)] without and with the classical communication time (see text) in terms of the initial fidelity F_0 and gate quality p_G ($L = 600$ km).

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

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

where

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

and $P_{\text{ES}}(0) = 1$ (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 $K(R_{\text{Rep}})$ and without classical communication $K(R_{\text{Rep,NC}})$, i.e.,

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

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

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

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 $K(R_{\text{Rep,NC}})$, 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 $k_N = 0$,

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

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 $\tau^{\mathrm{D}}(k_0,0)$,

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

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

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

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

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

The solution of this relation is

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

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

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

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

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

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

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

The repeater rate is given by

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

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

[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).

Measurement-device independent quantum key distribution with quantum memories.
S. Abruzzo, H. Kampermann, and D. Bruß.
ArXiv: 1306.3095, 2013. (submitted to Phys. Rev.A)

Journal: Submitted to Physical Review A
Impact Factor 2012: 3.042
Contribution: first author, idea to perform the analysis, scientific work and preparation of the manuscript.
Percentage of my work: 90%.

Measurement-device-independent quantum key distribution with quantum memories

Silvestre Abruzzo, Hermann Kampermann, Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany

We generalize measurement-device-independent quantum key distribution [H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012)] to the scenario where the Bell-state measurement station contains also heralded quantum memories. We find analytical formulas, in terms of device imperfections, for all quantities entering in the secret key rates, i.e., the quantum bit error rate and the repeater rate. We assume either single-photon sources or weak coherent pulse sources plus decoy states. We show that it is possible to significantly outperform the original proposal, even in presence of decoherence of the quantum memory. Our protocol may represent the first natural step for implementing a two-segment quantum repeater.

I. INTRODUCTION

Quantum communication has been developed in the last thirty years. One prominent communication protocol is quantum key distribution (QKD) which aims at distributing a secret key between two distant parties. Suitable quantum systems for quantum communication are photons as they have very low decoherence and they can be easily generated, distributed and detected with standard technology. However, due to absorption in optical fibers (or free-space), QKD with reasonable rates is only possible up to ca. 150 km [1]. To overcome this problem quantum repeaters have been developed [2]. The idea is to divide the distance between Alice and Bob in segments, to create entanglement in each segment and then to enlarge the distance using entanglement swapping. Nowadays, the constituting parts of a quantum repeater have been realized and small networks have been implemented in a laboratory set-up [3]. However, a complete quantum repeater (even with two segments) that will permit to outperform direct transmission has not been realized yet [4].

Recently, measurement-device-independent QKD (MDI-QKD-RELAY) has been proposed [5, 6]. This protocol is based on the principle of a quantum relay [7] and uses weak coherent pulse (WCP) sources. Briefly speaking, two parties, Alice and Bob, each equipped with a WCP source, send photon pulses to a station which performs a Bell-state measurement (BSM) and communicates the result to Alice and Bob. Then Alice sends Bob information regarding the used basis such that if necessary Bob can implement a bit flip. This protocol is measurement-device-independent because Alice and Bob do not need to measure anything and therefore the protocol is immune to detector attacks [8, 9]. The MDI-QKD-RELAY has already been implemented experimentally both in laboratory environment and in a real-world environment [10–12]. Moreover, more efficient protocols have already been proposed [13–15] and finite-size corrections have been analyzed [15–17].

In this paper we extend the original MDI-QKD-RELAY protocol [5] introducing quantum memories in the BSM station. The first consequence is that heralding, provided by quantum memories, permits to improve the rate at a given distance where MDI-QKD can be used. The advantage of our protocol over other quantum repeater protocols is that it does not need entanglement sources but only commercial off-the-shelf weak coherent pulse sources. Quantum memories have not reached the commercial market yet but they are under active development. With our protocol we show that it is possible to use quantum memories with low coherence time.

The manuscript is organized as follows. In Sec. II we present a generalization of measurement-device-independent QKD with single-photon sources to the scenario with quantum memories. We derive the formula for the secret key rate and we study its dependency on the decoherence of the quantum memories. Finally, we compare the secret key rate obtained with our protocol with the one obtained with the quantum relay proposed in [5]. In Sec. III we generalize the whole analysis to WCP sources. In order to calculate the secret key rate we consider QKD with decoy states [18, 19]. In Sec. IV we give our conclusions.

II. SCHEME WITH SINGLE-PHOTON STATES

In this section we extend the MDI-QKD-RELAY protocol presented in [5] introducing quantum memories (QM) and using single-photon-sources (SPS), which would be the ideal type of source for this protocol. Therefore, although SPSs are still not practical they will permit to establish upper bounds on the achievable secret key rate, i.e. sources with many-photon pulses or with additional imperfections will lead to a worse secret key rates. We denote the protocol considered in this section as MDI-QKD-REPEATER-SPS .

A. The protocol

In the following we give the steps of the protocol which is a generalization of the one proposed in [5] (see Fig. 1):

1. Alice and Bob prepare randomly and independently one of the four qubit states $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ where $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$. We

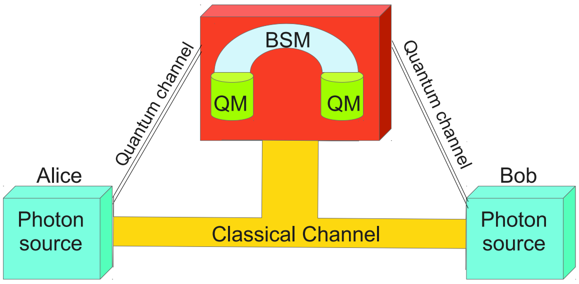


FIG. 1. (Color online) Scheme of a measurement-device-independent quantum repeater. The difference w.r.t. MDI-QKD-RELAY is that quantum memories are used. QM=quantum memories, BSM=Bell-state measurement. The two sources produce single-photon states or weak coherent pulses.

will refer to the set $\{|0\rangle, |1\rangle\}$ as the Z-basis (or rectilinear basis) and the set $\{|+\rangle, |-\rangle\}$ as the X-basis (or diagonal basis). The states are sent through the quantum channel to the repeater station. The information related to the created states is stored by Alice and Bob locally. This process is repeated continuously by Alice and Bob with frequency ν_s which is the repetition frequency of the source.

2. When both quantum memories are filled up, the quantum memories are read and a Bell-state measurement (BSM) is performed. The result of the BSM and the fact that the measurement was successful are sent to both Alice and Bob.
3. If the measurement was successful Alice and Bob will keep their stored information and if needed one of the two parties will perform a bit flip. If the measurement was not successful then Alice and Bob will remove their classical information from their stored pool of data.
4. After creating sufficiently many bits Alice and Bob do the usual QKD post-processing which consists of sifting, parameter estimation, error correction and privacy amplification [1].

The second step is different from the original MDI-QKD-RELAY protocol. Here quantum memories are used for increasing the entanglement swapping success probability. As a result the total secret key rate will be higher than for the case without quantum memories.

B. The secret key rate

Concerning the security, the protocol is equivalent to the entanglement-based repeater protocol [1] [5, 20, 21]. In this paper we consider the asymptotic secret key rate which gives an upper bound on the achievable secret key rate. Finite size corrections can be included using the analysis done in [16, 17]. The formula for the asymptotic secret key rate is given in [1, 5]

$$r_\infty^{\mathrm{REP}} := \frac{1}{<T>}(1 - h(e_Z) - h(e_X)), \qquad (1)$$

where $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy, $e_X(e_Z)$ is the quantum bit error rate (QBER) in the X-basis (Z-basis) and $\frac{1}{<T>}$ is the raw key rate[2]. The QBER represents the fraction of discordant bits in the raw key, which is the collection of bits stored by Alice and Bob before the post-processing.

We give now an analytical expression for the raw key rate. We denote by P_0 the probability that the quantum state sent by Alice (Bob) is stored in the quantum memory[3]. One knows that this event has happened because the quantum memories are supposed to be heralded. In the following we will measure the time in units of $\Delta t := \nu_s^{-1}$ which represents the time that the quantum memory has to wait between two attempts. We introduce the probability $P(k_A, k_B)$ that the photons of Alice AND Bob are stored at time-bin k_A and k_B and they where not stored before, i.e.

$$P(k_A, k_B) := P_0^2(1-P_0)^{k_A-1}(1-P_0)^{k_B-1}. \qquad (2)$$

The average number of attempts by the source necessary

[1] The equivalence is seen by the following arguments: consider an entanglement-based repeater protocol where Alice and Bob each produce the state $|\phi^+\rangle_{AC} = |\phi^+\rangle_{DB} := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The subsystems C and D are sent to the channel and subjected to a BSM. On the other hand, subsystems A and B remain in Alice's and Bob's laboratory and are measured in basis X or Z. For the case where both Alice and Bob have chosen basis Z, the measurement is described by two projectors $\{\Pi^{(0)} := |0\rangle\langle 0|, \Pi^{(1)} := |1\rangle\langle 1|\}$. The resulting state is given by $\left((\Pi^i_A \otimes \Pi^j_B) \otimes \mathcal{E}_{CD}\right)(|\phi^+\rangle_{AC} \otimes |\phi^+\rangle_{DB})$ with $i, j = 0, 1$. The QKD measurement and BSM act on different Hilbert spaces and therefore they can be interchanged leading to $\left(\mathcal{E}_{CD} \otimes (\Pi^i_A \otimes \ Pi^j_B)\right)(|\phi^+\rangle_{AC} \otimes |\phi^+\rangle_{DB}) = \mathcal{E}_{CD}(|i\rangle_C \otimes |j\rangle_D)$ where the state $|i\rangle_C \otimes |j\rangle_D$ represents two single photons prepared in the Z basis with polarization i and j. The case of the X basis is analogous.

[2] The sifting rate does not appear because we employ an asymmetric protocol where Alice and Bob produce with probability almost one a state in base X and the remaining times a state in base Z [22].

[3] Here, we consider a completely symmetric set-up which implies that the success probability is the same on Alice's and Bob's side. However, in case that Alice and Bob have different probabilities, it is easy to repeat the analysis keeping these two probabilities different.

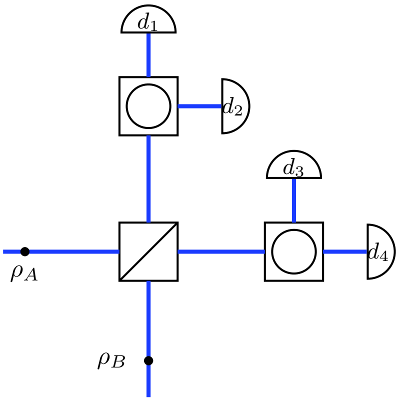


FIG. 2. (Color online) [adapted from [23]] Scheme for entanglement swapping with linear optics [3, 24]. The square with a diagonal line is a polarizing beam splitter in the rectilinear basis and the squares with a circle inside are polarizing beam splitters in the diagonal basis. Entanglement swapping is successful if d_1 and d_3 click (or d_1 and d_4 or d_2 and d_3 or d_2 and d_4). The state $\rho_A(\rho_B)$ is produced by Alice(Bob).

for generating one bit of the raw key is given by

$$\begin{aligned} < K > := &\sum_{s=0}^{\infty}\sum_{k=1}^{\infty} k\cdot s\cdot \\ &(P_{BSM}(k|k,k)(1-P_{BSM}(k|k,k))^s P(k,k)+ \\ &+\sum_{i=1}^{k-1} P_{BSM}(k|k,i)(1-P_{BSM}(k|k,i))^s P(k,i) \\ &+\sum_{i=1}^{k-1} P_{BSM}(k|i,k)(1-P_{BSM}(k|i,k))^s P(i,k)), \end{aligned} \tag{3}$$

where $P_{BSM}(k|k_A,k_B)$ is the probability that the BSM was successful at time $k=\max(k_A,k_B)$ when the two involved photons where stored at times k_A and k_B. Note that if we consider only the first line containing $P(k,k)$ then we recover the expression for the rate of the relay. The second (third) line accounts for the case that a photon sent by Bob (Alice) has been stored at a certain time $i<k$ and the photon sent by Alice (Bob) has been stored at time k. The average time becomes $<T>:=\Delta t<K>$.

In order to obtain a closed formula we consider a specific implementation of the BSM [3, 24] where the photons are first retrieved from the quantum memories and then measured with linear optics (see Fig. 2). This method is probabilistic and when implemented with perfect quantum memories and detectors leads to a maximal success probability of $\frac{1}{2}$ [25]. The BSM is successful when a particular two-fold detection happens. We consider practical threshold detectors with detection efficiency η_D and dark count probability p_D. We denote by η_M the retrieval probability of a photon from the quantum memory. The BSM success probability for the scheme given in Fig. 2 as a function of $\eta_{MD}:=\eta_M\eta_D$ is then given by [26]:

$$\begin{aligned} P_{BSM}(\eta_{MD}) :=&\frac{1}{2}(1-p_D)^2(\eta_{MD}^2+2(4-3\eta_{MD})\eta_{MD}p_D \\ &+8(1-\eta_{MD})^2p_D^2). \end{aligned} \tag{4}$$

For $p_D=0$ as we expect $P_{BSM}=\frac{\eta_{MD}^2}{2}$. Assuming that η_M does not depend on the time a simple expression for the average number of attempts in eq. (3) was derived in [27, 28],

$$< K > := \frac{1}{P_{BSM}(\eta_{MD})}\frac{3-2P_0}{(2-P_0)P_0}. \tag{5}$$

In the case of absence of quantum memories we get $< K >_{\text{relay}} := (P_{BSM}(P_0\eta_D))^{-1}$. For small P_0 the rate of the repeater scales as P_0^{-1} while the rate for the relay scales as P_0^{-2}. Moreover for the repeater, dark counts do not play a role as typically $p_D \ll \eta_{MD}$. The equivalent condition for the relay would be $p_D \ll \eta_D P_0$, which is much more difficult to ensure. For the quantum repeater η_M plays the role of P_0 for the relay.

With the same formalism we calculate the QBER which enters in the formula of the secret key rate. Let $e_j(k|k_A,k_B)$ be the QBER in the basis $j\in\{X,Z\}$ when the BSM has been performed at time k and the two photons were stored at times k_A and k_B, respectively. Then the average QBER in the basis j is given by

$$\begin{aligned} e_j = \sum_{k=1}^{\infty}\Big[&e_j(k|k,k)P(k,k) \\ &+\sum_{i=1}^{k-1} e_j(k|k,i)P(k,i) \\ &+\sum_{i=1}^{k-1} e_j(k|i,k)P(i,k)\Big], \end{aligned} \tag{6}$$

where the first line gives the QBER for the case of a quantum relay, i.e. when both photons arrive at the same time. The second and third lines include the contribution to the QBER given by the measurements where one photon arrived at $i<k$ and the second arrives at time k.

Here, we consider a simple model of decoherence where the quantum memory stores perfectly a quantum state for a certain time τ and then it transforms the quantum state to the identity for $t>\tau$ [27]. We call τ the coherence time and measure it in units of Δt. This model is valid in quantum memories where the fidelity remains approximately constant for a certain time and then it drops very fast. Formally, we have

$$\begin{aligned} e_j(k|k_A,k_B) :=& e_j(\infty)\Theta[\tau-(k-k_A)]\Theta[\tau-(k-k_B)] \\ &+\frac{1}{2}(1-\Theta[\tau-(k-k_A)]\Theta[\tau-(k-k_B)]), \end{aligned} \tag{7}$$

where $\Theta[t]$ is the Heaviside step function [29] such that $\Theta[t]=1$ for $t\geq 0$ and $\Theta[t]=0$ for $t<0$ and $e_j(\infty)$ is the QBER that would be obtained if the memory does not decohere ($\tau \to \infty$) and it is given by [30]

$$
\begin{aligned}
e_X(\infty) &= e_Z(\infty) \\
&= \frac{2p_D\left(2\left(\eta_{MD}-1\right)^2 p_D - \left(\eta_{MD}-2\right)\eta_{MD}\right)}{\eta_{MD}^2 + 8\left(\eta_{MD}-1\right)^2 p_D^2 + 2\left(4-3\eta_{MD}\right)\eta_{MD}p_D}.
\end{aligned} \tag{8}
$$

Inserting eq. (2), eq. (7) and eq. (8) in eq. (6) we obtain a closed formula for the average QBER:

$$
e_j = e_j(\infty) + \frac{1}{2}\frac{\left(\frac{1}{2}-e_j(\infty)\right)\left(1-P_0\right)^{1+\tau}}{2-P_0}. \tag{9}
$$

It is easy to verify $e_j(\infty) \leq e_j \leq \frac{1}{2}$ and moreover $\lim_{\tau\to\infty} e_j = e_j(\infty)$ and $\lim_{P_0\to 0} e_j = \frac{1}{2}$. Note that due to our specific set-up $e_X = e_Z$.

If the QBER is too high it is not possible to extract a secret key as the secret key rate in eq. (1) becomes non-positive. When $e_X = e_Z$ the maximal QBER for a non-zero secret key rate is given by $e^{\mathrm{MAX}} := 0.11$. A critical parameter is therefore τ_{SPS}^{MIN} which represents the minimal τ permitting to extract a secret key and can be obtained from eq. (9) by requiring that $e_X = e^{\mathrm{MAX}}$. The minimal allowed coherence time is given by

$$
\tau_{SPS}^{\mathrm{MIN}} = \frac{\log\left(\frac{(P_0-2)\left(e_X(\infty)-e^{\mathrm{MAX}}\right)}{(P_0-1)(2e_X(\infty)-1)}\right)}{\log\left(1-P_0\right)}. \tag{10}
$$

In the following section we will provide numbers for the minimal coherence time and the secret key rate in a realistic scenario.

C. Performance

We discuss now the performance of the protocol as a function of the imperfections of the set-up. Then we analyze the relation with the original MDI-QKD-RELAY with single-photon states. We consider an implementation where photons are transmitted through optical fibers. Therefore $P_0 := \eta_T$ where $\eta_T := 10^{-\frac{\alpha L}{2\cdot 10}}$ is the probability that a photon has not been absorbed after traveling for a distance $\frac{L}{2}$ and α is the absorption coefficient. Throughout the whole paper we will consider $\alpha = 0.17$ dB/km which is the lowest attenuation in common optical fibers. In the following analysis we will consider detectors with detection efficiency $\eta_D = 0.2$ and dark count probability $p_D = 10^{-6}$. Such detectors are considered optimistic but not unrealistic [1]. Regarding quantum memories we use $\eta_M = 0.6$ which is a value already achieved experimentally [3].

In Fig. 3 we show τ_{SPS}^{MIN} versus the distance between Alice and Bob. For $L = 400$ km we get $\tau^{MIN} \approx 4 \cdot 10^4$ which can be transformed in seconds multiplying by Δt. For an hypothetical source at 100 MHz this would correspond to a coherence time of the order of 400 microseconds. Note that single-photon sources at such a speed do not yet exist. We will reconsider this number in the next section when we will consider WCP sources. By increasing the repetition frequency it is possible to use quantum memories with lower coherence times. This is different to standard quantum repeater protocols where the coherence time depends also on the communication time. We see that the curve of τ^{MIN} is tightly upper bounded by the average maximal time that is necessary to wait before both quantum memories are filled up. This can be understood by observing that for $P_0 \ll 1$ and $e_X \approx 0$ we have $< K > P_{BSM} \approx \frac{3}{2P_0}$ and $\tau^{MIN} \approx \frac{log(2e^{MAX})}{-P_0} \approx \frac{1.51}{P_0}$.

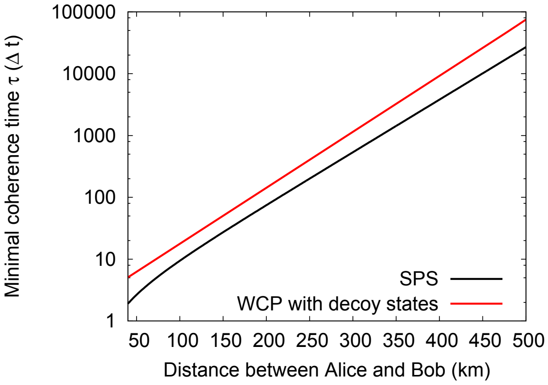


FIG. 3. (Color online) Minimal coherence time τ^{MIN} in units of Δt such that the secret key rate is non-zero. Black-solid line: SPS protocol (see eq. (10)). Red-solid line: WCP protocol (derived by calculating the zero of eq. (11)). Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km.

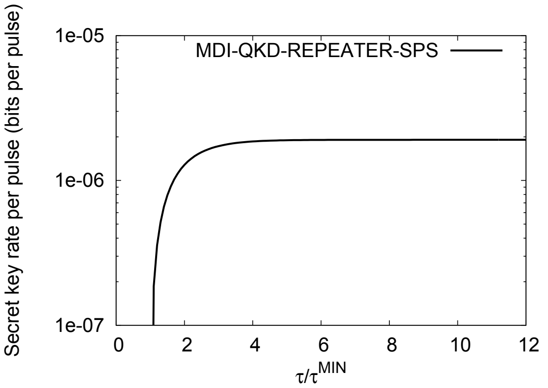


FIG. 4. (Color online) Secret key rate per pulse as function of $\tau/\tau_{SPS}^{\mathrm{MIN}}$. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km, $L = 400$ km.

In Fig. 4 we show the secret key rate as a function of $\tau/\tau_{SPS}^{\mathrm{MIN}}$ for a fixed distance between Alice and Bob ($L = 400$ km). We see that a flat region is reached for $\tau \approx 5\tau_{SPS}^{\mathrm{MIN}}$. The same behavior is found also for other values of the distance between Alice and Bob.

Finally, we discuss the secret key rate as a function of the distance and compare it to a set-up without quantum memories. As shown in Fig. 5, the set-up with quantum

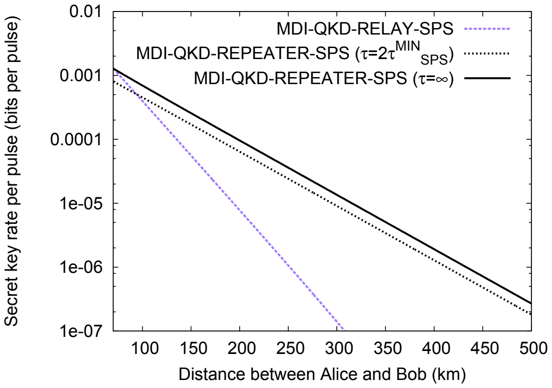


FIG. 5. (Color online) Secret key rate per pulse versus distance between Alice and Bob. Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 10^{-6}$, $\alpha = 0.17$ dB/km.

memories permits to increase significantly the secret key rate with respect to a set-up without quantum memories. For $\eta_{\mathrm{D}} = 0.2$, $\eta_M = 0.6$ and $p_D = 10^{-6}$ the cross-over distance is around 100 km. Moreover, we see that the difference between $\tau = 2\tau^{MIN}$ and $\tau = \infty$ is very small. This result suggests that the protocol is not very susceptible to decoherence of quantum memories: perfect quantum memories are not needed as coherence times slightly bigger than τ^{MIN} permit to achieve the maximal secret key rate obtainable with perfect quantum memories. Moreover, we have performed numerical simulations for quantum memories where the decoherence model is depolarization[4], and we found that this result does not change qualitatively.

Concluding this section, we have proven that using single-photon sources and imperfect quantum memories it is possible to essentially double the distance with respect to MDI-QKD-RELAY when implemented with single-photon sources.

III. SCHEME WITH WEAK COHERENT PULSE SOURCES

A critical assumption of the previous section was that Alice and Bob have on-demand single-photon sources at their disposal. In this section we consider sources of weak coherent pulses which offer a very high repetition frequency - with current technology even in the order of GHz [31]. On the other hand this type of source requires a more complicated security analysis due to the fact that multi-photon pulses are susceptible to the photon-number-splitting (PNS) attacks [32]. In order to detect this attack it is possible to use decoy states [18, 19]. In the scheme with decoy states Alice and Bob prepare phase randomized weak coherent pulses of the form $\rho = \sum_{n=0}^{\infty} p(n) \left|n\right\rangle \left\langle n\right|$ with $p(n) := e^{-\mu}\frac{\mu^n}{n!}$. The parameter μ is the intensity (average photon number) of the pulse.

The QKD protocol with decoy states [18, 19] which we employ here is analogous to the one described in sec. II, apart from the following differences:

- when Alice and Bob prepare the state they choose at random and independently also its intensity μ which is a continuous parameter with $0 \leq \mu < \infty$. One particular intensity $\overline{\mu}$ is chosen with probability almost one,
- the measurements for pulses with intensity $\overline{\mu}$ are used for extracting a secret key, whereas the others are used for detecting Eve's PNS attack.

The formula for the secret key rate is analogous to eq. (1) with the modifications due to the fact that Eve can perform PNS attacks. It is given by [5]:

$$r_\infty := \max_{\mu>0}\left[\frac{1}{<T>}(f_{11}(1-h(e_X^{11}))-h(e_Z))\right], \quad (11)$$

where f_{11} is the fraction of bits in the raw key which are generated when Alice and Bob send single-photon states and e_X^{11} is the QBER of these bits. The QBER e_X^{11}, is accessible due to the fact that we use decoy states [5]. The QBER e_Z is determined using all data. All quantities entering in the formula of the secret key rate in eq. (11) depend on a generic intensity μ. This intensity is used as free-parameter for the optimization of the secret key rate. The optimal intensity is denoted by $\overline{\mu}$ (see above). In the following we derive analytical expressions for these parameters as function of the imperfections of the set-up. We will assume that detectors have no dark counts. This will permit to have closed formulas which will allow to understand the role of each parameter. Dark counts do not play a crucial role as long as $\eta_{MD} \gg p_D$. For realistic choice of parameters this condition is easily satisfied.

Given a pulse of n-photons, the probability that at least one photon is stored into the quantum memory is given by $(1-(1-\eta_T)^n)$ where η_T is the probability that one photon has not been absorbed by the quantum channel. In general, the probability P_0 that a state has been stored into the quantum memory is given by

$$\begin{aligned} P_0 &:= \sum_{n=1}^{\infty} p(n)(1-(1-\eta_T)^n) \\ &= 1-e^{-\mu\eta_T}, \end{aligned} \quad (12)$$

which for $\mu\eta_T \ll 1$ reduces to $P_0 = \mu\eta_T$ as expected.

The BSM success probability depends on the probability to store a state with n-photons given that the source

[4] The model we have considered is $D(\rho) := e^{-\frac{t}{\tau}}\rho + \frac{1-e^{-\frac{t}{\tau}}}{2}\mathbf{1}$ where τ is the coherence time.

has generated a state of m-photons with $m \geq n$. Formally,

$$P(n) := \sum_{m=n}^{\infty} p(m) \binom{m}{n} \eta_T^n (1-\eta_T)^{m-n}$$
$$= \frac{(\eta_T \mu)^n}{n!} e^{-\eta_T \mu}. \tag{13}$$

The quantity $\binom{m}{n}\eta_T^n(1-\eta_T)^{m-n}$ is the probability that n photons survive from a state with m-photons after the transmission through the channel. The probability that the BSM is successful given that one quantum memory contains n_a photons and the other n_b photons is given by (see the appendix for our derivation)

$$P_{BSM}(n_a, n_b) = [(1-\frac{\eta_{MD}}{2})^{n_a} - (1-\eta_{MD})^{n_a}] \cdot$$
$$\cdot [(1-\frac{\eta_{MD}}{2})^{n_b} - (1-\eta_{MD})^{n_b}]. \tag{14}$$

For $n_a = n_b = 1$ we obtain $P_{BSM}(1,1) = \frac{1}{2}\eta_{MD}^2$ in accordance to eq. (4). Thus, the BSM success probability is given by

$$P_{BSM} := 2\frac{\sum_{n_a=1}^{\infty}\sum_{n_b=1}^{\infty} P(n_a)P(n_b)P_{BSM}(n_a,n_b)}{\sum_{n_a=1}^{\infty}\sum_{n_b=1}^{\infty} P(n_a)P(n_b)} \tag{15a}$$

$$= 2\frac{e^{-2\mu\eta_T(\eta_{MD}-1)}\left(e^{\frac{1}{2}\mu\eta_{MD}\eta_T}-1\right)^2}{\left(e^{\mu\eta_T}-1\right)^2}. \tag{15b}$$

The denominator in eq. (15a) gives the probability that two photons are stored in the quantum memories which is equal to P_0^2. The numerator is the total probability of all events in which the BSM is successful when one quantum memory contains n_a photons and the other one contains n_b photons. The factor 2 comes from the fact that the BSM with linear optics can distinguish only two Bell states. For the limiting case $\mu\eta_T \ll 1$ we obtain $P_{BSM} = P_{BSM}(1,1)$.

The fraction of measurements coming from single-photons is denoted as f_{11} and given by

$$f_{11} = \frac{P(1)^2 P_{BSM}(1,1)}{\sum_{n_a=1}^{\infty}\sum_{n_b=1}^{\infty} P(n_a)P(n_b)} \tag{16a}$$

$$= \frac{\mu^2\eta_{MD}^2\eta_T^2 e^{\mu\eta_{MD}\eta_T - 2\mu}}{4\left(e^{\frac{1}{2}\mu\eta_{MD}\eta_T}-1\right)^2}, \tag{16b}$$

which in the limit $\mu\eta_T \ll 1$ becomes $f_{11} = 1$ as in this limit all measurements come from single-photon states. The numerator of eq. (16a) represents the probability that the sources of Alice and Bob produce single-photons which are stored in the quantum memories and which lead to successful BSM. The denominator is the total probability to obtain a state which does not contain the vacuum.

Regarding the QBER we observe that if there are no dark counts then both e_X^{11} and e_Z are zero. This property of the protocol has been discussed also in [5]. Therefore, errors will arise only due to decoherence. The calculation is analogous to the one for single-photon sources of sec. 6. We assume the same decoherence model. The only difference comes from the fact that now P_0 is different, in particular we have

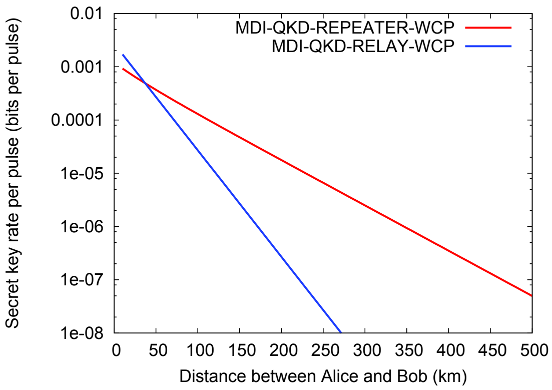


FIG. 6. (Color online) Secret key rate versus distance between Alice and Bob. Comparison between relay [5] (blue) and repeater (see eq. (11))(red). Parameters: $\eta_D = 0.2$, $\eta_M = 0.6$, $p_D = 0$, $\alpha = 0.17$ dB/km, $\tau = \infty$.

$$e_X^{11} = e_X^{11}(\infty) + \frac{1}{2}\frac{\left(\frac{1}{2} - e_X^{11}(\infty)\right)(1-P_0^{11})^{1+\tau}}{2-P_0^{11}}, \tag{17}$$

$$e_Z = e_Z(\infty) + \frac{1}{2}\frac{\left(\frac{1}{2} - e_Z(\infty)\right)(1-P_0)^{1+\tau}}{2-P_0}, \tag{18}$$

with $P_0^{11} = p(1)\eta_T$ the probability to store single-photon states in one quantum memory.

We have thus derived all quantities present in the formula of the secret key rate, and we can now evaluate and characterize the protocol.

In Fig. 6 we show the comparison between MDI-QKD-REPEATER-WCP and MDI-QKD-RELAY-WCP . As we see quantum memories permit to increase significantly the secret key rate or the distance where it is possible to perform QKD.

As shown in Fig. 3, the minimally allowed coherence time τ_{WCP}^{MIN} is larger then τ_{SPS}^{MIN} . The reason is that now the produced state contains also a vacuum that reduces the probability that a photon arrives to the quantum memory. However, the difference is less than one order of magnitude. Moreover, analogously to the case of SPS the flat region($\tau \to \infty$) of the secret key rate is reached already with $\tau = 5\tau_{WCP}^{MIN}$.

In practical cases, only a finite number of different decoy states is used. In order to adapt our result to this case it is enough to use the results of [13]. Moreover, finite-size corrections are necessary for giving realistic estimates. This can be done by adopting the formalism developed in [15–17]

IV. CONCLUSIONS

In this paper we have explored the possibility to enable long distance QKD without entanglement sources. We have shown that when quantum memories are used it is possible to improve the distance where measurement-device-independent quantum key distribution can be implemented. Moreover, we have shown that the protocol we consider in this paper is robust against common device imperfections such as detector efficiency, quantum memory retrieval efficiency and finite decoherence time. We believe that our result could be used as a first step in the development of long-distance quantum key distribution. It requires weak coherent pulse sources, which are already available commercially, and heralded quantum memories which are under current development.

ACKNOWLEDGMENTS

We would like to thank Sylvia Bratzik and Tobias Moroder for valuable and enlightening discussions. We acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, Project QuOReP).

APPENDIX

We prove eq. (14) when the Bell-state measurement is done between two WCP states in the computational basis. The proof for the case of the diagonal basis is analogous.

We define

$$G_{i_1 i_2 i_3 i_4}\left(\rho_A^{(n_a)}, \rho_B^{(n_b)}\right) := \text{tr}\left(\Pi^{(1)}_{d_{i_1}}\Pi^{(0)}_{d_{i_2}}\Pi^{(1)}_{d_{i_3}}\Pi^{(0)}_{d_{i_4}}\mathcal{E}\left(\rho_A^{(n_a)} \otimes \rho_B^{(n_b)}\right)\right) \tag{19}$$

where $\mathcal{E}$ represents the action of the partial BSM and is given by the following mapping (see Fig. 2)

$$b_H \to \frac{d_3 + d_4}{2}, \quad b_V \to \frac{d_1 - d_2}{2}, \tag{20}$$

$$a_H \to \frac{d_1 + d_2}{2}, \quad a_V \to \frac{d_3 - d_4}{2}, \tag{21}$$

where a_H, a_V are the modes of ρ_A and b_H, b_V are the modes of ρ_B. The POVM elements of threshold detectors are given by

$$\Pi^{(0)} := \sum_{i=0}^{\infty}(1-\eta_D)^i \left|i\right\rangle\left\langle i\right|, \Pi^{(1)} := \sum_{i=0}^{\infty}(1-(1-\eta_D)^i)\left|i\right\rangle\left\langle i\right|. \tag{22}$$

The success probability of a BSM is given by

$$P_{BSM}(n_a, n_b) := \frac{1}{4}\sum_{i_1 i_2 i_3 i_4 \in \mathcal{A}}\sum_{\phi \in \mathcal{B}} G_{i_1 i_2 i_3 i_4}\left(\phi^{\otimes n_a}, \phi^{\otimes n_b}\right), \tag{23}$$

where $\mathcal{A} = \{1234, 1243, 2134, 2143\}$ is the set containing the combinations of two-fold detection leading to a successful entanglement swapping and $\mathcal{B} = \{\left|HH\right\rangle\left\langle HH\right|, \left|VV\right\rangle\left\langle VV\right|\}$ is a set containing the quantum states produced by the two sources of Alice and Bob when they choose the computational basis. The set $\mathcal{B}$ does not contain the cross-terms like $\sigma := \left|HH\right\rangle\left\langle VV\right|$ because $G_{i_1 i_2 i_3 i_4}(\sigma^{\otimes n_a}, \sigma^{\otimes n_b}) = 0$. Due to the symmetries of the map $\mathcal{E}$ we find that the function G is equal for all combinations of indices in $\mathcal{A}$ and quantum states in $\mathcal{B}$, therefore

$$P_{BSM}(n_a, n_b) = \frac{4 \cdot 2}{4} G_{1234}\left(\left|HH\right\rangle\left\langle HH\right|^{\otimes n_a}, \left|HH\right\rangle\left\langle HH\right|^{\otimes n_b}\right). \tag{24}$$

Using the fact that $\left|HH\right\rangle := a_H^{\dagger} b_H^{\dagger}\left|0\right\rangle$ and using the definition of $\mathcal{E}$ it is straightforward, but lengthly, to calculate

G and finally to find the result in eq. (14).

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932–5935 (1998).
[3] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Reviews of Modern Physics **83**, 33 (2011).
[4] N. Sangouard, Nature Photonics **6**, 722 (2012).
[5] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[6] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[7] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, Phys. Rev. Lett. **92**, 047904 (2004).
[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics **4**, 686 (2010).
[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Communications **2**, 349 (2011).
[10] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, ArXiv e-prints (2012), arXiv:1204.0738 [quant-ph].
[11] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, ArXiv e-prints (2012), arXiv:1207.6345 [quant-ph].
[12] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, Q. Zhang, and J.-W. Pan, ArXiv e-prints (2012), arXiv:1209.6178 [quant-ph].
[13] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[14] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).
[15] F. Xu, M. Curty, B. Qi, and H.-K. Lo, ArXiv e-prints (2013), arXiv:1305.6965 [quant-ph].
[16] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Phys. Rev. A **86**, 022332 (2012).
[17] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[18] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[19] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[20] C. Bennett, G. Brassard, *et al.*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (Bangalore, India, 1984).
[21] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557–559 (1992).
[22] H. K. Lo, H. Chau, and M. Ardehali, Journal of Cryptology **18**, 133 (2005).
[23] J. c. v. Minář, H. de Riedmatten, and N. Sangouard, Phys. Rev. A **85**, 032313 (2012).
[24] H. Weinfurter, EPL (Europhysics Letters) **25**, 559 (1994).
[25] J. Calsamiglia and N. Lütkenhaus, Applied Physics B: Lasers and Optics **72**, 67 (2001).
[26] P. Kok and B. W. Lovett, *Introduction to optical quantum information processing* (Cambridge University Press, Cambridge, 2010).
[27] O. Collins, S. Jenkins, A. Kuzmich, and T. Kennedy, Physical Review Letters **98**, 060502 (2007).
[28] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).
[29] M. E. Abramowitz *et al.*, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, Vol. 55 (Courier Dover Publications, 1964).
[30] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).
[31] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, Lightwave Technology, Journal of **28**, 2572 (2010).
[32] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

Finite-range multiplexing enhances quantum key distribution via quantum repeaters.
S. Abruzzo, H. Kampermann, and D. Bruß.
ArXiv: 1309.1106, 2013. (submitted to Phys. Rev.A)

Journal: Submitted to Physical Review A
Impact Factor 2012: 3.042
Contribution: first author, idea to perform the analysis, scientific work and preparation of the manuscript.
Percentage of my work: 90%.

Finite-range multiplexing enhances quantum key distribution via quantum repeaters

Silvestre Abruzzo, Hermann Kampermann, Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany

Quantum repeaters represent one possible way to achieve long-distance quantum key distribution. Collins et al. in [Phys. Rev. Lett. 98, 060502 (2007)] proposed multiplexing as method to increase the repeater rate and to decrease the requirement in memory coherence time. Motivated by the experimental fact that long-range connections are practically demanding, in this paper we extend the original quantum repeater multiplexing protocol to the case of short-range connection. We derive analytical formulas for the repeater rate and we show that for short connection lengths it is possible to have most of the benefits of a full-range multiplexing protocol. Then we incorporate decoherence of quantum memories and we study the optimal matching for the Bell-state measurement protocol permitting to minimize memory requirements. Finally, we calculate the secret key rate and we show that the improvement via finite-range multiplexing is of the same order of magnitude as via full-range multiplexing.

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] allows two parties to share a secret key which might be used for applications in cryptography. The preferred quantum systems used for transmitting information are photons. These can be generated, distributed and measured fairly easily with standard technology. However, photons are usually transmitted through optical fibers and due to absorption the maximal distance where QKD is feasible is around 150 km [3]. In order to overcome this problem the concept of quantum repeaters can be used [4, 5]. For increasing the final repeater rate and the final fidelity many variations of the original protocol have been investigated [6–8], where one of the influential generalizations is *multiplexing* [9].

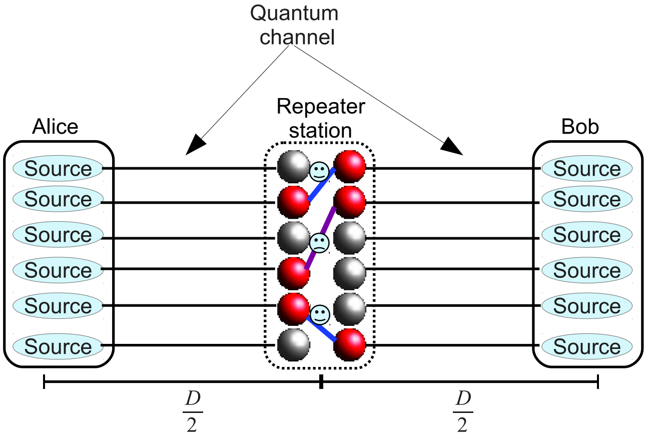


FIG. 1. (Color online) Alice and Bob are equipped with single-photon sources. Each source is connected through an optical fiber to a quantum memory in the repeater station. Red spheres represent filled quantum memories whereas gray spheres represent empty quantum memories. In this example the maximal connection length is one, therefore the connections indicated in blue are allowed and the magenta one is forbidden.

In fig. 1 we show a typical set-up of a quantum repeater with multiplexing. Alice and Bob have many single-photon sources which are connected to a quantum memory in the repeater station. Optical fibers are lossy, therefore after one attempt some quantum memories are filled up (red spheres in the picture) and some are empty (gray spheres). One possibility is to perform Bell-state measurements (BSMs) only between parallel quantum memories; the second possibility, which is called multiplexing is to allow BSMs between two arbitrary quantum memories of the two arrays. In Ref. [9] the authors give an analytical formula for the entanglement production rate with multiplexing when quantum repeaters with two segments are considered. The conclusion of [9] was that multiplexing gives only a modest improvement on the rate w.r.t. the case of parallel connections. However, it improves significantly the requirements on memory decoherence. In Ref. [10] a new protocol based on the Duan-Lukin-Cirac-Zoller protocol [6] has been studied and it has been found numerically that $R_M \approx R_P^{1.12}$ where R_M is the rate using multiplexing and R_P is the rate using parallel connections. Other works concerning multiplexing include Ref. [11] which studied the repeater rate and the final fidelity in the limit of large number of quantum memories, Ref. [12] which derived an analytical formula for the average number of attempts necessary for performing the first connection and Ref. [13] where a new protocol based on multiplexing has been proposed.

In this paper we assume a set-up with one repeater station, i.e. two segments (see fig. 1). We consider multiplexing when few quantum memories are used. We introduce the *finite-range multiplexing protocol* (FIRMP), which is motivated by the fact that long-range connections are experimentally demanding [14–16]. We provide analytical formulas for the repeater rate using the *full-range multiplexing protocol* (FURMP) and the FIRMP. Then we investigate quantum memory decoherence, and we study numerically the optimal algorithm such that the memory requirements for QKD are minimized.

The manuscript is organized as follows. In sec. II we introduce quantum key distribution and the quantum repeater protocol with finite-range multiplexing. Moreover,

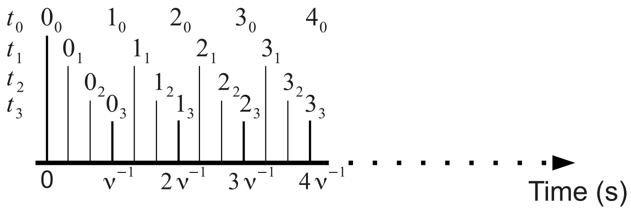

t_0 0_0 1_0 2_0 3_0 4_0
t_1 0_1 1_1 2_1 3_1
t_2 0_2 1_2 2_2 3_2
t_3 0_3 1_3 2_3 3_3
0
ν^{-1}
$2\nu^{-1}$
$3\nu^{-1}$
$4\nu^{-1}$
Time (s)

FIG. 2. (Color online) Description of our notation of time. Refer to the main text for the meaning of t_i. Bold vertical lines which are proportional to ν^{-1} represent the instant where sources produce new photons. The quantity ν is the frequency of the source measured in pairs per second.

we describe different Bell-state measurement strategies. In sec. III we derive analytical formulas for the repeater rate in the case of deterministic and probabilistic Bell-state measurements. In sec. IV we show how to minimize the memory requirement such that quantum key distribution is still possible and in sec. V we calculate the secret key rate. Finally, in sec. VI we summarize the results and outline possible future developments.

II. THE PROTOCOL

A. General description

Alice and Bob are two parties at a distance D who want to create a secret key using QKD. Throughout the present paper we consider that they use a quantum repeater with two segments, i.e. one repeater station. This set-up is particularly important because Alice and Bob do not necessarily need entanglement sources or quantum memories. Instead, single-photon sources or weak coherent pulse sources are sufficient. This set-up resembles the measurement-device independent QKD protocol proposed in [17, 18]. This protocol has been extended to the quantum repeater scenario with quantum memories in [19]. In this paper, the sources are supposed to be single-photon sources. However, the analysis for weak coherent pulse sources can be done following the methods developed in [17, 19]. We assume that the repeater station contains two arrays of m quantum memories, where one side receives the photons sent from Alice and the other one receives the photons sent from Bob (see fig. 1).

In the following we give the steps of the multiplexing protocol with finite-range connection. We define time variables denoted by t_i with integers $t \in [1, \infty)$ and $i = 0, 1, 2, 3$ interpreted as follows. The value of t denotes the attempts of the sources to produce photons. As shown in fig. 2 the variable t_i can be always related to the elapsed time in seconds from the beginning of the experiment by using the repetition frequency ν of the source which is measured in pairs per second. Therefore $1_0 \equiv \nu^{-1}$, $2_0 \equiv 2\nu^{-1}$, etc. We will call the interval between t_0 and $(t+1)_0$ a time-bin. The subindex i permits to describe instants contained in a time-bin. At time $t_0 = 0_0$ all quantum memories are empty and the protocol is just starting. The steps are the following (see fig. 3):

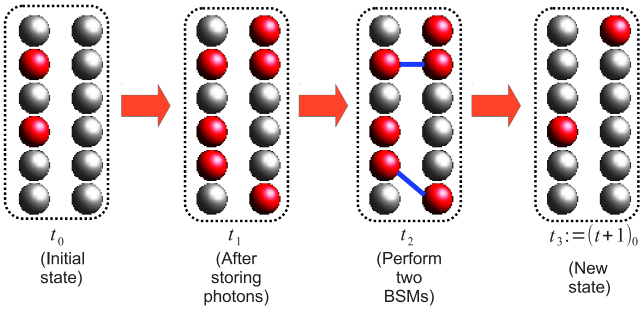


FIG. 3. (Color online) Representation of the repeater station, performing FIRMP: Steps performed in the repeater protocol in one time-bin. A red (gray) sphere indicates that the quantum memory is filled (empty). We have $m = 6$ quantum memories for each array and the connection length is $w = 1$. In t_2 it is not possible to perform all possible connections due to the limited connection length. In the case of FURMP in t_2 three BSMs would be possible and in t_3 all quantum memories would be empty.

at t_0 : Alice and Bob prepare randomly and independently m random states each according to a chosen QKD protocol[1]. They store the information regarding the preparation and they send the states to the repeater station.

at t_1 : Arriving photons are stored and heralded in the corresponding quantum memory.

at t_2 : The repeater station performs the maximal number of Bell-state measurements ℓ compatible with the maximal connection length w. For $w = 0$ only BSMs in parallel are allowed and for $w = m - 1$ any connection is possible.

at t_3 : The measured quantum memories are again empty. Restart from $i = 0$, i.e. $t_3 \equiv (t+1)_0$.

The repeater station communicates to Alice and Bob which pairs of quantum memories were used for the BSMs, as well as the measurements result. The protocol ends after a given number of rounds. After that, Alice and Bob will execute the standard QKD protocol which consists of sifting, parameter estimation, error correction and privacy amplification [3].

The advantage of a multiplexing protocol occurs at time t_2 where BSMs are performed such that the number of connections is maximized. In the case of FURMP

[1] For example, in the case of BB84 they prepare one of the four qubit states $|\psi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ where $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$.

this corresponds to performing as many BSMs such that one array of quantum memories is completely empty. In the case of FIRMP the maximal number of connections can be found using the *maximum cardinality bipartite matching* [20, 21], i.e. the maximum number of edges in a given bipartite graph such that each vertex has at most one neighbor. This problem can be explicitly formulated as follows: There is a list of filled quantum memories on the left. Each quantum memory on the left may be connected to several quantum memories on the right, depending on the maximal connection length. This defines a bipartite graph. By solving the maximum cardinality bipartite matching algorithm we find the maximal number of possible connections. In the case of full-range multiplexing the optimal matching will always leave one of the two arrays completely empty. This is not the case with finite-range multiplexing. However, it remains true that at least one of two involved quantum memories has been filled in the same time-bin when the connection is done. Obviously, there could be several possible matchings which maximize the number of connections. The chosen matching can have an influence on the final state fidelity due to memory decoherence. Possible strategies for choosing a matching are discussed in the following.

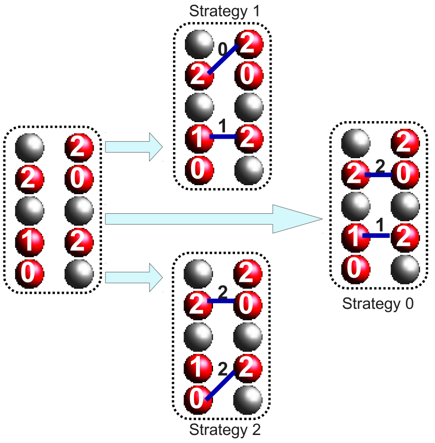


FIG. 4. (Color online) A red (gray) sphere indicates that the quantum memory is filled (empty). The number in the sphere represents the arrival time of the corresponding photon. On the left we have the situation at time 2_1 (see fig. 3). We consider $w = 1$. On the right three possible matching strategies are shown. Blue lines indicate the difference between the arrival times of the photons. It is possible to see the schemes on the right side as weighted bipartite graphs: red spheres are vertices and blue edges have indicated weights.

B. Multiplexing strategies

We can view the set-up in a repeater station as a bipartite weighted graph where the filled quantum memories are the vertices and the possible connections restricted by the maximal connection length are edges. To each vertex is assigned an integer value given by the arrival time of the stored photon. If the quantum memory is empty it does not represent a vertex.

A protocol for the BSMs matching consists of the following steps:

1. Identify all possible connections between the vertices. Assign to each edge a weight Δ given by the absolute value of the difference between the arrival times. This quantity identifies the amount of decoherence that has been experienced by the older quantum memory. This is a meaningful quantity because one of the two involved quantum memories is always fresh. The resulting data structure is a weighted bipartite graph $\mathcal{A} = \{(e_j, \Delta_j)\}$, i.e. a set of edges (vertex-pairs) and edge weights.

2. For each weighted bipartite graph $\mathcal{A}$ solve the *maximum cardinality bipartite matching* problem. We denote by $\mathcal{M}$ the subset of $\mathcal{A}$ containing graphs with exactly ℓ edges, where ℓ is the highest matching cardinality obtained over all graphs. This subset contains all graphs which maximize the number of connections, and thus the repeater rate.

3. Select one element $A_i \in \mathcal{M}$ by the following strategies:

Strategy 0 : choose with equal probability an arbitrary A_i from $\mathcal{M}$

Strategy 1 : minimize the sum of the weights $\sum_{j=1}^{l} \Delta_j$

Strategy 2 : maximize the sum of the weights $\sum_{j=1}^{l} \Delta_j$

The optimization involved in strategy 1 and 2 is known in literature as *maximum weighted bipartite matching*[20] and the optimization algorithm has complexity $O(m^3 \log m)$ [22] where m is the number of quantum memories on one side.

Strategy 1 connects pairs which arrived with a short time difference giving as a result the highest correlations which are possible to produce at a certain time. The disadvantage is that older pairs remain in the memories and therefore are used at a later time, having experienced decoherence for a long time. Strategy 2 resolves this mentioned problem, connecting pairs with the largest time difference. This strategy removes from the quantum memories older pairs as soon as possible, leaving only quantum memories which suffered decoherence for a short time. The disadvantage is that poor correlations are produced even when perfect correlations could be obtained. We have seen therefore, that both strategies have advantages and disadvantages. In sec. IV we will discuss which strategy minimizes the memory requirements for QKD. However, note that the repeater rate is independent of the matching strategies.

III. REPEATER RATE AS FUNCTION OF CONNECTION LENGTH

In this section we derive analytical formulas for the repeater rate for the FURMP and FIRMP. Let T_{C} be the current time (measured in time-bins as defined in the previous section), then the repeater rate is the fraction of successful BSMs per memory per time-bin calculated over the whole running time of the quantum repeater protocol, i.e.

$$R(T_{\mathrm{C}}) := \frac{1}{T_{\mathrm{C}}} \sum_{t=1}^{T_{\mathrm{C}}} \frac{< \ell > (t_2)}{m}, \tag{1}$$

where $< \ell(t_2) >$ is the average number of successful BSMs at time t_2. Many quantum repeater protocols are based on a probabilistic Bell-state measurement [6, 8]. The BSM is probabilistic when implemented with linear optics [23] or with detectors of finite efficiency [8]. When a measurement fails, the involved quantum memories are supposed to be emptied and this attempt is marked as unsuccessful. Let P_{BSM} be the success probability of the BSM. The probability that ℓ BSMs are successful is given by

$$\mathrm{Prob}[\Sigma = \ell](t_2) := \sum_{i=\ell}^{m} \binom{i}{\ell} \mathrm{Prob}[\Lambda = i](t_2) P_{BSM}^{\ell} (1 - P_{BSM})^{i-\ell}, \tag{2}$$

where Σ and Λ are random variables that can assume values 0,1, ..., m. The random variable Σ denotes the number of successful BSM and Λ the number of performed BSMs. The factor $P_{BSM}^{\ell}(1 - P_{BSM})^{i-\ell}$ represents the probability that ℓ BSM are successful and $i - \ell$ are not successful. This event can happen in $\binom{i}{\ell}$ different ways.

The average number of successful BSM at time t_2 is given by

$$\langle \ell \rangle (t_2) := \sum_{\ell=0}^{m} \ell \; \mathrm{Prob}[\Sigma = \ell](t_2) \tag{3}$$

In the following we will focus on Prob[Λ].

We denote as $\mathbf{c} = (\mathbf{a}, \mathbf{b})$ one possible configuration of the quantum memories in the repeater station. The vectors $\mathbf{a}$ and $\mathbf{b}$ of length m represent the status of the quantum memories on Alice's and Bob's side, respectively (see fig. 1). Each component takes the value 0 if the corresponding quantum memory is empty and 1 otherwise. We define as $\mathcal{H}_w^m(\ell)$ the set of all configurations leading to ℓ BSMs where w is the maximal connection length. For example, let $\mathbf{a} = (0, 1, 0, 1, 1, 0)$ and $\mathbf{b} = (1, 1, 0, 0, 0, 1)$ be the configurations of the quantum memories as seen in fig. 3 at t_2, then $(\mathbf{a}, \mathbf{b}) \in \mathcal{H}_1^6(2)$ and $(\mathbf{a}, \mathbf{b}) \in \mathcal{H}_5^6(3)$ but $(\mathbf{a}, \mathbf{b}) \notin \mathcal{H}_1^6(3)$ because when $w = 1$ the maximal number of connections is $\ell = 2$. Moreover, the set of all possible configurations is $\mathcal{H}_w^m := \cup_{\ell=0}^m \mathcal{H}_w^m(\ell)$.

We model the whole process consisting of storage and measurement with two maps. The *storage map* $\sigma_\ell : \mathcal{H}_w^m(0) \to \mathcal{H}_w^m(\ell)$ connects configurations at time t_0, i.e., before photons are received, to configurations at time t_1, i.e., after photons are received and stored. Given $\mathbf{c} \in \mathcal{H}_w^m(0)$, the probability to have the configuration $\mathbf{c}' \in \mathcal{H}_w^m(\ell)$ is given by

$$\begin{aligned} \mathrm{Prob}[\sigma_\ell(\mathbf{c}) = \mathbf{c}'] &:= \mathrm{Prob}[\mathbf{c}'|\mathbf{c}] && (4)\\ &:= \prod_{i=1}^{m} \mathrm{Prob}[c_i'|c_i] && (5)\\ &:= \prod_{i=1}^{m} \mathrm{Prob}[a_i'|a_i] \mathrm{Prob}[b_i'|b_i], && (6) \end{aligned}$$

with

$$\begin{aligned} \mathrm{Prob}[a_i'|a_i] := (1-p)(1-a_i')(1-a_i) \\ + p a_i'(1-a_i) + a_i' a_i, \end{aligned} \tag{7}$$

where p is the probability that a photon has not been absorbed by the quantum channel. The probability Prob[$b_i'|b_i$] is defined analogously. Equation (6) holds because the channels connecting each source to each quantum memory are independent. Equation (7) gives the conditional probability to have a final configuration a_i' starting from an initial configuration a_i. The three addends on the right-hand side of eq. (7) are mutually exclusive, i.e. given a certain configuration at most one is not zero.

The measurement map $\mu_\ell : \mathcal{H}_w^m(\ell) \to \mathcal{H}_w^m(0)$ relates configurations at time t_1 and $(t+1)_0$, i.e., after the quantum memories have been used for the BSMs. This map is deterministic, as the configuration $\mathbf{c}' \in \mathcal{H}_w^m(\ell)$ after the measurement is uniquely determined by the matching algorithm.

Coming back to the probability Prob[$\Lambda = \ell$](t_2) to have ℓ BSMs we get

$$\begin{aligned} \mathrm{Prob}[\Lambda = \ell](t_2) &:= \sum_{\mathbf{c}' \in \mathcal{H}_w^m(\ell)} \mathrm{Prob}[\mathbf{c}'](t_1) && (8)\\ &= \sum_{\mathbf{c}' \in \mathcal{H}_w^m(\ell)} \sum_{\mathbf{c} \in \mathcal{H}_w^m(0)} \mathrm{Prob}[\sigma_\ell(\mathbf{c}) = \mathbf{c}'] \mathrm{Prob}[\mathbf{c}](t_0), && (9) \end{aligned}$$

which is the sum over all possible initial configurations $\mathbf{c}$ and configurations $\mathbf{c}'$ at time t_2 of the probability that $\mathbf{c}$ leads to $\mathbf{c}'$ weighted with the probability that the configuration $\mathbf{c}$ was realized at time t_0. The probability Prob[$\mathbf{c}$](t_0) is given by

$$\mathrm{Prob}[\mathbf{c}](t_0) = \sum_{\mathbf{c}' \in \mathcal{H}_w^m(0)} \sum_{l=0}^{m} \mathrm{Prob}[\mu_\ell \circ \sigma_\ell(\mathbf{c}') = \mathbf{c}]\mathrm{Prob}[\mathbf{c}']((t-1)_0), \tag{10}$$

i.e., given a state $\mathbf{c}' \in \mathcal{H}_w^m(0)$ at time $(t-1)_0$, we calculate the probability that photon storage and measurement will lead to $\mathbf{c} \in \mathcal{H}_w^m(0)$ at time t_0. This last probability can be rewritten as

$$\mathrm{Prob}[\mu_\ell \circ \sigma_\ell(\mathbf{c}) = \mathbf{c}'] = \sum_{\mathbf{c}'' \in \mathcal{H}_w^m(\ell)} \delta_{\mu_\ell(\mathbf{c}''),\mathbf{c}'} \mathrm{Prob}[\sigma_\ell(\mathbf{c}) = \mathbf{c}''], \tag{11}$$

where $\delta_{\mathbf{a},\mathbf{b}}$ is the Kronecker delta such that $\delta_{\mathbf{a},\mathbf{b}} = 1$ iff $\mathbf{a} = \mathbf{b}$ and $\delta_{\mathbf{a},\mathbf{b}} = 0$ otherwise. Using the previous formulas and the initial condition $\mathrm{Prob}[(\mathbf{a}, \mathbf{b})](0_0) = \delta_{\mathbf{a},\mathbf{0}}\delta_{\mathbf{b},\mathbf{0}}$ we have now all elements for calculating the repeater rate in eq. (1). In order to do that one inserts eq. (11) into eq. (10) which is then inserted in eq. (8) which is finally used for calculating eq. (3) through eq. (2). The calculation was performed in C++. The measurement map has been implemented using the library provided at Ref. [24]. The complexity of the calculation is proportional to the number of time steps because for calculating $< l > (t)$ it is sufficient to know quantities at time $t-1$. However, the set $\mathcal{H}_w^m(\ell)$ grows quite fast as function of m and therefore reasonable time considerations restricted the calculation to a maximal of $m \leq 7$. Regarding fig. 5 the calculation ran for two days on a cluster of 10 nodes, cpu with four-cores and eight GB of RAM.

In the following and for the rest of the paper we consider $p = 0.001$ which represents the transmission probability of a single photon over an optical fiber of length $D = 150$ km and for an absorption coefficient $\alpha = 0.2$ dB/km. The relation between p and the distance between Alice and the repeater station D is $p = 10^{-\frac{\alpha D}{10}}$ [25].

As seen in fig. 5 the repeater rate increases as function of the time reaching a plateau at time $t \approx 10^4$. We see that this behavior persists when changing the maximal connection length w. Analyzing the dependence on the maximal connection length, we observe in fig. 5 that the gap between $w = 0$ and $w = 1$ is almost the same than the gap between $w = 0$ and $w = 4$ which represents full-range multiplexing. This shows that in an experimental implementation in order to profit of multiplexing it is not necessary to have long-range connection. Moreover, for our set-up with a source at 1 kHz, the loading time is 10 s long. This result could give a hint that in more complex quantum repeater protocols with many repeater stations, using distillation and classical communication, the loading time could play a significant role in the total time of the execution of the quantum repeater protocol.

Finally, we give an analytical formula for the rate when the plateau is reached. The time evolution of our system is specified in eq. (10). For $t \to \infty$, the rate becomes time-independent:

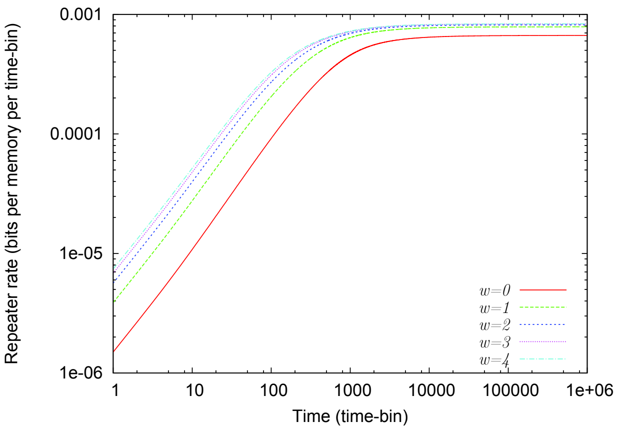


FIG. 5. (Color online) Repeater rate per memory as function of the time for $m = 5$ and various maximal connection length w (see eq. (1)). Parameters: $p = 0.001$, $P_{BSM} = 1$.

$$\mathrm{Prob}[\mathbf{c}] = \sum_{\mathbf{c}' \in \mathcal{H}_w^m(0)} \sum_{l=0}^{m} \mathrm{Prob}[\mu_\ell \circ \sigma_\ell(\mathbf{c}') = \mathbf{c}]\mathrm{Prob}[\mathbf{c}']. \tag{12}$$

Here Prob[**c**] is the unknown to be determined. We derive an analytical form of Prob[**c**] in App. A. Here, we use this formula (eq. (A2)) for calculating the asymptotic repeater rate as function of the BSM success probability. As shown in fig. 6 the largest improvement is possible to have with full-range multiplexing, but already a similar improvement is reached with maximal connection length $w = 1$, instead of $w = 4$. Moreover, the linear behavior can be justified as follows. In the case of $p = 0.001$ and for $w = 1$ we obtain $\mathrm{Prob}[\Lambda = 1] = 3.9 \cdot 10^{-3}$, $\mathrm{Prob}[\Lambda = 2] = 5.5 \cdot 10^{-6}$ and $\mathrm{Prob}[\Lambda > 2] \ll \mathrm{Prob}[\Lambda = 2]$. Therefore, eq. (3) becomes $\langle \ell \rangle \approx P_{BSM}\mathrm{Prob}[\Lambda = 1]$ which is linear in P_{BSM}. For other values of the maximal connection length the order of magnitude of the probabilities is the same.

IV. DECOHERENCE OF THE QUANTUM MEMORIES

In case of multiplexing, even when the rate is maximized it is possible to connect pairs in different ways. In this section, we study the optimal matching algorithm for the BSM in relation to memory decoherence. For simplicity we will stick to deterministic entanglement swapping, i.e. $P_{BSM} = 1$ in eq. (3).

Our figure of merit for optimizing the matching algo-

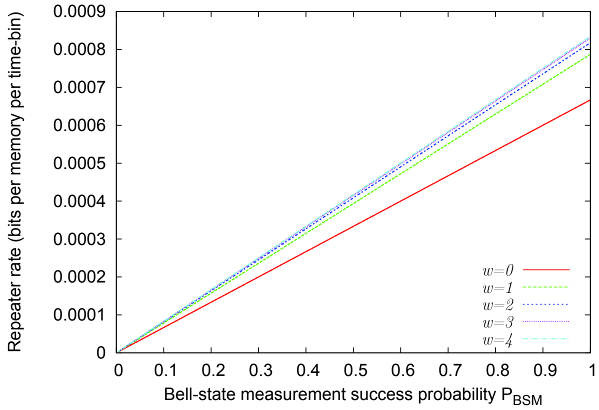


FIG. 6. (Color online) Repeater rate per memory per time-bin (eq. (1), eq. (3), eq. (A2)) as a function of the BSM success probability. Parameters: $p = 0.001, m = 5$.

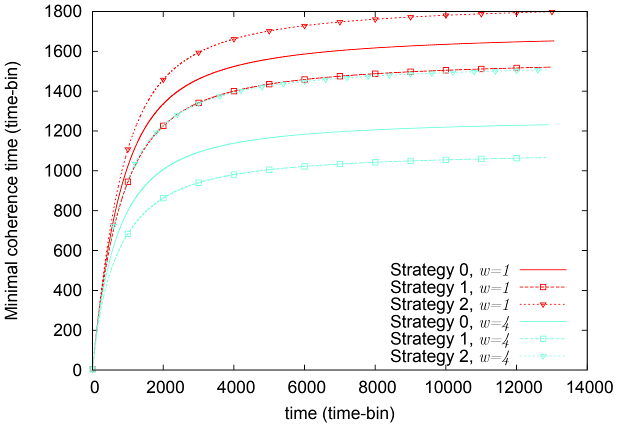


FIG. 7. (Color online) Minimal necessary coherence time τ (see eq. (15)) as function of the time t for different strategies. Strategy 0 (solid lines), strategy 1 (dashed lines with squares), strategy 2 (dotted lines with reversed triangles). Parameters: $p = 0.001, m = 5, w = 1, 4$.

rithm will be the secret fraction, which in QKD characterizes the fraction of secret bits that can be extracted the from measured qubits [3]. In the case of the BB84 protocol the secret fraction is given by [3]

$$r_\infty := 1 - h(e_X) - h(e_Z), \tag{13}$$

where e_X, e_Z are the quantum bit error rates (QBER) in base X and Z and $h(p) := -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy. For simplicity, we consider a symmetric error model such that $e_X = e_Z =: e$. The QBER resulting from measurements performed at time t_2 is

$$\overline{e}(t_2) := \sum_{\delta=0}^{t_2} \tilde{e}(\delta)\mathrm{Prob}[\Delta = \delta](t_2), \tag{14}$$

where $\mathrm{Prob}[\Delta = \delta](t_2)$ is the fraction of measurements of quantum memories which have experienced decoherence for a time $\Delta = \delta$. This probability depends on the BSM strategy (see sec. II). The QBER after these measurements is given by $\tilde{e}(\delta)$. This quantity depends on the decoherence mechanism of the quantum memories. In this paper we consider depolarization. Given ρ_0, the state of the quantum memory at time t_0, after depolarization it becomes

$$\rho(t - t_0) := p(t - t_0)\rho_0 + \frac{1 - p(t - t_0)}{2}\mathbb{1}, \tag{15}$$

where $p(t) := e^{-\frac{t}{\tau}}$ and τ is the decoherence time of the quantum memory.

For the BB84 it holds[2]

$$\tilde{e}(\delta) := \frac{2}{3}(1 - p(\delta)). \tag{16}$$

The total QBER is calculated between all outcomes that Alice and Bob get from the beginning of the protocol until time T_C which is equal to

$$e(T_\mathrm{C}) := \frac{\sum_{t=0}^{T_\mathrm{C}} \langle \ell \rangle (t_2) \sum_{\delta=0}^{t_2} \tilde{e}(\delta)\mathrm{Prob}[\Delta = \delta](t_2)}{\sum_{t=0}^{T_\mathrm{C}} \langle \ell \rangle (t_2)}. \tag{17}$$

Here, the denominator is the total number of BSMs from the beginning of the protocol until time T_C. The numerator is the average QBER for each time-bin weighted with the total number of successful measurements for each time-bin. The secret key rate is not zero whenever $e(T_\mathrm{C}) \leq 0.11$. This will be used to obtain a lower bound on the necessary coherence time τ.

We have calculated eq. (17) using numerical simulations. It is also possible to proceed analytically as explained in sec. III. However, the space of the configurations is so large that the analytical computation becomes unfeasible. We have performed numerical simulations by repeating many times the protocol, and from the obtained connections we have calculated the averages. The number of used experiments is about 10^9 which permits to have a variance of the mean smaller than 0.001. The simulations were performed for the strategies 0, 1, and 2, which were introduced in sec. II.

[2] The reason is that entanglement swapping between two depolarized states with fidelities F_0 and F_1, respectively, will result in a depolarized state of fidelity $F_2 = \frac{1}{3}(1 - F_1 - F_0 + 4F_0F_1)$. Inserting $F_1 = 1$ and $F_0 = p$ and using the fact that $e = \frac{2}{3}(1 - F_2)$ [25] the result follows.

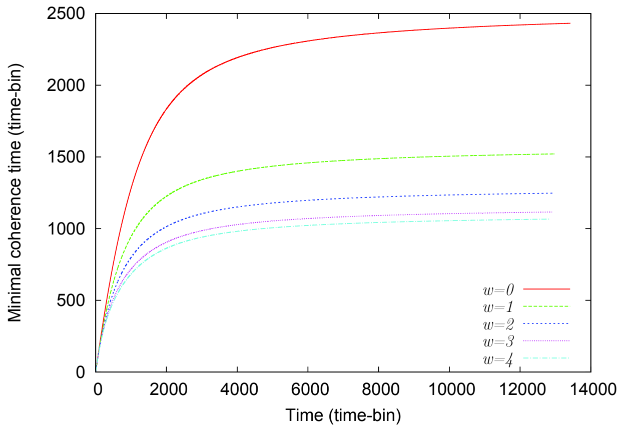


FIG. 8. (Color online) Minimal coherence time τ (see eq. (15)) as function of the time t for different maximal connection length. Parameters: $p = 0.001, m = 5$.

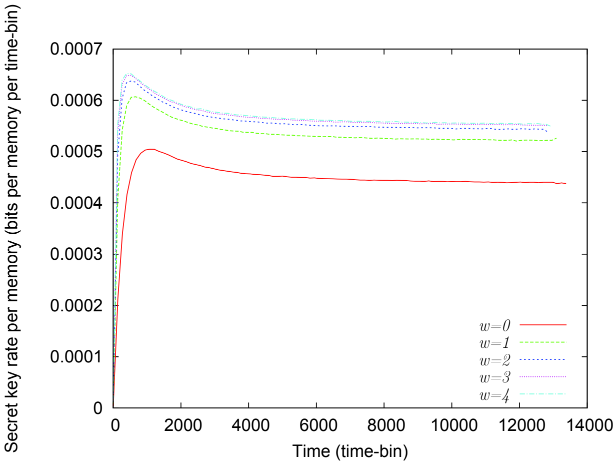


FIG. 9. (Color online) Secret key rate as function of the time t. for different maximal connection length. Parameters: $p = 0.001, m = 5$. The coherence time is shown in tab. I.

As shown in fig. 7 the minimal necessary coherence time is given by strategy 1. We see that strategy 0 is between strategy 1 and 2 and that the ordering between the strategy remains the same by changing the maximal connection length.

We then studied how the minimal coherence time scales as function of w. As seen in fig. 8 even a maximal connection length of $w = 1$ has a significant impact on the minimal coherence time, compared to $w = 0$. In particular we observe that for $t = 12000$ the improvement from $w = 0$ to $w = 1$ is roughly 60%.

V. SECRET KEY RATE

In this section we will sum up the results of the previous two sections and we will calculate the secret key rate. The secret key rate at time T_C is calculated as the product of the repeater rate and the secret fraction [3], i.e. [3, 27]

$$K(T_C) := R(T_C) \cdot r_\infty(e(T_C)), \tag{18}$$

where the repeater rate or raw key rate $R(T_C)$ was defined in eq. (1) and the QBER was given in eq. (17). For our calculation we have used the minimal coherence time calculated in the previous section. In particular we have chosen

$$\tau = 5\tau_{\min}(12800). \tag{19}$$

We use $t = 12800$ because it is the highest achievable with our simulation (see fig. 8). In tab. I we report the used coherence time for each value of w. As shown in fig. 9 the finite-range multiplexing with $w = 1$ leads to a similar improvement as with $w = 4$. Interestingly, we see that the secret key rate has a maximum for $t < 1000$ and then it slowly decreases. This fact can be explained by observing that there are two competing behaviors: the repeater rate increases with the time and the secret fraction decreases with the time, as the QBER increases with time, due to the fact that the probability that poor connections happen increases. An improvement may be to remove very old pairs which are known not to contribute to the final secret key. This method will certainly decrease the QBER at the expense to decrease also the repeater rate. We postpone to future investigations new possible schemes which could permit to have a secret key rate which has a monotonic behavior.

w	τ (time-bin)
0	12133.02
1	8989.75
2	7997.70
3	7631.75
4	7533.51

TABLE I. Value of the coherence time τ used for calculating the secret key rate. In order to obtain the value in seconds it is sufficient to divide by the frequency of the source.

VI. CONCLUSIONS

Quantum repeaters offer the possibility to enlarge the distance where quantum key distribution becomes feasible. In this paper we have considered the scenario with one repeater station in the middle, containing several pairs of quantum memories. This is a generalization of measurement-device independent QKD with quantum memories and single-photon sources. We have consid-

[3] The sifting rate is not explicitly written because we assume that a biased choice of the bases is done [26]. Therefore the sifting rate in the asymptotic case is 1.

ered multiplexing as a scheme for performing the Bell-state measurement. We introduced the concept of finite-range multiplexing which originates from the experimental constraint that long range connections are demanding. We have characterized analytically the repeater rate for the case of probabilistic and deterministic Bell-state measurement. We found that in a multiplexing protocol already short-range connections cover most of the improvement over a standard protocol. Decoherence of the quantum memories and different strategies for connecting the pairs were also studied. We found that it is always optimal to connect pairs with the shortest time difference in arrival time: this strategy minimizes the necessary coherence time required by the quantum memories in order to extract a secret key. Moreover, we have shown that also for the figure of merit "minimal coherence time" short-range multiplexing is almost as good as general multiplexing. Finally, we have studied the secret key rate which characterizes the performance of quantum key distribution, finding results analogous to the previous sections. Future questions may include the case of Alice and Bob using weak coherent pulses. This can be done by following [19]. The analysis of finite-size effects for QKD can be performed by following [28–30]. The techniques derived in our paper may also be used for addressing more complicated multiplexing protocols involving distillation and classical communication. Our work suggests that in more complex protocols the loading time may play a significant role, thus reducing the repeater rate w.r.t. asymptotic formulas.

VII. ACKNOWLEDGMENT

We would like to thank Sylvia Bratzik, Michael Epping, René Schwonnek and Peter van Loock for valuable and enlightening discussions. We acknowledge financial support by the German Federal Ministry of Education and Research (BMBF, Project QuOReP).

Appendix A: Derivation of the repeater rate in the asymptotic case

In order to determine the left-hand side of eq. (12), we define a function $\gamma : 0, 1, ..., N \to \mathcal{H}_w^m(0)$ where $N = |\mathcal{H}_w^m(0)|$ is the cardinality of $\mathcal{H}_w^m(0)$. We rewrite eq. (12) in the following way

$$f(x) = \sum_{x'=0}^{N} q(x', x) f(x'), \tag{A1}$$

where $f(x) := \text{Prob}[\gamma(x)]$ and $q(x', x) := \sum_{l=0}^{m} \text{Prob}[\mu_\ell \circ \sigma_\ell(\gamma(x')) = \gamma(x)]$. The solution is the following

$$f(x) = \frac{K_N(N, x)}{\sum_{x'=0}^{N} K_N(N, x')}, \tag{A2}$$

with

$$K_N(x', x) := \frac{K_{N-1}(N-1, x)}{1 - K_{N-1}(N-1, N-1)} K_{N-1}(x', N-1) + K_{N-1}(x', x), \tag{A3}$$

$$K_0(x', x) := q(x', x). \tag{A4}$$

In order to see that observe that eq. (A1) can be seen as a system of equations of the unknowns $\{f(0), f(1), ..., f(N)\}$, with the additional condition $\sum_{x=0}^{N} f(x) = 1$ which comes from the fact that $f(x)$ is a probability and we sum over the whole space. Therefore we have

$$f(0) = q(0, 0) f(0) + \sum_{x'=1}^{N} q(x', 0) f(x') \tag{A5}$$

$$\Rightarrow f(x) = \sum_{x'=1}^{N} K_1(x', x) f(x'), \tag{A6}$$

with $K_1(x', x)$ given in eq. (A3). Repeating the procedure, the function $f(x)$ can be expressed as

$$f(x) := K_N(N, x) f(N). \tag{A7}$$

The form in eq. (A2) is obtained by using the additional constraint $\sum_{x=0}^{N} f(x) = 1$.

[1] C. Bennett, G. Brassard, *et al.*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Vol. 175 (Bangalore, India, 1984).

[2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

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

[4] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932–5935 (1998).

[5] W. Dür, H. J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169–181 (1999).

[6] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413–418 (2001).

[7] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

[8] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Reviews of Modern Physics **83**, 33 (2011).

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

[10] L. Jiang, J. M. Taylor, and M. D. Lukin, Physical Review A **76**, 012301 (2007).

[11] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).

[12] N. K. Bernardes, L. Praxmeyer, and P. van Loock, Phys. Rev. A **83**, 012323 (2011).

[13] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, Nature Photonics **4**, 792 (2010).

[14] D. R. Leibrandt, J. Labaziewicz, R. J. Clark, I. L. Chuang, R. J. Epstein, C. Ospelkaus, J. H. Wesenberg, J. J. Bollinger, D. Leibfried, D. J. Wineland, *et al.*, Quantum Information & Computation **9**, 901 (2009).

[15] N. Sangouard, R. Dubessy, and C. Simon, Physical Review A **79**, 042340 (2009).

[16] M. Kumph, M. Brownnutt, and R. Blatt, New Journal of Physics **13**, 073043 (2011).

[17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[18] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[19] S. Abruzzo, H. Kampermann, and D. Bruß, ArXiv: 1306.3095 (2013).

[20] D. West, *Introduction to graph theory* (Prentice Hall, 2001).

[21] J. Kleinberg and E. Tardos, *Algorithm Design* (Pearson Education, 2006).

[22] L. Liu and D. A. Shell, in *Proceedings of Robotics: Science and Systems* (2012).

[23] J. Calsamiglia and N. Lütkenhaus, Applied Physics B: Lasers and Optics **72**, 67 (2001).

[24] L. Liu, "A primal based task allocation method," `http://students.cse.tamu.edu/lantao/codes/iprimal.php/` (2012), [Online; accessed 24-August-2013].

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

[26] H. Lo, H. Chau, and M. Ardehali, Journal of Cryptology **18**, 133 (2005).

[27] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Phys. Rev. A **87**, 052315 (2013).

[28] T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, Phys. Rev. A **86**, 022332 (2012).

[29] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[30] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, ArXiv e-prints (2013), arXiv:1307.1081 [quant-ph].

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

Düsseldorf, den 05. November 2013

(Silvestre Abruzzo)

Hiermit erkläre ich, dass ich die Dissertation keiner anderen Fakultät bereits vorgelegt habe und keinerlei vorherige erfolglose Promotionsversuche vorliegen.

Düsseldorf, den 05. November 2013

(Silvestre Abruzzo)