Long-distance quantum key distribution with imperfect devices

Nicoló Lo Piparo

School of Electronic and Electrical Engineering

University of Leeds

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

9th March 2015

Acknowledgements

Foremost, I would like to express my sincere gratitude to my supervisor Dr. Mohsen Razavi for the continuous support given during my Ph.D, for his patience, motivation, enthusiasm, and knowledge. His guidance helped me throughout my research and writing of this thesis. I could not have imagined having a better supervisor and mentor for my Ph.D.

I thank my fellow office mate Christiana Panayi for the fruitful discussions about the paper she wrote.

Last but not the least, I would like to thank my parents and all my friends.

Declarations

The candidate confirms that the work submitted is his own, except where work which has formed part of jointly authored publications has been included. The contribution of the candidate and the other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others. The material contained in the chapters of this thesis has been previously published in research articles written by the author of this work (Nicoló Lo Piparo), who appears as lead (first) author in all of them, and Dr. Mohsen Razavi. The research has been supervised and guided by Dr. Mohsen Razavi, and he appears as a co-author on these articles. All the material included in this document is of the author's entire intellectual ownership.

The work in chapter 3 of the thesis has appeared in publication as follows:

- *Measurement−device−independent quantum key distribution with ensemble−based memories* by N. Lo Piparo, M. Razavi and C. Panayi, to appear in IEEE Journal of Selected Topics in Quantum Electronics (2015), special issue on Quantum Communications. I have analyzed the system by calculating the secret key rate when quantum memories are affected by multiple-excitation and have a finite coherence time.

- *Quantum Memories in Action* by M. Razavi, N. Piparo, C. Panayi, X. Ma, and N. Ltkenhaus, Invited Paper to Quantum Information and Measurement conf., Messe Berlin, Berlin Germany (2014).

The work in chapter 4 of the thesis has appeared in publication as follows:

- *Long-distance quantum key distribution with imperfect devices* by N. Lo Piparo and M. Razavi, Phys. Rev. A 88, 012332 (2013).

The work in chapter 5 of the thesis has appeared in publication as follows:

- *Long-distance trust-free quantum key distribution* by N. Lo Piparo and M. Razavi, to appear in IEEE Journal of Selected Topics in Quantum Electronics (2015), special issue on Quantum Communications.

- *Architectural considerations in hybrid quantum-classical networks* by M. Razavi, N. Lo Piparo, C. Panayi, and D. E. Bruschi, invited paper to the IEEE's Iran Workshop on Commun. and Inf. Theory, Tehran, Iran, May 2013.

Abstract

Quantum key distribution (QKD) is one of the most promising techniques for the secure exchange of cryptographic keys between two users. Its unique property of relying on the laws of physics makes it an appealing tool for secure communications. While QKD has been implemented over distances on the order of a few hundreds of kilometers, the transmission rate of the key severely drops, when we go to further distances. An easy solution to this could rely on a network of trusted nodes. This solution, however, is far from ideal. In this thesis, we focus on obtaining long-distance secure communications by using trust-free intermediate nodes between two users. Quantum repeaters will then be at the core of our work and we analytically study different systems under realistic scenarios. We cover a range of repeater setups incorporating quantum memories (QMs), in terms of their short-term and long-term feasibility and in terms of ease of access for end users. We consider the main imperfections of the employed devices. In particular, we consider ensemble-based QMs, which offer a feasible route toward the implementation of probabilistic quantum repeaters. We study the effects of multiple excitations in such QMs and its effects on the key rate in a memory-assisted measurement-device-independent QKD (MDI-QKD) system. We then analytically compare the performance of two probabilistic quantum repeater protocols by calculating their secure key rates. We identify under which regimes of operation one system outperforms the other. Source and memory imperfections are considered in our analysis. Finally, we combine a quantum repeater scheme with the MDI-QKD protocol and we derive the largest distances that is possible to reach under practical

assumptions. Overall we obtain a realistic account of what can be done with existing technologies in order to improve the reach and the rate of QKD systems within a larger quantum network.

Abbreviations

Abbreviations used in this thesis	Full expression
BC	Bit commitment
BSM	Bell-state measurement
DLCZ	Duan-Lurin-Cirac-Zoller
MDI-QKD	Measurement-device-independent QKD
PNS	Photon-number-splitting
QBER	Quantum bit error rate
QKD	Quantum key distribution
QM	Quantum memory
SPS	Single-photon source

Contents

List of Figures

Chapter 1

Introduction

Sharing information has become a daily operation, which involves millions of users around the world. People, separated by large distances, need to communicate in a secure and confidential way for buying and selling goods, or simply for having a private conversation. Therefore, it is very important to develop methods and techniques to secure data storage and data transmission. This is the main objective of cryptography. Throughout history, different cryptographic systems have been developed aiming at providing security against potential eavesdroppers who attempt to hack them. These systems often relied on the complexity of encryption algorithms in order to make it more challenging for an eavesdropper to decrypt the message. An alternative approach to ensuring security is offered by quantum cryptography, whose security relies on the laws of nature. In fact, in a quantum cryptographic protocol, any attempt by an eavesdropper to intercept the secret key can, in principle, be detected by the users. On the one hand, the quantum nature of such systems provides unconditional security but, on the other, it makes such systems quite fragile. This thesis is focused around one of the key applications of quantum cryptography knows as quantum key distribution (QKD). Here, I study how we can implement reliable QKD systems over long distances despite of imperfections in our employed devices. Before explaining the work done in this thesis, in the following, I will present a historical background, which will help me introduce the main topics studied in this thesis.

1.1 Cryptography

The word cryptography etymologically comes from the Greek word $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$, hidden or secret, and $\gamma\rho\alpha\phi\eta$, writing, and it might be defined as the science that deals with encrypting and decrypting messages in order to ensure their authenticity, integrity and security.

In the 20^{th} century, many cryptographic systems have been developed, pushed especially by the urge of secure communication during the two world wars. One particular important cryptosystem was proposed in 1917 by G. Vernam, hence called the Vernam cipher or the one-time pad. This was a substitution cipher, where each letter was advanced by a random number of positions in the alphabet. In this way, by knowing the number series, i.e., the key, it was possible to reconstruct the original message. Although this kind of cipher was quite secure against enemies with low computational power, it faced the problem of how to distribute the key in a secure way. Later on, we will see the importance of such a cipher in the recent developments of cryptography and how QKD can help us with this problem. A machine that had a big relevance in the cryptographic world and was used massively during the second world war was the so called Enigma machine, invented by Arthur Schrebious. It consisted of a set of rotating wired wheels, which could perform a very sophisticated substitution cipher. Further improvements brought the Enigma machine to produce 159×10^{18} possible combinations (cryptoraphic keys), which made it the hardest cryptographic machine to break in those times. Today, a Pentium-based computer can decipher an Enigma-crypted message in a few minutes [3]. We need therefore a cryptographic system whose security can hardly be jeopardized by the most advanced computers.

In the world of cryptography there are two main branches that have been developed throughout the years: public-key cryptography and secret key cryptography. In the following subsections I briefly describe the main features of them.

1.1.1 Public-key cryptography

Public-key cryptography, also known as asymmetric cryptography, was invented in 1976 by Whitfield Diffie and Martin E. Hellman [4] and is perhaps the key

enabling technique in providing security in the today's Internet. It is used for authentication and to share initial seed keys, which will be used for various cryptographic protocols, between two users. I will explain in this section how it works. A user (Alice) creates two keys. One is the public key, which is available to everyone, and the other one is a secret key, which is stored in a secure place. Anyone who wants to communicate with Alice uses the public key to encrypt his/her message and then sends it to Alice, who can decrypt it using her private key. In practice, public keys are normally distributed through trusted authorities. The public and the secret keys are mathematically interconnected, so that it is theoretically possible to find out the secret key if someone has access to strong computational power.

Today the most widely used public cryptographic system is the RSA cryptosystem, whose name is the acronym of the inventors, Rivest, Shamir and Adleman [5]. It exploits the difficulty of factoring large numbers. In particular, Alice picks two large prime numbers, p and q, and makes their product public. Then, she chooses two large numbers e and d such that $(de-1)$ is divisible by $(p-1)(q-1)$. The public key consists of the product $N = pq$ together with the number e; N and d make the private key. With e, anyone can encrypt a message M by calculating $S = M^e \bmod N$, where S is the encrypted text, and $M^e \bmod N$ is the remainder of the Euclidean division of M^e by N. To decipher the encrypted message Alice uses her private key and calculates $M = S^d \bmod N$. This example shows that, in order to break the RSA system, one has to find the prime factors of N, which is currently a challenging computational problem for classical computers.

In last decades there have been several attempts to break an RSA system [6, 7]. In one of the most recent attack a 768 bit key was cracked by a network of classical computers [8]. In the future, when quantum computers will be available, it will be possible to decrypt an RSA system in polynomial time [9]. As a consequence, RSA may become obsolete. Hence, let us consider another type of cryptography to find out whether it offers more security.

1.1.2 Secret-key cryptography

The other branch of cryptography is called secret-key cryptography, also known as symmetric cryptography. In this case, the two users will use the same key to encrypt and decrypt a message. Therefore, sharing the key in a secure way *such that any eavesdropping attempt can be detected* is fundamental. One example of a classical cryptographic system is the aforementioned Verner cipher. The principle of this cipher is to add a random key to the message in order to establish secure communication between the two legitimate users. The encryption algorithm E can be written as [3]

$$E_K(M) = (M_1 + K_1, M_2 + K_2, ...M_n + K_n) \bmod 2, \tag{1.1}$$

where $M = (M_1, M_2, ...M_n)$ is the message in bits and $K = (K_1, K_2, ...K_n)$ is the secret key, generally consisting of random bits. To decipher the encrypted message it is sufficient to apply the same procedure as in (1.1), on $E_K(M)$. Applying the mod-2 operation twice is equivalent to the identity, hence

$$M = E_K(E_K(M)) = (M_1 + K_1 + K_1, M_2 + K_2 + K_2, ...M_n + K_n + K_n) \bmod 2. \tag{1.2}$$

In order to guarantee the security, this system must fulfill three requirements: (1) the length of the key must be the same as the length of the message; (2) the key must be purely random; and (3) it must be used only once (that is why it is also called one-time pad). But even if all the three requirements hold, the secret key has to be shared between the users who, in most cases, are located far apart from each other. The current practice for sharing secret keys involves using public-key cryptography whose security, as mentioned in Sec 1.1.1, is at risk. In the next section, I will show how quantum cryptography can help us with the key distribution problem by making it impossible for an eavesdropper to remain undetected if he/she acquires an unacceptable amount of information about the key.

1.2 Quantum cryptography

Quantum cryptography is the discipline that applies the principles of quantum mechanics to cryptography. The major aim of quantum cryptography is to devise protocols that are *information-theoretically secure* by exchanging quantum states. That means that the security is guaranteed by the laws of nature, as we understand them today, even if the adversary has unlimited computational power. The fundamental principle that makes quantum cryptography so special is the fact that, as stated by the measurement principle, any measurement in quantum mechanics may modify the state of the system. Therefore, if a potential eavesdropper tries to interfere with the quantum protocol, he/she would introduce errors in the system and would be eventually detected. Note that, quantum cryptography does not prevent the leakage of information during the communication but it enables us (in theory) to detect the presence of malicious parties.

The best known application in quantum cryptography is quantum key distribution (QKD), on which this thesis is focused. We will describe QKD in more detail in Sec. 1.2.1. However, quantum cryptography is not limited to QKD. In fact, it covers topics such as Bit commitment (BC), which is a cryptographic technique involving two parties, Alice and Bob, wherein Alice chooses an encoded bit of information and commits to it until a certain time at which she reveals it to Bob, without being able to change it [10]; Quantum fingerprint, which is a way to distinguish with high probability between two long strings of bit by comparing an exponentially shorter string associated with the long ones. This has found an application in a public-key digital signature scheme [11]; and Quantum data hiding, which aims at storing quantum or classical information in a bipartite quantum state shared by Alice and Bob, which can successively be recovered with high fidelity [12]. Other examples are the authentication of quantum messages [13], the encryption of quantum states [14], and the calculation of one-way functions useful for quantum computers [15]. Next, We describe QKD as the main application of interest in this thesis.

1.2.1 Quantum key distribution (QKD)

Quantum key distribution (QKD) is one of the main applications in quantum cryptography that makes use of laws of quantum physics to guarantee secure communications. It enables two users, usually named Alice and Bob, to produce a shared secret random bit string, which can be used as a key in cryptographic applications. QKD relies on the use of non-orthogonal quantum states. Its security follows from the Heisenberg uncertainty principle, which does not allow us to discriminate non-orthogonal states with certainty and without disturbing the measured system. In classical physics, it is possible to remain undetected as an eavesdropper, because information encoded into a certain property of a classical object may be obtained without altering the state of the object. In quantum cryptosystems, instead, the inviolability of the channel is tested by the use of non-orthogonal quantum states as information carriers.

It should be emphasized that quantum mechanics does not prevent possible eavesdropping; it only enables us to detect the presence of an eavesdropper, usually named Eve. If Eve attempts to listen in, that would unavoidably introduce discrepancies between Alice's and Bob's keys. Using post-processing techniques, these discrepancies can be found, and, if necessary, the key can be discarded and the users repeat the procedure to generate a new key.

There are several types of QKD protocols. One group relies on prepare-and measure schemes, such as BB84 [16] and B92 [17]. As the denomination of these protocols suggests, Alice sends a single photon encoded in a specific polarization, which corresponds to bit 1 or 0, and Bob measures it according to a determined orientation. They repeat this procedure several times until they share a sufficiently long string of bits. Then, Bob publicly announces the basis chosen for the measurement (sifting). They keep the bits if the bases chosen by Alice and Bob are identical. They discard it otherwise. If Eve attempts to intercept the photon sent by Alice, she will inevitably introduce some errors, which can be detected by estimating the discrepancy rate of sifted keys. Another class of protocols use a specific property of quantum mechanics, which does not exist in classical physics: entanglement. Entanglement is a non-classical property of physical systems. Two

systems are said to be entangled when their joint quantum state cannot be expressed by a linear combination of a tensor product states; see Sec. 2.4. The main examples of entanglement-based QKD are Ekert91 [18] and BBM92 [19] protocols. The goal of these protocols is to create correlated bits through certain measurements on entangled pairs shared by Alice and Bob. The security of an entanglement-based protocol relies on Bell's inequality [20], which concerns measurements made by observers on pairs of particles that have interacted and then separated. In particular, generalizing Bell's original inequality, John Clauser, Michael Horne, Abner Shimony and Richard A. Holt, introduced the CHSH inequality, [21] which puts classical limits on the sum of four correlations in Alice and Bob's experiment

$$-2 \leq S \leq 2 \tag{1.3}$$

where

$$S = E(a,b) - E(a^{'},b) - E(a,b^{'}) + E(a^{'},b^{'}) \tag{1.4}$$

where a and $a^{'}$ are detector settings on Alice side, b and $b^{'}$ on Bob side, and the four combinations being tested in separate experiments. The terms $E(a,b)$ etc. are the quantum correlations of the particle pairs, where the quantum correlation is defined to be the expectation value of the product of the "outcomes" of the experiment. The mathematical formalism of quantum mechanics predicts a maximum value for S of $2\sqrt{2}$, which is greater than 2, and CHSH violations are therefore predicted by the theory of quantum mechanics. Therefore, if an eavesdropper interferes with the entangled pairs shared by Alice and Bob, he will inevitably destroy the quantum correlation between the particles, leading to a non-violation of Bell's inequality.

In the original BB84 QKD protocol, one needs sources that emit only a single photon, which, today, are very hard to build. In the past few years several solutions have been suggested to overcome this limitation. It is now possible to use weak laser pulses that emit coherent-states instead of ideal single photons. The latter contain vacuum components and multi-photon components, which can be detrimental for the performance of a QKD protocol. Moreover, if the source emits more than one photon, the security of some QKD protocols can be compromised by the so called photon number splitting (PNS) attack [22], where

Eve can obtain information on the key without introducing any detectable error. However, it is still possible to share a secure key even with the possibility of a PNS attack, as shown in the GLLP security proof [23], although the secret key rate is significantly reduced (with PNS the rate scales as η_{ch}^2 as compared to η_{ch} for a single photon source, where η_{ch} is the transmittance of the quantum channel).

There are several solutions to the PNS attack. The most obvious is to use perfect single photon sources, but, as already mentioned, the current technology prevents us from such possibility. Another solution has been proposed in [24], where the BB84 protocol has been modified and in which the key rate scales as $\eta_{ch}^{3/2}$. One of the most promising solutions comes from using decoy state protocols [25–27], in which Alice send arbitrarily two different kinds of pulses: one used for extracting the key and the other one to detect the presence of an eavesdropper (decoy states). The latter can be used to prevent the PNS attack, since Eve cannot distinguish between the signal pulses and decoy pulses. I will explain more precisely how this protocol works in Ch. 2.

Along with the PNS attack, there is another group of attacks, which operate on the measurement devices located at users' sites [28–30]. Eve may be able to change the characteristics of the detectors by exploiting their flaws. Therefore, in addition to being costly, measurement devices can lead to compromising the security of a QKD protocol. A solution for this issue has been proposed recently in [1, 31]. Here, the authors suggest a QKD protocol, called measurement-device independent QKD (MDI-QKD), which delegates the measurement process to an untrusted party located in between Alice and Bob. In this way, the users do not need to know the characteristics of the measurement devices used. Moreover, it is possible to apply the decoy-state technique to this protocol, making it more resilient to malicious attacks. The users send BB84 decoy states to an untrusted party (Charlie), located, generally, in the middle. Charlie performs a Bell-state measurement (BSM), which creates a correlation between Alice and Bob's states. Later, he will announce the results of the measurements to Alice and Bob, who can deduce each others' bits. This protocol enables them to share the costs of measurement devices and can be considered as a prototype for a network system where many users can exchange secure keys through the BSMs located

in intermediate nodes. The security of this protocol is guaranteed by the reverse EPR protocol [31, 32].

As already mentioned, flaws in photodetectors can cause a range of attacks. The can also be detrimental for the performance of the protocol itself. In fact, a real implementation of a QKD protocol has to face some issues coming from the inefficiencies of the protocol's components, such as the detection efficiency, dark counts in photodetectors, imperfect sources and channel loss. All these inefficiencies limit the performance of a QKD protocol, which is commonly measured by considering the rate at which two users can share a secret key, called the secret key generation rate. In particular, the secret key generation rate between two distant sites will decrease exponentially with the length of the channel, due to noises and loss. Due to the no-cloning theorem [33], which forbids the creation of identical copies of an arbitrary unknown quantum state, we cannot duplicate the states, and, therefore, it would be challenging to implement QKD over arbitrarily long distances. In order to overcome this difficulty, quantum repeaters can be used as explained in the next Section.

1.3 Quantum repeaters

The principle of quantum repeaters relies on entanglement swapping operations, which consist of *teleporting* an entangled state from one location to another. The basic idea is to divide the transmission channel into many segments. First, entanglement is generated and, possibly, purified for each segment, and it is stored in quantum memories (QMs). Once entanglement is established over these elementary links, it is extended to a greater length by connecting two adjacent segments using entanglement swapping [34], which are performed by BSMs.

Depending on the nature of the entanglement swapping operations, we can distinguish between *deterministic* and *probabilistic* quantum repeaters. The first proposed quantum repeater protocol [35] belongs to the deterministic group, which performs BSMs through quantum gates in a deterministic way. Such devices are very demanding to implement, making this kind of protocol hard to implement. A perhaps more feasible approach, in the short term, was proposed by Duan and co-workers and called the DLCZ protocol [36], which is the first

probabilistic quantum repeater protocol. In such a protocol, the BSMs are performed simply by using a 50:50 beam splitter and photodetectors. This approach may be suitable for implementing quantum repeaters over up to around 1000 km.

In [36], authors, in order to store qubits, use ensemble-based quantum memories (QMs), which can be easier to implement than some other memory candidates. However, ensemble based QMs are strongly affected by multiple excitations, which can lead to the presence of more than one photon in the quantum channel, hence increasing the error rate. A quantum repeater protocol that addresses this issue is the single-photon source (SPS) protocol [37]. In this scheme, the QMs are loaded by the single photons sent by the users. Therefore, the problem of multiple-excitations in QMs is shifted to the one of having perfect single photon sources, which, at the present day, is still hard to solve.

1.4 Highlights and Outline

In this thesis, I will provide several examples of how we can use the quantum repeater idea to reach longer distances. I start with the analysis of the simplest of such systems, known as memory-assisted MDI-QKD [2], which is believed to require milder constraints on memory devices, and then proceed to consider several probabilistic quantum repeaters, in which the entanglement swapping part is achieved by partial BSMs performed at intermediate nodes. However, in real implementations there are several setup inefficiencies, which may affect strongly the performance of the protocol itself, such as the channel loss, detector efficiency, dark counts and multiple-excitations and decoherence in quantum memories. I will look at the performance of some quantum repeater setups by calculating analytically the secret key generation rate as the main figure of merit. I will include the effects of those inefficiencies and I will find the secret key rate as a function of several system's parameters, in order to estimate how they affect the system under examination.

The thesis is structured as follows:

- In Chapter 2, I will review the physical background and the relevant QKD protocols.

- In Chapter 3, I will discuss the effects of multiple excitations on a memory-assisted MDI-QKD protocol. I will show that the performance of the memory-assisted MDI-QKD protocol is adversely affected by such errors.
- In Chapter 4, I will study the effects of an imperfect SPS on the SPS protocol. By considering many sources of inefficiencies, I will determine the longest distance reachable for such a protocol in a quantum repeater setup up to three nesting levels. Then I will compare such a protocol with the DLCZ protocol.
- In Chapter 5, I will extend my analysis by considering an MDI-QKD setup combined with a quantum repeater scheme. This new quantum repeater scheme has the advantage of delegating the measurement process to an untrusted party; instead the end users are only equipped with encoder modules.
- In Chapter 6, I will draw the conclusions and present some topics for future research.

Chapter 2

Background

2.1 Introduction

This Chapter explains and summarizes the background required to understand the technical contribution of this thesis. I will review several QKD protocols that are relevant to the topics discussed in this thesis. I will describe the BB84 protocol [16] and the Ekert protocol [18], which are the first prepare-and-measure and entanglement-based protocols for exchanging secret keys, respectively. I will also introduce the decoy-state technique, which enables us to use weak laser pulses, rather than ideal single photons, in QKD. Next, I address long-distance quantum communications by describing deterministic [35] and probabilistic quantum repeaters [36]. The multiple-memory configuration, used to enhance the key rate, will be presented and I will model the main inefficiencies a QKD setup may have in real implementations.

2.2 BB84 protocol

QKD is best known by the protocol proposed by Charles Bennet and Gilles Brassard in 1984, coined as BB84, for exchanging secret information using non-orthogonal states. The security of BB84 protocol is guaranteed by quantum mechanics principles and it relies on the no-cloning theorem [33, 38] and the impossibility of perfectly distinguishing between non-orthogonal states, such that

Alice key bits	0	0	0	1	0	1	1
Alice's basis	×	+	+	×	×	+	+
Alice photon sent	↗	→	→	↖	↗	↑	↑
Bob's measurement basis	×	×	+	+	×	+	×
Photon polarization measured by Bob	↗	random	→	random	↗	↑	random
public discussion							
secret key	0		0		0	1	

Table 2.1: An example of the BB84 protocol

any attempt to intercept the signal will disturb the system. In BB84, Alice first generates a random key. In order to send her key bits to Bob, she randomly encodes single photons into two different bases. In the polarization encoding, she uses the rectilinear basis (+), represented by horizontal (→), and vertical (↑) polarizations or the diagonal basis (×), represented by 45°(↗) and 135°(↖) polarizations to encode her bits. An example of the BB84 operation is sketched in Table 2.1 and it works in the following way:

- Raw key exchange:
  - Alice randomly chooses a bit and encodes it in one of the two bases.
  - She sends the corresponding polarized photon to Bob.
  - Bob randomly chooses to measure the incoming photon in one of the two bases.
  - They repeat this procedure a sufficiently large number of times.
- Sifting:
  - They publicly declare which basis they have used.
  - They keep the bits when they have chosen the same basis (*sifted key)*, and discard the others.
- Postprocessing:

– They apply error correction and privacy amplification techniques to remove all discrepancies in their keys and to remove any information that might be have leaked to Eve during the procedure. The resulting key will be their final key.

To check the presence of an eavesdropper (Eve), Alice and Bob estimate the discrepancy rate, known as quantum bit error rate (QBER), between their sifted keys. If Eve attempts to intercept the key, she introduces some errors, therefore some of the Bob's sifted bits will differ from those of Alice even if the chosen bases coincide. If QBER is greater than a certain threshold value, Alice and Bob abort the protocol. The threshold depends on the employed post-processing technique and it ranges between 11% [39] and nearly 20% [40]. In principle, privacy amplification eliminates any partial Eve's information about Alice and Bob's key.

One of the main requirement of this protocol is that Alice has to send single-photons to Bob. Today, it is still hard to have a source that emits exactly one photon. More often, the available single-photon sources also produces multi-photon components, which can be used by Eve to perform certain attacks. In particular, in the photon-number splitting (PNS) attack, if, for instance, two photons are present in the channel, Eve can store one photon in a QM and let the other pass by. Then, during the sifting procedure, she can measure it in the same basis chosen by Bob. In this way she will gain some information on the secret key and the security of the protocol will be compromised. In the following section, I will describe a method that is resilient to the PNS attack even if we use weak laser pulses to simulate the required single photons in QKD.

2.3 Decoy-state method

The decoy state method was first proposed in [25] to minimize the effects of multi-photon components, which can be used by Eve to perform the PNS attack in the BB84 protocol. This method allows Alice to use a laser to send pulses to Bob, making the protocol more feasible for a practical implementation. The main feature of the decoy state idea is that Alice uses two different sets of signals:

the standard BB84 states, which are used for key generation only; and the decoy states, which are used to detect the presence of an eavesdropper. Let us see more precisely how the combination of the BB84 protocol and the decoy-state technique works. In the BB84 plus decoy-state protocol, Alice tunes her laser source intensity, and sends to Bob extra signals (decoy states) with different intensities (expected photon number), μ. The key point of this technique is that Eve cannot distinguish between states used for extracting the key and the decoy states. In fact, we have that

$$\begin{aligned} Y_i\,(decoy) &= Y_i\,(signal) \\ e_i\,(decoy) &= e_i\,(signal) \end{aligned} \tag{2.1}$$

where Y_i is the yield, i.e., the conditional probability of a detection on Bob's side, given that Alice sends i photons; and e_i is the QBER, i.e., the ratio between the probability of an erroneous bit assignment and the probability of successful bit transmission, when Alice sends i photons.

In order to reduce the amount of necessary privacy amplification, and, therefore, to increase the secure communication distance, Alice and Bob need to estimate Y_1 and e_1. This can be achieved in the infinite decoy protocol [26] for example, by sending an infinite number of decoy states. For each intensity μ, we obtain

$$\begin{aligned} Q_\mu &= \sum_{i=0}^{\infty} Q_i \\ E_\mu Q_\mu &= \sum_{i=0}^{\infty} e_i Y_i \tfrac{\mu^i}{i!} e^{-\mu} \end{aligned} \tag{2.2}$$

where Q_μ is the overall gain, i.e., the sum of gain parameters of i photon states Q_i, given by:

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{2.3}$$

and E_μ is the overall QBER for all pulses with intensity μ. If we use infinitely many intesities we can in principle estimate Q_1 and e_1, accurately. However, it can be shown that one or two decoy states are sufficient for practical purposes [27].

The procedure for the decoy-state QKD is as follows [41]:

- Alice sends decoy and signal states to Bob, who measures them in the two conjugate bases.
- Alice announces the pulses used for decoy states and they determine all the gains of signals and of decoy states.
- They compare all bases used for the decoy states to determine the QBER.
- They perform error correction and privacy amplification to find the final secret key.

In [26] authors derive the key rate formula when the decoy-state method is applied to the BB84 scheme. In the limit of infinitely many decoy states and infinitely long keys, the key rate is lower bounded by:

$$R \geq q \left\{ Q_1 \left[1 - h\left(e_1 \right) \right] - Q_\mu f h\left(E_\mu \right) \right\}, \tag{2.4}$$

where q is the basis reconciliation factor, f is the error correction inefficiency, and h is the binary entropy, $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$. In the BB84 protocol $q = 1/2$ because half of the time Alice and Bob disagree on the basis chosen. If one uses the efficient BB84 protocol [42] we can approximate q by 1. Moreover, they show that it is possible to reach much longer distances (about 140 km) by applying this technique than what one could do at the time without using decoy states [26]. We will use (2.4) to evaluate the secret key rate in Chapters 3 and 5.

As shown in this section, it is possible to apply the decoy-state method when signals are under the control of the users. In the next section we will present a new type of protocol to exchange secret keys, where the source is placed between Alice and Bob and, therefore, it is not possible to apply the decoy-state method. Nevertheless, the following QKD protocol has had a big importance since its appearance and, as the BB84 protocol, it represents a milestone for many protocols that came after.

2.4 Ekert protocol

In 1991 Ekert proposed a different type of protocol based on entangled states [18]. Entanglement represents a correlation between two or more properties (such as spin, polarization, etc) of two physical systems in such a way that is impossible to express the entangled state as a tensor product, which is a characteristic of separable states. In particular, let H_1 and H_2 be finite-dimensional Hilbert spaces, a density matrix ρ acting on $H_1 \otimes H_2$ is separable if there exist $p_i \geq 0$ and two sets of mixed states of the respective subsystems $\{\rho_1^i\}$ and $\{\rho_2^i\}$, such that

$$\rho = \sum_i p_i \rho_1^i \otimes \rho_2^i, \tag{2.5}$$

where $\sum_i p_i = 1$. When it is not possible to express ρ as in Eq. (2.5) then ρ is an entangled state.

In the following I will briefly describe how this protocol works. In the Ekert protocol, a source of entangled photon pairs is located between Alice and Bob and it emits polarized photons in the singlet states:

$$|\varphi\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle \right). \tag{2.6}$$

Alice and Bob will pick one of the three coplanar axes to do a polarization measurement. The orientations of the analyzers of Alice and Bob, which represent a basis, are given respectively by:

$$\begin{aligned} \varphi_A &= 0°,\ 45°,\ 90° \\ \varphi_B &= 45°,\ 90°,\ 135°. \end{aligned} \tag{2.7}$$

Whenever the bases of Alice and Bob are the same, they will share an anticorrelated state, meaning Alice will measure horizontal polarization and Bob vertical polarization or vice versa. If the bases chosen are different the outcomes will be random.

This procedure is repeated many times until they share a string of bits. Then, as in the BB84 protocol, they publicly announce which basis they have used, and divide the measurements into two groups depending on which orientation they have chosen. If they have used the same orientation (first group), then the results of these measurement will be used to extract the key. They will use the results

of the second group to test the Bell inequality [20]. Any classical system satisfies the Bell inequality, while, it is violated by entangled states. If Eve intercepts entangled states, she demolishes the quantum correlation between the two subsystems and the Bell inequality holds. In this case Alice and Bob can detect the presence of Eve and the protocol is aborted.

The Ekert protocol launched a new type of QKD protocols, which rely on using entangled photons, called *entanglement-based* QKD protocols. One of them is the BBM92 protocol [19], which has been proposed by Bennett, Brassard and Mermin shortly after the Ekert protocol and can be regarded as an entanglement-based version of the BB84 protocol. The same idea was behind alternative QKD protocols such as the time-reversed EPR scheme [31, 32], and the device-independent QKD protocol [43]. An experimental implementation of a modified version of the BB84 scheme that uses entangled photons has been made in [44]. However, both prepare-and-measure and entanglement-based protocols are affected by a range of attacks performed on the measurement devices [45, 46], which might compromise the security of the protocol itself. In the next section, I will present a protocol, called measurement-device-independent QKD (MDI-QKD), which is not affected by such attacks. In such a protocol, the measurement process is delegated to an untrusted party, by using entanglement swapping and the time-reverse EPR protocol. It has also the practical advantage of using the decoy-state technique. In the next section, I will describe the main features of such a protocol.

2.5 MDI-QKD protocol

MDI-QKD [1] is a clever protocol that combines BB84 source states with the time-reversed EPR protocol [47] in order to remove all side-channel attacks on the measurement modules. In this protocol practical weak coherent pulses can be used as sources, and the decoy state technique, which was described in section 2.3, is applied; see Fig. 2.1. This allows us to reach further distances as compared to the decoy-state BB84 scheme [1].

The MDI-QKD protocol works as follows: Alice and Bob both prepare their states in one of the four BB84 states by choosing a rectilinear or diagonal basis.

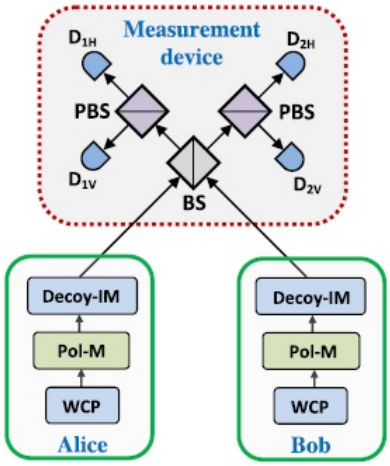

Figure 2.1: MDI-QKD scheme with polarization encoding [1].

They send their state to a middle site where a partial BSM is performed, projecting the states to one of the Bell states by an untrusted party, called Charlie. Charlie announces which detectors click. Alice and Bob repeat this procedure several times. Later, over a public channel, they compare the bases chosen, and they keep the cases when the bases chosen are the same, otherwise they discard them. The security of such a protocol follows that of the time-reversed EPR QKD protocol in [31, 32, 48]. Because of relying on the reverse-EPR protocol [47], Charlie does not need to be trusted. The main achievements of the MDI-QKD protocol can be summarized as follows:

- it enables the two users to use laser sources for generating quantum states, hence low-complexity modules are needed for the end users.
- it creates correlated pairs of the pulses sent through a BSM performed by an untrusted party. The BSM operation effectively produces an entanglement swapping operation, similar to that of quantum repeaters.
- it removes all side-channel attacks on detector modules.

We will see how the above features will make this protocol a natural candidate for the access part of a quantum communication networks as will be discussed in Ch. 5.

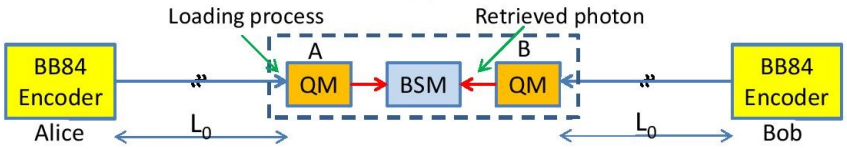

Figure 2.2: Memory-assisted MDI-QKD with heralding memories.

In the following we describe an MDI-QKD protocol embedded with quantum memories. This can be considered as an intermediate step towards the implementation of quantum repeaters.

2.6 Memory-assisted MDI-QKD

An improved version of the MDI-QKD scheme has been presented in [2]. With such a scheme, authors aim at improving the rate-versus-distance performance by introducing QMs just before the BSM performed in an MDI-QKD setup. Figure 2.2 shows how this scheme works. Alice and Bob send BB84 encoded states to a middle site where there are QMs. At each round, each QM tries to store the incoming pulse. Once both memories are loaded, the QM's states are retrieved and a BSM on the resulting photons is performed. They follow the same steps to share a key as in the MDI-QKD protocol. The main advantage of this scheme relies on the fact that the requirements for the QMs are less demanding than the ones used for a probabilistic quantum repeater protocol, by relaxing the condition of having long coherence times for QMs. Therefore, this may represent a valid middle-step toward the future implementation of quantum repeaters. Moreover, in [2], authors show that if fast memories with large storage-bandwidth products are used, it is possible to beat the conventional MDI-QKD systems with no memories. We can meet this requirement by using ensemble-based QMs. Writing times as short as 300 ps and bandwidths on the order of GHz have been reported for such memories [49, 50]. We will see in Ch. 3 how an MDI-QKD system with ensemble-based QMs will perform. Ultimately, the way to reach further distances is given by using quantum repeater protocols, as explained in the next section.

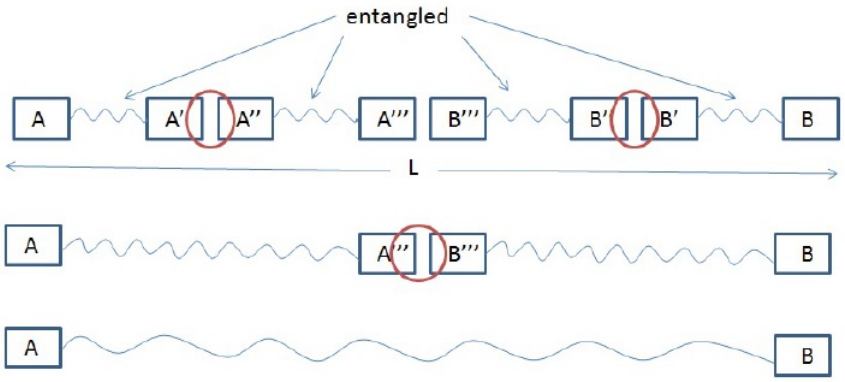

Figure 2.3: Entanglement swapping.

2.7 The principles of quantum repeaters-operation

Entanglement purification and connection of entangled pairs through entanglement swapping [51] are the main tools required for a quantum repeater. We will not discuss entanglement purification in here. What is important to know is that one can generate entangled pairs with a certain fidelity, starting from pairs with a lower initial fidelity via reasonably few purification steps. The other ingredient of a quantum repeater is the entanglement swapping procedure [51], which is shown in Fig. 2.3. Alice (A) and Bob (B) are separated by a distance L. They aim at sharing an entangled pair over such a distance. First, the quantum channel is split into smaller segments and entanglement is generated over each elementary link, such that $A - A^{'}$, $A^{''} - A^{'''}$, $B^{'''} - B^{''}$, and $B^{'} - B$ will have entangled pairs. Then, BSMs, labeled with the red circles in Fig. 2.3, are performed at the intermediate nodes. We end up with two new entangled pairs, i.e., $A - A^{'''}$ and $B^{'''} - B$. Once more, we perform a BSM on the intermediate link and we, finally, obtain a long-distance entangled pair between A and B. We can use this entangled pair to perform a measurement for sharing a key, as explained in Sec. 2.4.

Quantum memories are the fundamental building block of a quantum repeater. The reason for that comes from the probabilistic nature of entanglement distribution as it often relies on the transmission of single photons. In Fig. 2.3, we cannot perform entanglement swapping over $A^{'} - A^{''}$ unless we have established

entanglement over both $A - A^{'}$ and $A^{''} - A^{'''}$. Without having memories, we cannot guarantee the existence of entangled states over both links. With memories, however, we can successively attempt to create entanglement over each link independently. Whenever our attempt succeeds, we store the entangled state in QMs and wait for the other side to succeed as well.

The original quantum repeater protocol proposed in [35] is a deterministic quantum repeater, i.e., the BSM is performed in a deterministic way through quantum gates. This protocol contains "entanglement purification" steps that allow one to purify, in principle, the effects of imperfect operations. However, the implementation of such protocols is very demanding (for example the depolarization probabilities have to be very low [35]) and the use of a quantum gate makes it infeasible in the imminent future. Note that in the most recent proposals for quantum repeaters, the need of QMs as storage devices has been eliminated [52, 53].

As an alternative, one can use probabilistic quantum repeaters, which rely on post-selection techniques to alleviate some of these requirements. They are probabilistic because the BSM is performed in a probabilistic way by using only linear optics elements and photodetectors. The main example of the latter is the scheme proposed by Duan, Lukin, Cirac, and Zoller [36], which we refer to by DLCZ throughout this thesis and we will describe in more detail in Sec. 2.9. The key advantage of the DLCZ protocol is an inherent self-purification scheme, which, in practice, makes it suitable for QKD applications. That is, we may be able to implement such systems over moderately long distances in a nearer future. This is one of the key topics studied in this thesis by looking carefully at how different imperfections in the systems can change the overall system performance.

Different schemes for probabilistic quantum repeaters have been proposed over the past few years, which rely on the DLCZ idea and try to improve its performance. In [54], authors describe a protocol where entanglement swapping is based on two-photon detections, which leads to a constant vacuum component in the created state. Then, in [55] an improvement has been reported regarding enhanced robustness against phase fluctuations in the channel [56]. A modification of the DLCZ protocol based on photon pairs and multimode memories is

reported in [57]. A protocol based on single-photon sources (SPS), which leads to an enhanced rate compared to the DLCZ protocol is also reported in [37].

In this thesis, we will provide a comparative analysis of the above schemes when used for QKD. In particular, we evaluate one important parameter for QKD, i.e., its secure key generation rate. This parameter will measure the performance of the setups we are analyzing. There might be different lower bounds for the key rate, depending on which security proof we are considering. For example, when the decoy-state method is used, the key rate is given by Eq. (2.4). Moreover, in a quantum repeater setup we can have a faster key rate if more QMs are used at each link. We will describe in more detail how it is possible to reach faster rates in the next section.

Recently, two deterministic quantum repeater protocols have been proposed. In [52], authors describe a quantum repeater protocol that directly transmits qubits over optical fibers using error correction schemes. This protocol is similar to how we communicate classical data and it offers high exchange rate of quantum data. However, it requires highly demanding quantum processing, which makes its implementation very challenging. Moreover, it requires very efficient interface between light and matter. Another protocol with no QMs has been proposed in [53]. Here, authors consider an all photonic quantum repeater protocol based on flying qubits, in which QMs in the repeater nodes are substituted by cluster states. The performance of this protocol is very high but it requires large cluster states and very efficient single photon sources. This thesis is mostly focused though on probabilistic repeaters, which have a better chance to be implemented in the near future.

2.8 Multiple-memory configuration

In the previous section we described the principles of a quantum repeater setup and, in particular, of a probabilistic quantum repeater protocol. We highlighted that in such a setup we need QMs to store an entangled pair for a sufficiently long time in order to perform a BSM with an adjacent entangled pair. In order to increase the chances of having such entangled pairs ready to be used, we can add more memories at each memory site. This will increase the rate we can share a

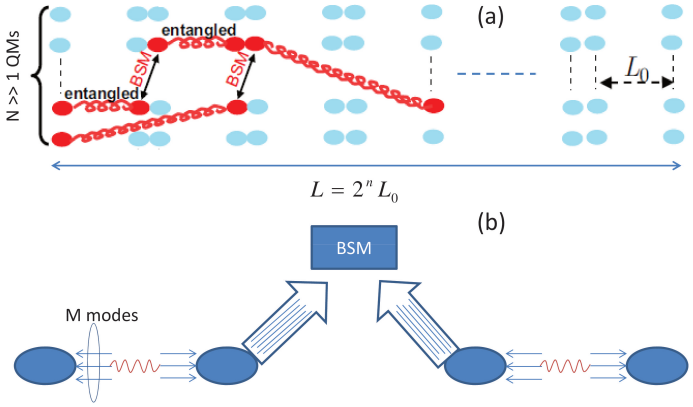

Figure 2.4: (a) A quantum repeater with multiple quantum memories per node. At each round, we employ entanglement distribution protocol to entangle any unentangled memory pairs over shortest links. At any such cycle, we also match up entangled pairs at different stations to perform Bell-state measurements (BSMs). (b) A quantum repeater with multimode memories. In each round, we apply our entanglement distribution scheme on all M modes, until one of them becomes entangled. BSM will be followed as soon as entanglement is established on both sides.

secret key. We consider the multiple-memory configuration shown in Fig. 2.4(a) along with the cyclic protocol described in [58]. In this protocol, in every cycle of duration L_0/c, where L_0 is the length of the shortest segment in a quantum repeater, and c is the speed of light in the channel, we try to entangle any unentangled pairs of memories at distance L_0. We assume our entanglement-distribution protocol succeeds with probability $P_S(L_0)$. At each cycle, we also perform as many BSMs as possible at the intermediate nodes. The main requirement for such a protocol is that, at the stations that we perform BSMs, we must be aware of establishment of entanglement over links of length $l/2$ before extending it to l (*informed* BSMs). We use the results of [58] to calculate the generation rate of entangled states *per memory* in the limit of infinitely many memories.

Suppose that at the initial time 0 there is no entanglement in the scheme. Then, at time T_0, we establish, on average, NP_S entangled pairs over the elementary length L_0, where N is the number of memories used in each bank. After this stage, we perform the BSMs of the first nesting level, which succeeds with probability $P_M^{(1)}$ and we produce $NP_SP_M^{(1)}$ entangled pairs over a length $2L_0$. By

following this procedure, for a setup with n nesting levels, at time L/c we will have on average $N_{\text{ent}} = NP_S P_M^{(1)} ... P_M^{(n)}$, where $P_M^{(i)}$ is the BSM success probability for nesting level i, over the total distance L. Now, for $N \to \infty$, we have that the average number of entangled states generated per cycle over distance L, in the steady state, is upper bounded by N_{ent}. This is due to the fact that the protocol repeats the same procedure at times T_0, $2T_0$ and so on, to the pairs which are not yet entangled. This implies that at time $L/c + T_0$ we can overestimate the number of entangled pairs by N_{ent}, assuming that the number of free memories at time T_0 is N. If we want to find a rate that takes into account the cost, specified by the number of memories used, we can simply divide that upper bound by the total number of memories per unit of time. This normalized rate is given by [58]:

$$\begin{aligned} R_{\text{ent}} &= \tfrac{N_{\text{ent}}}{N 2^{n+1} T_0} \\ &= P_S (L/2^n) P_M^{(1)} P_M^{(2)} ... P_M^{(n)} / (2L/c). \end{aligned} \tag{2.8}$$

We use the following procedure, in the forthcoming Chapters, to find the secret key generation rate of the setup in Fig. 2.4(a). For each entanglement distribution scheme, we find $P_S\left(L_0\right)$ and relevant P_M probabilities to derive $R_{\text{ent}}\left(L\right)$. We then find the sifted key generation rate by multiplying $R_{\text{ent}}\left(L\right)$ by the probability, Q_{click}, that an acceptable click pattern occurs upon QKD measurements. Finally, the ratio between the number of secure bits and the sifted key bits is calculated using the Shor-Preskill lower bound [39]. In the limit of an infinitely long key, the secret key generation rate per logical memory is lower bounded by

$$R_{\text{QKD}}\left(L\right) = \max(R_{\text{ent}}\left(L\right) Q_{\text{click}} \left[1 - 2\, h\left(E_Q\right)\right], 0), \tag{2.9}$$

where E_Q denotes the QBER, and $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$, for $0 \leq x \leq 1$.

2.8.1 Multimode configuration

Another way to speed up the entanglement generation rate is via using multi-mode memories [59]. As can be seen in Fig. 2.4(b), in this setup, we only use one physical memory per node but each memory is capable of storing multiple modes. In each round, we attempt to entangle memories at distance L_0 by entangling,

at least, one of the existing M modes. Once this occurs, we stop entanglement generation on that leg and wait until a BSM can be performed. For readout, all modes must be retrieved in order to perform BSMs or QKD measurements on particular modes of interest. In effect, this scheme is similar to that of Fig. 2.4(a), except that entanglement distribution is not sequentially applied to unentangled modes. The success probability for entanglement distribution between the two memories is, however, M times that of Fig. 2.4(a). One can show that, the generation rate of entangled states per mode is approximately given by $\left(\frac{2}{3}\right)^n R_{\text{ent}}(L)$ [60].

We can apply the multiple-memory configuration to the quantum repeater protocols we have mentioned in the previous sections. The first probabilistic quantum repeater protocol based on ensemble QMs is the aforementioned DLCZ protocol. In the following section, we will describe how it works and the physics behind it.

2.9 Quantum repeater protocols

In this section I will review two probabilistic schemes for quantum repeaters that we use in this thesis.

The first scheme is the original DLCZ scheme [36], which will be used as a reference in my thesis. We consider this protocol because this scheme relies on devices that are within the reach of current experimental technology. This makes it a very good candidate for a possible implementation in the near future. The main drawback of such a protocol stems from the use of ensemble-based QMs. In fact, they are strongly affected by multiple-excitations, which can cause errors as we explain in the following sections. The second protocol we consider is the single-photon scheme proposed in [37], which I refer to by the SPS scheme. Here, the main idea is to use single-photon sources to overcome errors caused by multiple-excitations. However, it is very common that such sources produce more than one photon. Therefore, the problem has been shifted from multiple-excitations in QMs to multiple-photon components in sources that are supposed to emit single photons. First, let us describe in more detail these two protocols.

Then, we will examine under which conditions, the SPS protocol outperforms the DLCZ protocol in Ch. 4.

2.9.1 DLCZ entanglement-distribution scheme

The DLCZ entanglement distribution scheme works as follows; see Fig. 2.5(a). Ensemble memories A and B, at distance L, are made of atoms with Λ-level configurations. They are all initially in their ground states. By coherently pumping these atoms, some of them may undergo off-resonant Raman transitions that produce Stokes photons [36]. The resulting photons are sent toward a 50:50 beam splitter located at $L/2$ between A and B. If, ideally, only one photon has been produced at one of the ensembles (for which we have to limit the excitation probability, p_c, to very small values), one and, at most, only one, of D_1 and D_2 clicks. According to the DLCZ protocol, if one of the two detectors in Fig. 2.5(a), clicks, A and B are heralded to be ideally in one of the Bell states $|\psi\rangle_{AB} = (|10\rangle \pm |01\rangle)/\sqrt{2}$, where $|0\rangle_J$ is the ensemble ground state and $|1\rangle_J = S_J^\dagger |0\rangle_J$ is the symmetric collective excited state of ensemble $J = A, B$, with $S_J^\dagger$ being the corresponding creation operator [36]; see next subsection for more detail. This entanglement can further be extended to long distances using entanglement swapping [36, 57].

An important feature of such collective excitations is that they can be read out easily by converting their states into photonic states as explained in the next subsection. These states will be used in the entanglement swapping operation, which works in the following way. Let us assume we want to share an entangled pair over a distance L. We first split the channel into two parts and we establish entanglement over each elementary link of length $L/2$. We now retrieve the states of the middle-site QMs by driving them with a laser pulse to, followed by a BSM measurement on the released photons. A click on one photodetector will project the final state to a maximally entangled state of the QMs separated by a distance L. This protocol has also the property of some built-in entanglement purification against dark-count noises and that there has been recently experimental progress to implement such systems [37]. This property relies on the fact that, in the presence of noise, the state we produce will be not a pure entangled state, but

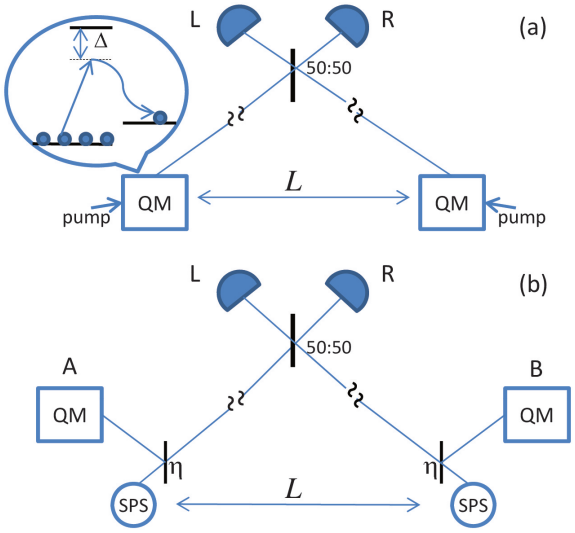

Figure 2.5: Schematic diagram for entanglement distribution between quantum memories (QMs) A and B for (a) the DLCZ protocol and (b) the SPS protocol. In both cases, we assume QMs can store multiple excitations. Sources, memories and detectors are represented by circles, squares and half-circles, respectively. Vertical bars denote beam splitters. In both protocols the detection of a single photon ideally projects the two memories onto an entangled state.

it will be a mixture state with a vacuum component. This vacuum component introduces some errors that affect the key rate. However, each time we swap entanglement, we require a detector click, which is mainly because of the presence of a photon. This removes, to some good extent, the added vacuum noise. This built-in entanglement purification is an essential tool of this setup.

The fundamental source of error in the DLCZ scheme is the multiple-excitation effect, in which more than one Stokes photon are produced [61]. This effect can be attenuated, to some extent, by using photon-number resolving detectors (PNRDs) rather than non-resolvig photodetectors (NRPDs) [61]. When we have one click at a PNRD, it means that exactly one photon is observed, whereas one click at an NRPD implies that *at least* one photon has been detected. In Chapter 4, we consider both types of detectors and compare the system performance in various scenarios.

Furthermore, even if the two ensembles emit at most one photon each, there is a probability p_c^2 that two photons will be emitted in total. If this happens and if one photon is lost during its transmission through the fiber or because

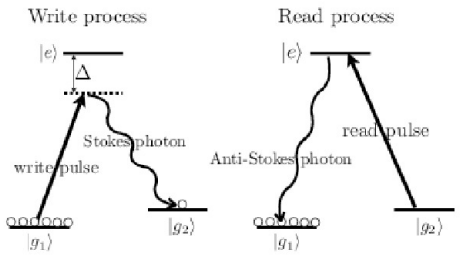

Figure 2.6: Level scheme for the creation of collective atomic excitations in atomic ensembles via spontaneous Raman emission (write process) and for their readout (read process), as proposed in the DLCZ protocol.

of the failure of the detector, the detection of a single photon in one of the two detectors generates the state $|11\rangle_{AB}$, which means that the two memories are full [37]. This state is not the desired entangled state and introduces errors and gives a low fidelity of the created entanglement. Therefore, one has to pump memories with low emission probability $p_c \ll 1$. In this way the probability to get simultaneous emissions at A and B is sufficiently small, but this limits the achievable distribution rate of entangled states [61]. We will see how the SPS protocol deals with $|11\rangle_{AB}$ term in Sec. 2.9.3. Before that, let us review the underlying physics that characterizes ensemble-based memories.

2.9.2 Ensemble-based memories: underlying physics

In this Subsection I briefly describe the underlying physics that explains the operation of ensemble-based memories. Let us consider an ensemble of N three-level systems with two quasi-stable states $|g_1\rangle$ and $|g_2\rangle$, with the energy of $|g_2\rangle$ slightly higher than that of $|g_1\rangle$, and an excited state $|e\rangle$, where all N atoms are initially in the state $|g_1\rangle$. An off-resonant laser pulse on the $|g_1\rangle - |e\rangle$ transition (*write* pulse) leads to the spontaneous emission of a Raman photon on the $|e\rangle - |g_2\rangle$ transition. I refer to this photon as the Stokes photon. As a result of the detection of the Stokes photon, since no information is revealed about which atom it comes from, we have an atomic state that is in a coherent superposition of all the possible terms with $N-1$ atoms in the $|g_1\rangle$ and one atom

in $|g_2\rangle$, i.e.,

$$\frac{1}{\sqrt{N}}\sum_{k=1}^{N} e^{i(\mathbf{k}_w-\mathbf{k}_S)\cdot\mathbf{x}_k}|g_1\rangle_1|g_1\rangle_2\ldots|g_2\rangle_k\ldots|g_1\rangle_N, \tag{2.10}$$

where $\mathbf{k}_w$ is the wave vector of the write laser, $\mathbf{k}_S$ is the wave vector of the detected Stokes photon, and $\mathbf{x}_k$ is the position of the kth atom. In practice the amplitudes of the terms can differ, depending on the laser profile and the shape of the atomic ensemble [37].

A remarkable feature of such collective excitations is that they can be read out efficiently by converting them into single photons that propagate in a well-defined direction, thanks to collective interference [37]. Resonant laser excitation of such a state on the $g_2 - e$ transition (the *read* pulse) leads to a similar state with $N-1$ atoms in g_1 and one excitation in e, but with an additional phase terms $e^{i\,\mathbf{k}_r\mathbf{x}_k^{'}}$, where $\mathbf{k}_r$ is the wave vector of the read laser and $\mathbf{x}_k^{'}$ is the position of the kth atom at the time of readout (which can be different from its initial position $\mathbf{x}_k$ if the atoms are moving).

All the terms in this state can decay to the initial state $|g_1\rangle^{\otimes N}$ while emitting a photon on the $e-g_1$ transition, i.e. the anti-Stokes photon. The total amplitude for this process is then proportional to

$$\sum_{k=1}^{N} e^{i(\mathbf{k}_w-\mathbf{k}_S)\cdot\mathbf{x}_k}e^{i(\mathbf{k}_r-\mathbf{k}_{AS})\cdot\mathbf{x}_k^{'}}, \tag{2.11}$$

where $\mathbf{k}_{AS}$ is the wave vector of the anti-Stokes photon [37].

The conditions for constructive interference of the N terms in this sum depend on whether the atoms are moving during the storage. If they are at rest ($\mathbf{x}_k = \mathbf{x}_k^{'}$ for all k), then there is constructive interference whenever the phase matching condition $\mathbf{k}_S + \mathbf{k}_{AS} = \mathbf{k}_w + \mathbf{k}_r$ holds, leading to a large probability amplitude for the emission of the anti-Stokes photon in the direction given by $\mathbf{k}_w + \mathbf{k}_r - \mathbf{k}_S$ [37]. For atomic ensembles that contain many atoms, emission in this one direction can totally dominate all the other directions [37]. If the atoms are moving, there can still be constructive interference, with the following conditions: $\mathbf{k}_S = \mathbf{k}_w$ and $\mathbf{k}_{AS} = \mathbf{k}_r$, which basically removes the dependence on x_k. Note that, as regards the emission of the Stokes photon, there is no preferred direction of emission.

This is due to the fact that the emission of a photon by different atoms leads to orthogonal final states and, therefore, the total emission probability for the Stokes photon is given by the sum of the emission probability of each single atom, without leading to a preferred direction of emission [37]. This would naturally result in low excitation probabilities in specific direction of interest.

2.9.3 SPS entanglement-distribution scheme

The SPS protocol, proposed in [37], aims at reducing multi-photon errors and, in particular, terms of the form $|11\rangle_{AB}$ by using single-photon sources. The architecture of this scheme is presented in Fig. 2.5(b). The two remote parties each have one single-photon source and one memory. In the ideal scenario, each source produces exactly one photon on demand, and these photons are sent through identical beam splitters with transmission coefficients η. It can be shown that the state shared by the QMs after a single click on one of the detectors in Fig. 2.5(b) is given by [37]

$$\eta^2|0\rangle_{AB\,AB}\langle 0| + (1-\eta)^2\,|\psi_\pm\rangle_{AB\,AB}\langle\psi_\pm| \tag{2.12}$$

which has our desired entangled state plus a vacuum component. The latter, at the price of reducing the rate, can be selected out once the above state is measured at later stages (self purification) [36, 61].

In the following two sections I will describe the main analytical tools I use to analyze the SPS protocol and the quantum repeater setups.

2.10 Butterfly module

As pointed out in the previous sections, QKD repeater setups are affected by different sources of inefficiency, which are modeled by fictitious beam splitters. Consequently, there are certain structures that appear here and again in our analysis of different systems. One of those common structures is our so-called butterfly module shown in Fig. 2.7. The butterfly module is a two-input two-output building block consisting of five beam splitters with generic transmission coefficients η_0, η_1, η_2, η_3 and η_4. What we are commonly interested in is to

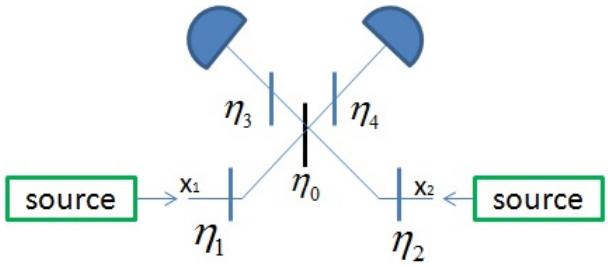

Figure 2.7: A generic butterfly module, represented by $B^{x_1x_2}_{\eta_0\eta_1\eta_2\eta_3\eta_4}$, where η_0, η_1, η_2, η_3, η_4 are transmittivities and x_1 and x_2 are the input modes shown in the figure

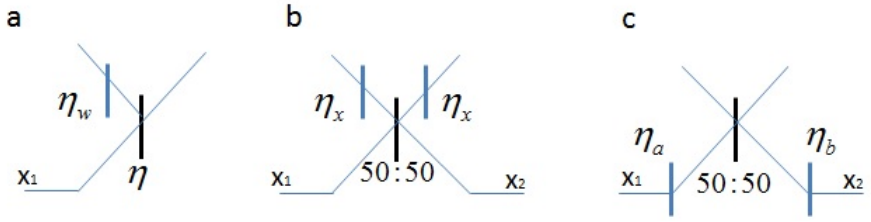

Figure 2.8: Three generic butterfly modules we use in this thesis.

find the input-output relationship from the source to before photodetector units. With input modes labeled by x_1 and x_2, a generic butterfly module is denoted by the operator $B^{x_1x_2}_{\eta_0\eta_1\eta_2\eta_3\eta_4}$.

Figure 2.8 shows three different configurations of the butterfly module that we will use throughout this thesis. In Fig. 2.8(a), η_0 and η_3 can assume generic numerical values. In Figs. 2.8(b) and 2.8(c), $\eta_0 = 1/2$ representing a 50:50 beam splitter. The butterfly module of Fig. 2.8(b) represents a symmetric setup where $\eta_1 = \eta_2$, $\eta_3 = \eta_4$ and $\eta_x = \eta_1\eta_4$. Instead the butterfly module in Fig. 2.8(c) represents an asymmetric setup, where $\eta_3 = \eta_4$ but $\eta_1 \neq \eta_2$. We use well-known models for beam splitters [62] to find output density matrices for relevant input states to a generic butterfly module. In Appendices A and B, we find the relevant input-output relationships for the states of interest. We use Maple 15 to simplify some of our analytical results.

2.11 Measurement operators

In our analysis of QKD setups and quantum repeaters, we often have to do measurements by photodetectors. This process can be modeled by applying proper measurement operators considering whether photon number resolving detectors (PNRDs) or non-resolving photodetectors (NRPDs) are used. For example, for a "click" on detector D_1, and no click on a detector D_2, each with a dark count rate of d_c, the explicit form of the measurement operator is given by

$$M^R_{D_1D_2} = (1-d_c)[|1\rangle_{D_1D_1}\langle 1| \otimes |0\rangle_{D_2D_2}\langle 0| \; + d_c|0\rangle_{D_1D_1}\langle 0| \otimes |0\rangle_{D_2D_2}\langle 0|] \;, \tag{2.13}$$

if we use PNRDs and we are interested in detecting exactly one photon, and

$$M^{NR}_{D_1D_2} = (1-d_c)[(I_{D_1} - |0\rangle_{D_1D_1}\langle 0|) \otimes |0\rangle_{D_2D_2}\langle 0| + d_c|0\rangle_{D_1D_1}\langle 0| \otimes |0\rangle_{D_2D_2}\langle 0|] \;, \tag{2.14}$$

if we use an NRPD, where we cannot distinguish between one or more photons. Here, I_{D_1} denotes the identity operator for the mode entering the detector D_1, and d_c is the dark-count rate per gate width per detector. The expression of the measurement operator of eqs (2.13) and (2.14) derives from the conditional probability of two independent events:

$$P(A \cup B) = P(A) + P(B)\,, \tag{2.15}$$

where A and B in Eq. (2.15) correspond to the case of one click in detector D_1 and no click in detector D_2, respectively. Note that a click can be produced either by a real photon or by a dark count event. The operators in Eqs. (2.13) and (2.14) take into account both sources of click. When applied to a density matrix, the operator of Eq. (2.13) projects the density matrix to the subspace of modes D_1 having one photon and D_2 having no photon ($|1\rangle_{D_1D_1}\langle 1| \otimes |0\rangle_{D_2D_2}\langle 0|$) joined with the subspace of modes D_1 and D_2 having both no photons ($|0\rangle_{D_1D_1}\langle 0| \otimes |0\rangle_{D_2D_2}\langle 0|$]). In Ch. 4 we use both operators. In all other cases we use only the operator of Eq. (2.14), which is of more practical relevance.

Memory writing efficiency, η_w
Path loss, η_{ch}
Detection efficiency, η_D
Memory retrieval efficiency, η_r
Dark count per pulse, d_c
Attenuation length, L_{att}
Speed of light, c
Decay (dephasing) time constants, T_1 (T_2)
Double-photon probability, p
Error correction inefficiency, f

Table 2.2: List of common parameters used in this thesis

2.12 List of parameters used

In Table 2.2 the main parameters of interests used in this thesis are listed. The inefficiencies considered for QMs are the writing efficiency, η_w, the reading or retrieval efficiency, η_r, the amplitude decay time, T_1 and the dephasing time T_2. Regarding the measurement devices we consider the detection efficiency, η_D, and the dark count, d_c. The path loss for a channel with length l is given by

$$\eta_{\text{ch}}(l) = \exp\left(-l/L_{\text{att}}\right), \tag{2.16}$$

with $L_{\text{att}} = 25$ km for an optical fiber channel. We also consider an imperfect SPS which emits two photons with probability p.

2.13 The contribution of this thesis

In Ch. 1, we described the main features of QKD and the challenges it faces in order to be implemented in real life. In this thesis, we look at the following challenges and try to come up with solutions that improve system performance. These problems and our take on them are summarized below:

Problem: Although QKD promises unconditional security relying only on the laws of physics, the real implementation of certain QKD systems suffers from

possible attacks performed on various parts of the system, especially the measurement devices used by the users. MDI-QKD seems a promising scheme to overcome such a drawback. However, the following questions arise (1) How does it perform in realistic scenarios? and (2) Is it possible to use quantum memories in an MDI-QKD setup in order to extend the distance between Alice and Bob?

Our contribution: We provide a full analysis of an MDI-QKD system in an asymmetric setup once imperfect sources are used. We also provide a full analysis of a memory-assisted QKD protocol, by analytically computing the secret key rate when imperfect quantum memories with multiple-excitation issues are used. The results are striking and clearly eliminate the possibility of using such memories in certain setups.

Problem: Because of the no-cloning theorem it is challenging to reach long distances due to the exponential decay of the secret key rate in optical fibers. Probabilistic quantum repeaters are used to extend the distance. A real-life implementation of such devices is still not feasible due to various imperfections, which limit the performance of the setups. For example, the DLCZ protocol suffers from multiple excitations in quantum memories. How can we mitigate this problem and outperform the DLCZ protocol?

Our contribution: we compare analytically an alternative protocol to the DLCZ, in terms of their secret key generation rates once used for QKD applications. Our analytical approach will allow us to identify the regimes of operation where one setup outperforms the other and sheds light into the proper design of repeater systems.

Problem: In common probabilistic quantum repeater systems, users are provided with quantum memories and measurement devices. How can we simplify the equipment but at the same time retain the ability to exchange a key over long distances without trusting many other nodes to create a quantum network?

Our contribution: we combine the MDI-QKD protocol with a quantum repeater setup by considering all kind of imperfections both in the entanglement swapping generation operations as well as in the measurement process. We find the longest distance achievable using several nesting levels in a multiple-memory scheme with a finite number of memories. That would shed light on how quantum networks can be designed in the future.

Chapter 3

Measurement-device-independent quantum key distribution with ensemble-based memories

3.1 Introduction

The MDI-QKD protocol is born from the urge of finding a QKD scheme which was not affected by a set of attacks performed on the measurement devices. Several hacking strategies have been developed to exploit small imperfections in photodetectors, such as the efficiency mismatch attack [63], and the time-shift attack [64]. One possible way to prevent such attacks is to use the device-independent QKD (DIQKD) schemes [43, 65, 66]. The main assumption for such schemes is that there must be no leakage of information from users' measurement apparatus. DIQKD, remarkably, removes all side-channel attacks. However, its main drawback is that it requires a loophole-free Bell test, which has not been performed so far. Moreover, its implementation would be too challenging due to the low tolerable error rate, which is 7.1%, and to high values for the minimun required transmittance (92.4%) [66]. The MDI-QKD protocol relaxes such contraints, leading to a more feasible implementation.

Certainly, in a real scenario there are several sources of error, due to setup imperfections, that can reduce its performance. Such imperfections might reduce the improvements this protocol offers. That is the reason why we analyze in

the following sections the performance of such a protocol in a realistic scenario by considering several sources of imperfection. Some of these imperfections, for instance the dark count, affect the reach of the protocol. However, even with ideally perfect devices the rate would drop because of the channel loss. For long distances, we then need to use the quantum repeater idea in one way or another.

While progress toward building repeater systems is underway, one can think of intermediary steps that can be implemented in a nearer future. On the one hand, they ease the way for future generations of quantum networks [52, 67], and, on the other, they offer services over a range of distances not currently available by conventional direct QKD links. Memory-assisted measurement-device-independent QKD (MDI-QKD) has recently been proposed with the above objectives in mind [2, 68]. Such systems will resemble a single-node quantum repeater link with quantum memories (QMs) in the middle node; see Fig. 3.1. There is, however, no QMs at the users' ends and they are only equipped with encoder/source modules. Instead of distributing entanglement over elementary links, users send BB84-encoded states toward the memories, and once both memories are loaded with relevant states, an entanglement swapping operation is performed on the memories. In a recent work [2], it has been shown that if one uses fast memories with large storage-bandwidth products, it would be possible to beat existing no-memory QKD systems in a practical range of interest using memories mostly attainable with current technologies. Among different developing technologies for QMs, ensemble-based memories have a good chance to satisfy both required conditions. Writing times as short as 300 ps and bandwidths on the order of GHz have been reported for such memories [49, 50]. They are however inflicted by multiple-excitation effects, which may cause errors in QKD setups relying on such QMs. Here, we show how sensitive the performance of memory-assisted MDI-QKD can be to this type of errors and propose a modified setup resilient to multiple-excitation effects.

MDI-QKD offers a key exchange approach resilient to detector attacks [1]. In this system, Alice and Bob send their encoded signals to a middle station, at which a Bell-state measurement (BSM) is performed. This BSM effectively performs an entanglement swapping operation, similar to that of quantum repeaters, on the incoming photons, based on whose result Alice and Bob can infer certain

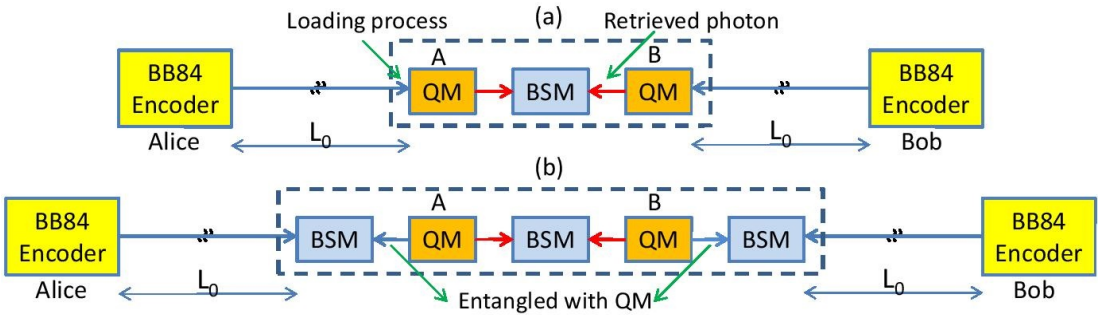

Figure 3.1: Different setups for memory-assisted MDI-QKD. (a) MDI-QKD with directly heralding quantum memories [2]. (b) MDI-QKD with indirectly heralding quantum memories [2]. At each round, an entangling process is applied to each QM, generating a photon entangled with the QM. These photons interfere at the side BSM modules next to the QMs with incoming pulses from the encoders.

correlations between their transmitted bits. Because of relying on the reverse-EPR protocol [31, 32], the middle party does not need to be trusted, nor does he need to perform a perfect BSM. In the memory-assisted MDI-QKD, we add two QMs before the middle BSM module. The objective is to obtain a better rate-versus-distance behavior as now the two photons sent by Alice and Bob do not need to arrive at the BSM module in the same round. This way, we expect to get the same improvement as in single-node quantum repeaters.

The required specifications for the QMs in Fig. 3.1 can be milder than that of a quantum repeater [2]. In a single-node quantum repeater, with two legs of length L_0 and one BSM module in the middle, we have to distribute entanglement between memories in each leg before being able to perform the BSM. For single-mode memories, the entanglement distribution scheme can only be applied once every $T_0 = L_0/c$, where c is the speed of light in the channel [58]. The required coherence time for the QMs is then proportional to T_0 as well. In the memory-assisted MDI-QKD of Fig. 3.1(a), the repetition rate is dictated by the writing time into QMs. If, therefore, a *heralding* mechanism is available, and if the QMs have short access times, we can run the MDI-QKD protocol faster than that of a quantum repeater, and, correspondingly, the required coherence time could also be lower [2].

The required heralding mechanism, by which we can tell if the QMs have been

loaded with the corresponding state to that sent by the users, can be implemented in several ways. In Fig. 3.1(a), we rely on a direct heralding mechanism in which we attempt to store the transmitted photons into the memories and non-destructively verify whether the writing procedure has been successful. This mechanism is only applicable to a limited number of QMs, such as trapped single atoms/ions, and it is often very slow [69]. In [2], the authors have analyzed an indirect heralding mechanism as in Fig. 3.1(b) in the single-excitation regime, that is, when QMs can only store a qubit. In this scheme, a photon is first entangled with the QM, and then immediately a side BSM is performed on this photon and the signal sent by the user. A successful side BSM, declared by two detector clicks, ideally teleports the user's state onto the QM and heralds a successful loading event. In order to outperform no-QM QKD systems, the setup of Fig. 3.1(b) must be equipped with memories with large storage-bandwidth products as well as short access and entangling times. It turns out that the state of the art for single-qubit memories, e.g., single atoms [70] or ions [69], is not yet sufficiently advanced to meet the requirements of practical memory-assisted protocols. In particular, we need faster memories for the practical ranges of interest.

In this Chapter we extend the analysis in [2] to the case of *ensemble-based* memories, which often offer very large bandwidths, or, equivalently, very short access times, suitable for the memory-assisted scheme. Such memories, however, suffer from multiple-excitation effects, which we carefully look into in this Chapter. In fact, when multiple-excitations are present, a seemingly successful side BSM may have been resulted from two photons originating from the QM in Fig. 3.1(b), in which case the final measurement results have no correlation with the transmitted signal by the user. Our results show that such effects can be so detrimental that we cannot beat no-memory QKD systems within practical ranges of interest.

This Chapter is organized as follows: Section 3.2 summarizes the contribution of this chapter. Sections 3.3, 3.4, 3.5, and 3.6 studies and analyses MDI-QKD with imperfect SPSs. Section 3.7 then covers MDI-QKD with ensemble-based memories. We conclude in Sec. 3.8.

3.2 This chapter's contribution

- We analyze an MDI-QKD protocol in a realistic scenario by considering two different types of sources. First, we assume that both users have an imperfect SPS that emits two photons with a probability p. We refer to this scenario by case A. In the second case (B), we assume that one of the users uses weak laser pulses while the other uses an imperfect SPS. We compare the two cases by calculating the secret key generation rate versus p, the dark count and the distance.

- In case A, we consider an asymmetric setup, where one of the users is located at the measurement site, and we compare this setup with the symmetric setup by calculating the secret key generation rate versus p. The asymmetric setup appears in our analysis of the memory-assisted MDI-QKD in Fig. 3.1(b).

- We compare the memory-assisted MDI-QKD protocol in Fig. 3.1(b) with imperfect ensemble-based QMs, i.e., affected by multiple excitations, with the conventional no memory setups. We plot the secret key rate versus the distance for these two schemes. It turned out that no matter how small these multiple excitations are, we cannot beat the no-memory systems in practical regimes of interest.

- Finally, we analyze the impact of finite coherence times (T_1) of the QMs, by calculating the secret key rate versus the distance for different values of T_1.

3.3 MDI-QKD with imperfect sources: Motivation

Regardless of the type of the material used, an ensemble-based memory can be modeled as a non-interacting ensemble of quantum systems. Here, for simplicity, but without loss of generality, we assume our QM is an ensemble of neutral atoms with the Λ-level configuration shown in Fig. 2.6. One possible way to entangle a

photon with such a QM is to pump all the atoms in the ensemble to be initially in their ground states $|g\rangle$; we then excite the ensemble by a short pulse in such a way that the probability, p, of driving an off-resonant Raman transition in the ensemble is kept well below one. In that case, the joint state of the released Raman optical field and the ensemble follows that of a two-mode squeezed state given by [71]

$$|\psi\rangle_{AP} = \sum_{n=0}^{\#\text{atoms}} \sqrt{(1-p)p^n}|n\rangle_A|n\rangle_P, \tag{3.1}$$

where $|n\rangle_P$ is the Fock state for n photons and $|n\rangle_A$ is the symmetric collective state to have n atoms in their $|s\rangle$ states. Assuming $p \ll 1$, we can truncate the above state at $n = 2$ without losing much accuracy. Furthermore, assuming that there is a post-selection mechanism by which the state $|0\rangle_A|0\rangle_P$ is selected out, the effective state for the photonic system P is given by

$$\rho_P(p) = (1-p)|1\rangle_{PP}\langle 1| + p|2\rangle_{PP}\langle 2|, \tag{3.2}$$

which resembles an imperfect single-photon source with a nonzero probability p for emitting two photons. This is the type of state that one would get for the photons entangled with the QMs in Fig. 3.1(b). That is, each leg of the system, can be modeled as an asymmetric MDI-QKD link, where the source on one side generates photons in the form of (3.2). The source on the user's end could be the same, or one may use decoy coherent states for practical purposes. This case will be investigated in the following sections. Note that the type of states as in (3.1) do not represent maximally entangled states. One can, however, combine two such states and obtain an effective entangled states after post-selection [72].

In this section, we study an MDI-QKD link with imperfect sources as in (3.2). Although we digress a bit from the memory-assisted problem, it gives us some insight into the analysis of the setup in Fig. 3.1(b), and, more generally, when MDI-QKD links are connected to quantum repeater setups as considered in Ch. 5. The type of ensemble memory considered here best fits into phase-encoded QKD setups as we will describe next [73].

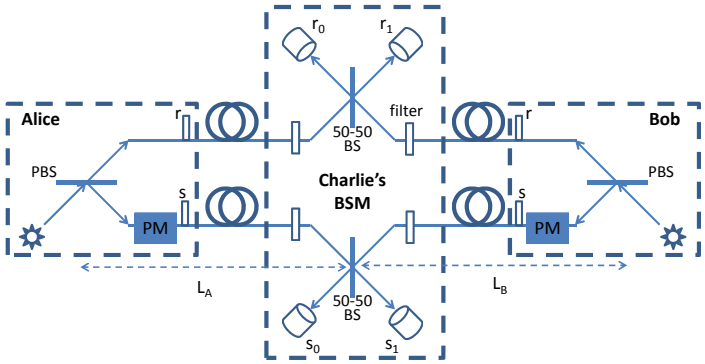

Figure 3.2: Diagram for MDI-QKD protocol, where PBS stands for polarizing beam splitter and PM stands for phase modulator.

3.4 Phase-encoded MDI-QKD

Figure 3.2 shows the setup for the phase-encoded MDI-QKD system we consider here. For the sake of convenience, we analyze the dual-rail setup of Fig. 3.2, but, for practical purposes, it is possible to implement the same scheme via time multiplexing, by using only one physical channel [73]. Here, states sent by Alice and Bob are encoded either in the z or the x basis. Encoding the states in the z basis is achieved by sending horizontally or vertically polarized pulses to a polarizing beam splitter (PBS) to, respectively, generate a signal in the r or in the s mode (corresponding to bits 0 or 1) in Fig. 3.2. To implement the x-basis encoding, +45-polarized pulses are prepared at the source and two relative phases, $\{0, \pi\}$ corresponding to bits $\{0, 1\}$, are used at the phase modulator. In this case, the PBS splits the signal into r and s modes, and photons will be in a superposition of these modes.

The procedure to establish a secret key is as follows. Alice and Bob, who are separated by a distance $L = L_A + L_B$, choose randomly a basis from $\{x, z\}$ and a bit from $\{0, 1\}$ and send a pulse to a middle site, where a BSM is performed by an untrusted party, Charlie. We make photons indistinguishable through the filters represented by empty boxes in Fig. 3.2. A click in exactly one of the r detectors, in Fig. 3.2, and exactly one of the s detectors will correspond to a successful BSM. When the users both choose the z basis, a successful BSM corresponds to complementary bits on the two ends. When they both choose the x basis, instead,

a different bit assignment will follow. If they pick the same phase then the state will be correlated and r_0 and s_0 or r_1 and s_1 will ideally click. We will refer to this detection event as type I. If they pick different phase values then the state will be anti-correlated and r_0 and s_1 or r_1 and s_0 will ideally click. The latter pattern of clicks is referred to as type II. In either case, Charlie announces her BSM results to Alice and Bob. Alice and Bob will compare the bases used for all transmissions. They keep the results if they have chosen the same basis and discard the rest.

In order to show how the protocol works, let us consider the ideal scenario when perfect SPSs are used. We label the modes corresponding to the Alice's side with a_r and a_s, where r and s refer to the upper and lower branches of Fig. 3.2, respectively. The corresponding modes on the Bob's side are b_r and b_s. If the phases chosen by Alice and Bob's are θ_a and θ_b respectively, the state in the Fock basis shared by Alice and Bob after the two PBSs in Fig. 3.2, is given by

$$(|1\rangle_{a_r}|0\rangle_{a_s} + e^{i\theta_a}|0\rangle_{a_r}|1\rangle_{a_s}) \otimes (|1\rangle_{b_r}|0\rangle_{b_s} + e^{i\theta_a}|0\rangle_{b_r}|1\rangle_{b_s}), \tag{3.3}$$

where we are neglecting the normalization factors for now. The relevant terms in Eq. (3.3), conditioned on a successful BSM outcome, are given by

$$|1\rangle_{a_r}|0\rangle_{a_s}|0\rangle_{b_r}|1\rangle_{b_s} + e^{i(\theta_a-\theta_b)}|0\rangle_{a_r}|1\rangle_{a_s}|1\rangle_{b_r}|0\rangle_{b_s} . \tag{3.4}$$

After the above state goes through two 50:50 beam splitters (one of each branch) in the BSM module, the resulting state is:

$$\begin{gathered}(|1\rangle_{r_0}|0\rangle_{r_1} + |0\rangle_{r_0}|1\rangle_{r_1}) \otimes (|1\rangle_{s_0}|0\rangle_{s_1} - |0\rangle_{s_0}|1\rangle_{s_1}) + \\ e^{i(\theta_a-\theta_b)}(|1\rangle_{r_0}|0\rangle_{r_1} - |0\rangle_{r_0}|1\rangle_{r_1}) \otimes (|1\rangle_{s_0}|0\rangle_{s_1} + |0\rangle_{s_0}|1\rangle_{s_1}) = \\ |1010\rangle_{r_0r_1s_0s_1} - |1001\rangle_{r_0r_1s_0s_1} + |0110\rangle_{r_0r_1s_0s_1} - |0101\rangle_{r_0r_1s_0s_1} \\ e^{i(\theta_a-\theta_b)}(|1010\rangle_{r_0r_1s_0s_1} + |1001\rangle_{r_0r_1s_0s_1} - |0110\rangle_{r_0r_1s_0s_1} - |0101\rangle_{r_0r_1s_0s_1})\end{gathered} \tag{3.5}$$

where r_0, r_1, s_0, and s_1 are the input modes to the corresponding detectors in Fig. 3.2. If $\theta_a - \theta_a = 0$, then the state of Eq. (3.5) is

$$|1010\rangle_{r_0r_1s_0s_1} - |0101\rangle_{r_0r_1s_0s_1} , \tag{3.6}$$

i.e., either detectors r_0 and s_0 click or r_1 and s_1 click. Instead, if $\theta_a - \theta_b = \pm\pi$, the state in Eq. (3.5) will be

$$|0110\rangle_{r_0r_1s_0s_1} - |1001\rangle_{r_0r_1s_0s_1} , \tag{3.7}$$

which corresponds to a click in detectors r_1 and s_0, or a click in detectors r_0 and s_1. In the end, Alice and Bob will share a correlated or anticorrelated pairs of bits, determined by the click patterns for each basis.

The above is an ideal description of how to determine a shared key string between Alice and Bob. In a real scenario, we have to consider setup's inefficiencies as well. As a consequence, they can reduce the performance of the system, by introducing some spurious terms in the density matrix, which have not been considered in the above scenario. In order to analyze the performance of such a setup, we analytically calculate the secret key generation rate in different scenarios, as described in the next section.

3.5 Key rate analysis of MDI-QKD versus setup inefficiencies

In [73], the key secret key rate has been calculated when users either both send single photons or laser pulses. In this section, the secret key generation rate for the MDI-QKD scheme of Fig. 3.2 is calculated when imperfect SPSs are used. As already mentioned, we consider two cases. In the first one (A), we assume that Alice and Bob have an imperfect SPS which can emit two photons. In the second (B), one of the party uses coherent states with the decoy-state protocol and the other one uses imperfect SPSs. For both types of sources used, we estimate the yield Y_{11}^z of having a successful click pattern in the z basis, and the phase error rate e_{11}^x in the x basis, provided that Alice and Bob both are sending a single photon. In the following sections we describe the other terms of the key rate in the cases of interest. We point out that this analysis constitutes a preliminary step for the study of the MDI-QKD setup embedded with memories, as we discuss in Sec. 3.7, or a quantum repeater protocol, as described in Ch. 5.

3.5.1 Imperfect single photon source (case A)

With the current technology, it is still challenging to generate single photon states and SPSs often suffer from the possibility of multiple-photon emissions. To address this issue, in this section, we consider non-ideal single photon sources with

nonzero probabilities for two-photon emissions, p. In Fig. 3.2, if our sources emit one photon with probability $1-p$ and two photons with probability p, then we have the following input density matrix for the initial state shared by Alice and Bob

$$\rho_C^{(\text{in})} = [\rho_{r_A}(p) \otimes \rho_{s_B}(p) + \rho_{s_A}(p) \otimes \rho_{r_B}(p)]/2, \tag{3.8}$$

if they are sending complementary bits and

$$\rho_E^{(\text{in})} = [\rho_{r_A}(p) \otimes \rho_{r_B}(p) + \rho_{s_A}(p) \otimes \rho_{s_B}(p)]/2 \tag{3.9}$$

if they are sending the same bits, where

$$\rho_{x_j}^{(in)} = (1-p)\,|1\rangle_{x_j x_j}\langle 1| + p\,|2\rangle_{x_j x_j}\langle 2|, \qquad x = s, r; j = A.B \tag{3.10}$$

In a practical regime of operation, $p \ll 1$; hence, in our following analysis, we neglect $O(p^2)$ terms corresponding to the simultaneous emission of two photons by both sources. We assume the value of p can be randomly changed according to the decoy-state protocol. We assume Alice and Bob are located at, respectively, distances L_A and L_B from the BSM module, and the total path loss for a channel with length l is given in Eq. (2.16). Initially, we assume $L_A = L_B$. We treat the asymmetric case in Sec. 3.6.4. Here, we model our setup with fictitious beam splitters representing the setup's inefficiencies as explained in Sec. 2.12 and we consider NRPDs, represented by the measurement operator of Eq. (2.14).

To calculate the key rate, we, then, have to take into account the probability of a successful click pattern in the z basis when the input is given by (3.10), Q_{pp}^z, as well as the corresponding quantum bit error rate, E_{pp}^z in the z basis. The key rate will be given by

$$R_{ss} \geq Q_{11}^z\,(1 - H\,(e_{11}^x)) - Q_{pp}^z f\,H\left(E_{pp}^z\right) \tag{3.11}$$

where Q_{11}^z is $(1-p)^2 Y_{11}^z$, and Y_{11}^z is the probability of a successful click pattern when Alice and Bob send exactly one photon each. The term $Q_{pp}^z f\,H\left(E_{pp}^z\right)$ in Eq. (3.11) is the cost of error correction, I_{ec}. In Eq. (3.11), Y_{11}^z and e_{11}^x have already been calculated in [73], hence, here we will derive the other terms. To find the relevant probabilities in (3.11), we apply the butterfly operation shown

in Fig. 2.8(b), whose input-output relationships are shown in Table B.2, to Eq. (3.8). The output density matrix will be given by

$$\rho_{AB}^{(out)} = B_{0.5,\eta_s}\left(\rho_{AB}^{(in)}\right), \tag{3.12}$$

where $\eta_s = \eta_{ch}\eta_D$, and $B_{0.5.\eta_s} = B^{a_s,b_s}_{0.5.\eta s,\eta s,1,1} \otimes B^{a_r,b_r}_{0.5,\eta_s,\eta_s,1,1}$ as explained in Sec. 2.10.

A successful click pattern is given by one click in one of the upper photodetectors (r_0, r_1), and one of the lower photodetectors $(s_{0,}s_1)$ of Fig. 3.2. The measurement operators, which includes dark count, on the modes entering the photodetectos of Fig. 3.2, depending on which detector clicks, are given by

$$\begin{array}{l} M_{x_0} = M^{NR}_{x_0 x_1}, \quad \mathrm{x = r,\ s} \\ M_{x_1} = M^{NR}_{x_1 x_0}, \quad \mathrm{x = r,\ s} \end{array} \tag{3.13}$$

which refer to Eq. (2.14).

The probability to get a click on r_i and s_j detectors will be then

$$P_{r_i s_j} = \mathrm{Tr}(\rho_{AB}^{(out)} M_{r_i} M_{s_j}), \qquad i,\ j = 0,\ 1. \tag{3.14}$$

The probability that an acceptable click pattern occurs in the z basis, Q^z_{pp} is defined as:

$$Q^z_{pp} = Q^z_C + Q^z_E, \tag{3.15}$$

where Q^z_C is the probability that a correct click pattern occurs, which corresponds to the case when Alice and Bob send complementary bits, and it is given by

$$Q^z_C = 1/2\left(P_{r_0 s_0} + P_{r_1 s_1} + P_{r_0 s_1} + P_{r_1 s_0}\right) \tag{3.16}$$

and Q^z_E is the probability that an error occurs, which, in the z basis, corresponds to the case when Alice and Bob send the same bit. Finally, E^z_{pp} is given by

$$E^z_{pp} = \frac{Q^z_{EE}}{Q^z_{pp}} \tag{3.17}$$

where $Q^z_{EE} = e_d Q^z_C + (1 - e_d) Q^z_E$, and e_d is the misalignment parameter, which will be discussed in Sec. 3.5.3.

3.5.2 One coherent source and an imperfect single photon source (case B)

We now substitute one of the two imperfect single photon sources in Fig. 3.2 with a coherent source with mean photon number $|\alpha|^2$, in order to use a decoy-state version of the scheme, which has been described in Sec. 2.3. In this case, the initial density matrices in (3.8) are

$$\begin{array}{c} \rho_A^{(in)} = |\alpha\rangle\langle\alpha| \\ \rho_B^{(in)} = (1-p)\,|1\rangle\langle 1| + p\,|2\rangle\langle 2| \end{array} . \tag{3.18}$$

We phase randomize $|\alpha\rangle$, and average over, in the end. To calculate the key rate, we have to take into account the probability of a successful click pattern in the z basis, $Q^z_{\alpha p}$, when the input is given by Eq. (3.18), and the corresponding quantum bit error rate $E^z_{\alpha p}$ in the z basis. The key rate will be lower bounded by

$$R_{cs} \geq Q^z_{11}\left(1 - H\left(e^x_{11}\right)\right) - Q^z_{\alpha p} f\, H\left(E^z_{\alpha p}\right), \tag{3.19}$$

where now $Q^z_{11} = (1-p)\,\alpha^2 e^{-\alpha^2} Y^z_{11}$. The procedure to find the relevant terms of the key rate of Eq. (3.19) follows the same steps described in Sec. 3.5.1. However, in this case, we use the input-output relationships listed in Table C.1 to find the relevant states of interest.

3.5.3 Misalignment

In this section we describe where the parameter e_d in the expression for $Y^z_{error_{pp}}$ comes from. We have assumed so far that the photons impinging the measurement apparatus are indistinguishable. This goal can be reached by putting filters before the measurement scheme itself as shown in Fig. 3.2. Variations of the central frequency of the pulses as well as a not perfect stability of the sources can lead to a failure of this condition, and, therefore, the photons will be distinguishable, resulting in a statistical misalignment probability. This could compromise the security of our protocol, and a leakage of the key to an untrusted party. Depending on the way the key bits are encoded, phase stabilizers or polarization maintenance is required. To address this issue we have introduced another source of error, e_d, which takes into account the effects of misalignment and mismatch.

η_D	0.93
η_{r0}	0.87
d_c	10^{-9}
L_{att}	25 km
p	10^{-4}
e_d	10^{-3}

Table 3.1: Nominal values used in our numerical results

3.6 Numerical Results

In this section, we present the numerical results for the secret key generation rate of the MDI-QKD protocol, in the two aforementioned cases, and we compare them versus different system parameters. We have used Maple 15 to analytically derive expressions for Eqs. (3.11) and (3.19).

Unless explicitly stated, we have used the parameter values listed in Table 3.1. The near-optimal nominal values for quantum efficiency and dark count have been achieved in [74] and for the reading efficiency in [75].

3.6.1 Rate versus $|\alpha|^2$

Figure 3.3 shows the secret key generation rate versus the mean photon number for (a) different values of d_c and (b) different values of e_d at $L = 100$ km. It can be seen in Fig. 3.3(a) that there exist optimal values of $|\alpha|^2$, around 1, that maximize the key rate. For higher values of d_c and e_d, this optimal source parameter slightly decreases. Dark count and misalignment represent the main sources of error in the QBER of the term $E^z_{\alpha p}$, hence, when d_c and e_d increase, the cut-off point for the maximum allowed value of $|\alpha|^2$ reduces. This leads to a slightly shifted curve, hence lower values for the optimal values of $|\alpha|^2$. On the contrary, $E^z_{\alpha p}$, is not significantly affected by the double photon probability p and there is little difference when p increases. This has been explained in Sec. 3.6.2. We use 1 as the optimal value for $|\alpha|^2$ in all the subsequent results.

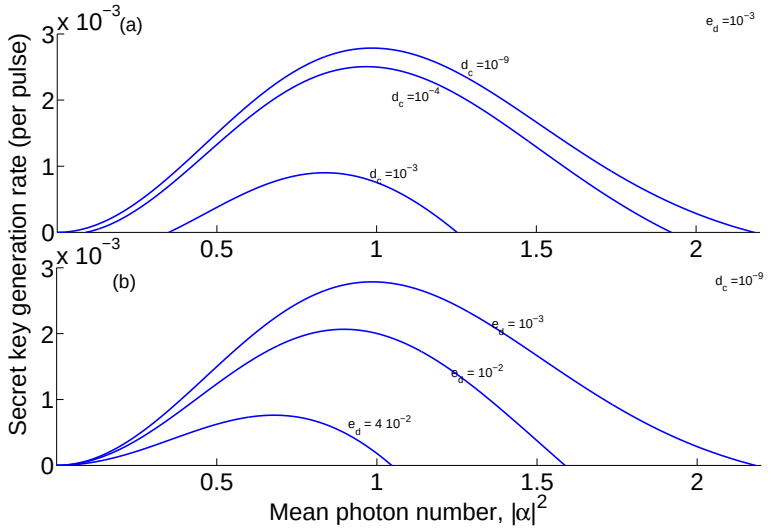

Figure 3.3: Rate versus the mean photon number $|\alpha|^2$ for different values of (a) dark count rates and (b) misalignment. Here, L = 100 km the other values

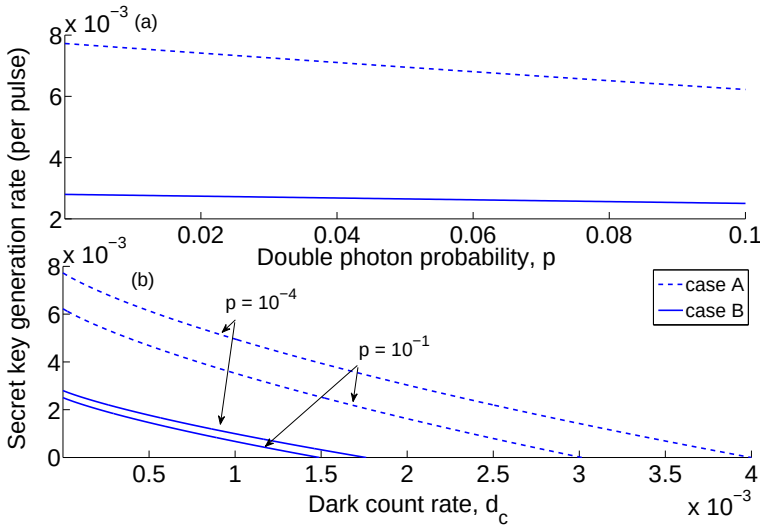

Figure 3.4: Rate versus (a) the double photon probability, p, and (b) dark count rate, d_c, at $p = 10^{-4}$ and $p = 10^{-1}$. Here, L = 100 km.

3.6.2 Rate versus p and d_c

Figure 3.4 shows the secret key generation rate at the optimal value of $|\alpha|^2$, versus (a) the double photon probability, p, and (b) dark count rate, d_c. From Fig. 3.4(a), it is clear that for low values of the double photon probability, the performance of the setup remains almost invariant. The main reason for this behavior is the fact that the only error term in Eqs. (3.11) and (3.19) that depends on p is E^z_{pp}. An error in the z basis arises from the cases where Alice and Bob are both sending the same bits, for instance both send a signal in their respective r modes, but one r detector and one s detector clicks in Fig. 3.2. The click on the s detectors comes from dark counts and is not affected by the double photon states in the r modes. However, double photons slightly change the rate, as we disregard double-click cases, and that is the reason for lower key rates once p increases. In order to appreciate a more visible dependence on p, we should relinquish the condition $p \ll 1$.

Furthermore, Fig. 3.5(b) shows that tolerable dark count rates are lower in case B. By increasing p, we expect a lesser difference between the two cases. In fact, Figure 3.4 shows that there is only a little difference for the dark count cut-off at $p = 0.1$, which is roughly the same probability as for a coherent state with $|\alpha|^2 = 1$ to have two photons (~ 0.18).

3.6.3 Rate versus L

Figure 3.5 shows the secret key generation rate at the optimal value of α, versus the distance between Alice and Bob, L, for (a) two values of dark count and (b) two values of misalignment. As shown in the figure, low dark count rates can considerably change the cutoff distance. In particular, it is possible to share a secret key rate over 500 km although the rate is very low. On the contrary, for high values of the dark count the distance is reduced. The same effects are observed for misalignment.

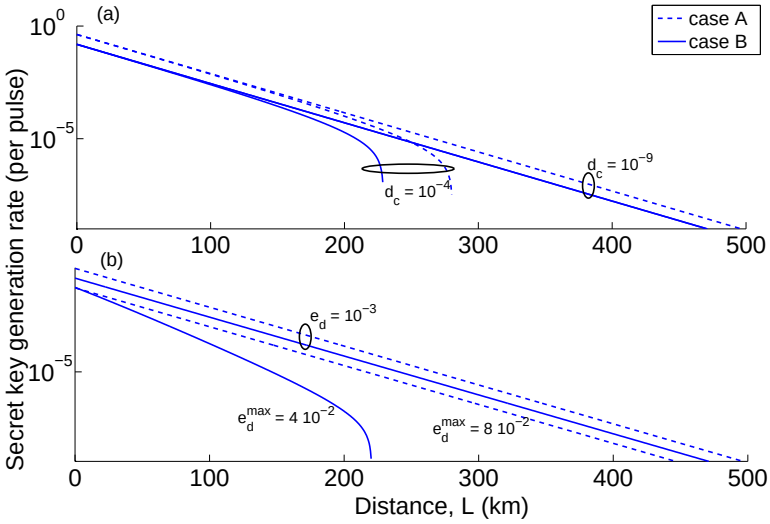

Figure 3.5: Rate versus (a) distance between Alice and Bob for different values of d_c and (b) e_d.

3.6.4 Key rate of the asymmetric setup

In this section, we compare an asymmetric setup with $L_A = L$ and $L_B = 0$ with the symmetric setups, versus p at $e_d = 0$. Figure 3.6 shows that in both the asymmetric and symmetric setup there seems to be little effect on the key rate as a result of introducing double photons. The reason for this behavior has already been explained in Sec. 3.6.2.

We have so far analyzed the effects of the main inefficiencies in a real implementation of the MDI-QKD protocol based on phase encoding. We have found the longest distance we can reach by considering fundamental sources of error, such as misalignment and dark counts. We have shown that an imperfect SPS does not introduce substantial degradation in performance.

As already stated, the memory assisted version of the MDI-QKD protocol improves the rate-versus-distance compared to the no-memory setup and uses QMs with lower requirements than probabilistic quantum repeater protocols. However, if we use ensemble-based QMs, we end up with situations like an MDI-QKD setup with double-photon sources. In the next section, we use the results we have obtained in the above sections to investigate how an imperfect QM, that

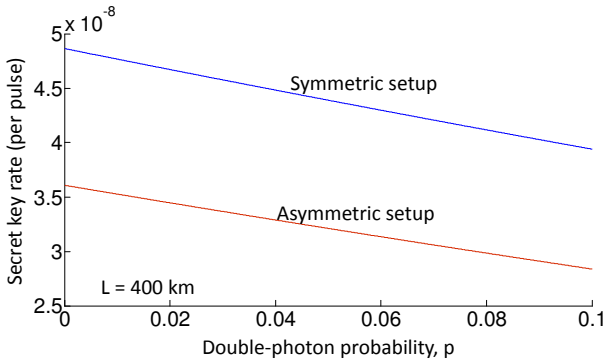

Figure 3.6: Secret key generation rate per transmitted pulse versus the double-photon probability, p. In all curves $L = 400$ km and all other parameters are taken from Table 3.1. In the symmetric case, $L_A = L_B$, whereas in the asymmetric case, $L_A = L$ and $L_B = 0$.

emits two photons with a probability p, affects the memory assisted MDI-QKD protocol.

3.7 MDI-QKD with ensemble-based memories

In this section, we analyze the effect of multiple excitations in (3.1) on the key rate of the memory-assisted MDI-QKD link of Fig. 3.1(b) by using the phase-encoding scheme described in Sec. 3.4 and combine it with four ensemble-based memories as described below. In contrast to the previous section, where double-photon terms had little effect on system performance, it turns out that, within the setup of Fig. 3.1(b), multiple excitations in memories would harshly affect the achievable key rate.

3.7.1 Setup description

Figure 3.7 shows the phase-encoding variant of the memory-assisted MDI-QKD system. Here, in order to focus on the memory effects, we assume Alice and Bob are using perfect single-photon sources. For each photon encoded and sent by the users, we pump the corresponding memories A_1, A_2, B_1, and B_2 in order to generate a joint photonic-atomic state. The state sent by the user is indirectly loaded to the memories by the side-BSM modules in Fig. 3.7. For instance, on

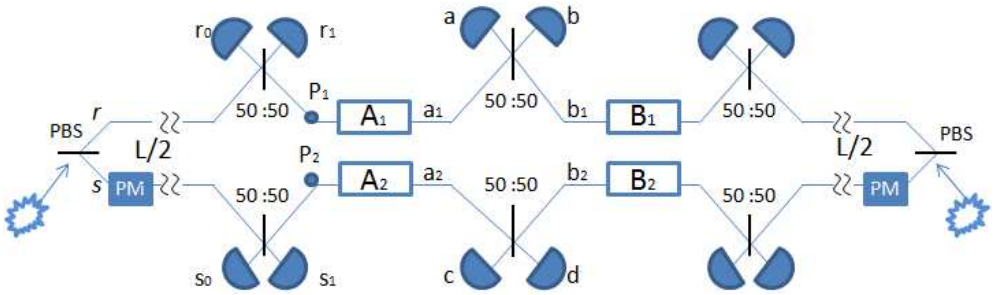

Figure 3.7: Schematic diagram for the MDI-QKD setup with ensemble-based memories, represented by A_1, A_2, B_1, B_2.

Basis	Alice BSM	Bob BSM	Middle BSM	Bit assignment
z	type I/II	type I/II	type I/II	Bob flips his bit
x	type I (II)	type I (II)	type I	Bob keeps his bit
x	type I (II)	type I (II)	type II	Bob flips his bit
x	type I (II)	type II (I)	type I	Bob flips his bit
x	type I (II)	type II (I)	type II	Bob keeps his bit

Table 3.2: Bit assignment protocol depending on the results of the three BSMs in Fig. 3.7.

the Alice side, we perform a BSM on the single-photon state sent by Alice and P_1 and P_2 states using the same BSM module as that of Fig. 3.2. A successful side BSM, that is when detectors click on each branch, would ideally load the memories with a state corresponding to what the users have sent. For instance, if Alice uses the z basis, and sends a signal in the r mode, a successful BSM on her side, would imply that the memories A_1-A_2 are ideally in the $|01\rangle_{A_1A_2}$ state. Of course, considering the dark current and double-photon terms, we will deviate from this ideal case, and that is what we are going to study in this Section. Alice and Bob attempt repeatedly to load their memories until they succeed, at which point they wait for the other party to complete this task. Once both sets of memories are loaded, we read out all four memories and proceed with the middle BSM. Once the results of all three BSMs as well as the bases used are being communicated to users, Alice and Bob can come up with a sifted key bit. Table 3.2 shows what bits Alice and Bob assign to their sifted keys depending on the results of the three BSM operations.

3.7.2 Key rate analysis

In this section, the key rate for the setup of Fig. 3.7 is obtained under the normal operation condition when no eavesdropper is present. We assume users have perfect SPSs. Using the efficient QKD protocol, where the z basis is used more often than the x basis, the secret key rate per transmitted pulse is lower bounded by

$$R_{\mathrm{QM}} \geq Y_{11}^{\mathrm{QM}} \left[1 - h\left(e_{11;x}^{\mathrm{QM}}\right) - h\left(e_{11;z}^{\mathrm{QM}}\right)\right], \tag{3.20}$$

where $e_{11;x}^{\mathrm{QM}}$ and $e_{11;z}^{\mathrm{QM}}$, respectively, represent the QBER between Alice and Bob in the x and z basis, when single photons are sent, and Y_{11}^{QM} represents the probability that, in the z basis, both sets of memories A and B are loaded *and* the middle BSM is successful. In Appendix A.2, we derive all above terms assuming that memories may undergo amplitude decay according to an exponential law. That is, if the recall/reading efficiency, right after a successful writing procedure, is denoted by η_{r0}, the reading efficiency after a time t is given by $\eta_r(t) = \eta_{r0} \exp(-t/T_1)$, where T_1 is the amplitude decay time constant.

In the absence of dark counts, memory decay, and source imperfections, the major source of noise in the setup of Fig. 3.7 is the multiple-excitation terms originated from the ensemble-based QM. Even if the users send exactly one photon, the state loaded to the QMs may contain more than one excitation overall. These additional excited atoms will cause errors in the middle BSM setup. The errors in the latter stage are partly similar to what we studied in the previous section, when we considered imperfect single-photon sources. These cases correspond to loading states like $|20\rangle_{A_1A_2}$ into A_1-A_2 memories, or similar states for B_1-B_2. There are, however, other terms that must be considered, such as $|11\rangle_{A_1A_2}$, and they turn out to have even more contribution to the noise terms in Eq. (3.20). Our analysis in this section, considers up to two excitations in each memory module.

Figure 3.8 shows the effect of multiple excitations in the scheme of Fig. 3.7 and compares it with a symmetric no-memory setup as in Fig. 3.2. Assuming no decay or misalignment in the setup and with a negligible amount of dark count as in Table 3.1, Fig. 3.8 shows that the memory-assisted system of Fig. 3.7 cannot outperform the no-memory system within a reasonable range of rates and/or

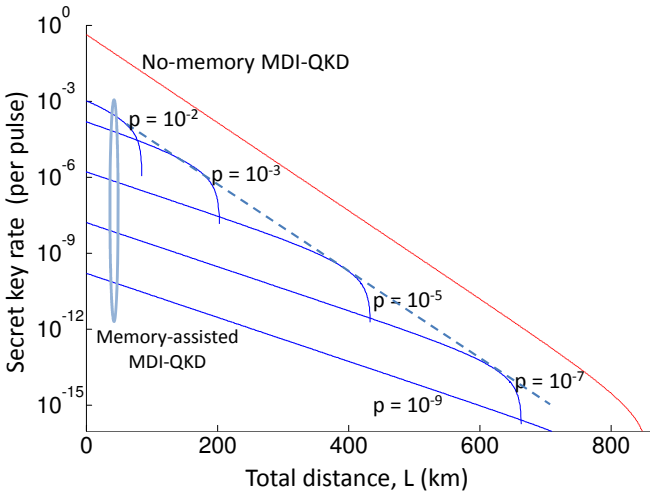

Figure 3.8: Secret key generation rate per transmitted pulse versus distance for the MDI-QKD scheme with (Fig. 3.7) and without (Fig. 3.2) memories for different values of the excitation probability p. Nominal values are used as in Table 3.1 with $T_1 = \infty$. For the no-memory curve, $L_A = L_B$ and $p = 0$.

distances. Here, we have considered different values of p. As we decrease the value of p, the chance of entangling a photon with the memories become lower, and that is why the initial key generation rate drops. However, lower values of p will make the generation of multiple-excitation states less likely and that is why the cut-off security distance becomes longer. We nevertheless never cross the no-QM rate curve.

In order to understand the above behavior, we need to look more closely at the dynamics of different terms in Eq. (3.20). The term $Y_{11}^{\rm QM}$ is proportional to the loading probability, i.e., the success probability in each of the side BSMs of Fig. 3.7. In order to have a successful BSM we need to get two clicks, one on the upper arm, and one in the lower one. For short distances, the two clicks are typically caused by the photon sent by the user and a photon entangled with the two memories on each side. The loading probability, in this limit, is then on the order of $p\exp[-(L/2)/L_{\rm att}]$, where p is the probability that one of the two ensembles on each side has one excitation, and $\exp[-(L/2)/L_{\rm att}]$ is the channel efficiency for the transmitted photon by the user. The initial slope of the curves in Fig. 3.8 corresponds to the above scaling with distance, similar to that of quantum re-

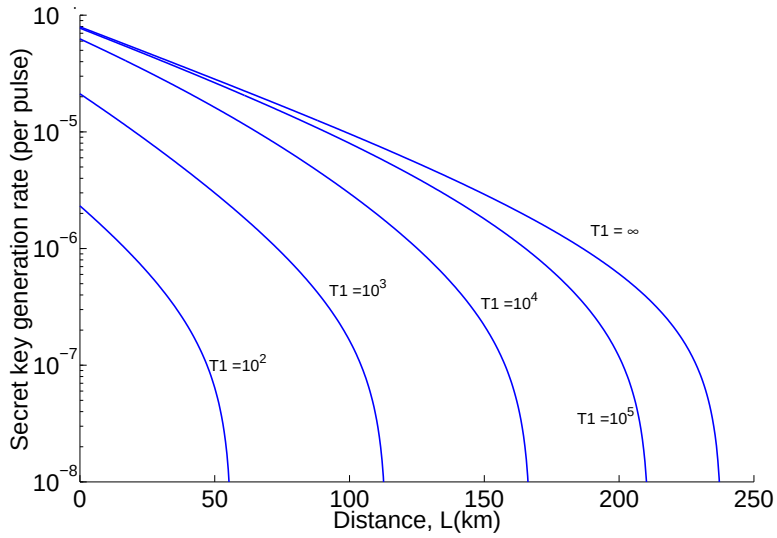

Figure 3.9: Rate versus the distance for assisted-memory MDI-QKD scheme with imperfect QMS for different values of the decoherence time T_1 at $p = 10^{-4}$.

peaters. As the distance becomes longer and longer, the chance of receiving the photon sent by the user becomes slimmer and slimmer. In this limit, a successful BSM is often caused by photons originating from memories, in particular, terms like $|11\rangle_{A_1A_2}|11\rangle_{P_1P_2}$. Such successful BSMs do not imply any correlations between the states of memories and that of Alice or Bob, and will simply result in random errors and the eventual decline of the key rate to zero. Given that the probability of generating a two-photon state is on the order of p^2, the transition from the first region to the cut-off region roughly occurs at a distance L_c, where $p\exp[-(L_c/2)/L_{\text{att}}] \approx p^2$, or equivalently, when $\exp[-(L_c/2)/L_{\text{att}}] \approx p$. This implies that the total rate would then scale as $p\exp[-(L_c/2)/L_{\text{att}}] \approx \exp[-L_c/L_{\text{att}}]$, which is similar to a no-QM system. This is evident in Fig. 3.8 by the envelop (dashed line) of QM-assisted curves, which is parallel to the no-QM curve. Considering the additional inefficiencies in the memory-assisted system as compared to the no-QM one, for the range of values used in our calculations, it becomes practically impossible to beat the no-QM system if we use ensemble-based memories in the setup of Fig. 3.7. Note that the performance would further degrade if memory decay effects are also included, as shown in Fig. 3.9

3.8 Conclusion

In this Chapter, we analyzed the MDI-QKD protocol with phase encoding proposed in [73] in terms of the secret key generation rate with two different types of sources and with and without memories. We compared an imperfect single photon source, having a probability p of emitting two photons, with a more affordable source, such as a laser, which emit coherent states with the decoy-state protocol, under practical assumptions. We considered various sources of imperfections in our analysis, such as path loss, quantum efficiency and dark counts, and obtained the optimal regime of operation as a function of system parameters. We first estimated the optimal value of the mean number of photons of the coherent source (laser). With this value, we compared the key rate of the two cases versus different setup parameters, such as double-photon probability and dark count. The highest distance at which it is possible to share a secret key is over 500 km at $p = 10^{-4}$, $e_d = 10^{-3}$ and for negligible values of d_c for both cases. By increasing the dark count and the misalignment this limit is reduced. In particular, for $d_c = 10^{-4}$, the largest distance lies between 200 and 300 km. We can estimate the highest tolerable misalignment, e_d^{max}. For the imperfect source $e_d^{max} = 8 \cdot 10^{-2}$ and for the coherent case $e_d^{max} = 4 \cdot 10^{-2}$. It turns out that, although using two imperfect single photon states allow us to have higher tolerable values for dark counts, the performance of the protocol is almost equivalent when one source is substituted with a laser which emit coherent states.

We analyzed the effects of double-photon emission in MDI-QKD system and in the memory-assisted MDI-QKD system. We showed that in the no memory case an imperfect single photon source emitting two photons does not affect much the performance of the protocol, whereas a memory-assisted MDI-QKD system is strongly affected by multiple excitations in QMs. In [2], authors showed that memory-assisted MDI-QKD beats the conventional no-memory system if qubit-based QMs are fast and have sufficiently long coherence times. In this Chapter, we showed that multiple excitations in QMs deteriorate the performance of ensemble-based memory-assisted MDI-QKD systems to the extent that they can no longer beat their no-memory counterparts. Ultimately, in order to go to arbitrarily long distances quantum repeaters are needed as we will study in the next Chapters.

Chapter 4

SPS versus DLCZ quantum repeater

4.1 Introduction

Despite all practical progress with QKD [76, 77], its implementation over long distances remains to be a daunting task. In conventional QKD protocols such as BB84 [16], channel loss and detector noises set an upper bound on the achievable security distance [78]. In addition, the path loss results in an exponential decay of the secret key generation rate with distance. Both these issues can, in principle, be overcome if one implements entanglement-based QKD protocols [18, 19] over quantum repeater systems [35, 36, 61, 79]. However, as already mentioned in Chapter 2, this approach, is not without its own challenges. Quantum repeaters require QM units that can interact with light and can store their states for sufficiently long times. Moreover, highly efficient quantum gates might be needed to perform two-qubit operations on these QMs [35]. The latter issue has been alleviated, to some extent, by introducing the DLCZ protocol [36] introduced in the second Chapter, in which initial entanglement distribution and swapping, thereafter, rely on probabilistic linear-optic operations. Since its introduction, the DLCZ idea has been extended and a number of new proposals have emerged [37, 54, 57, 80]. Such probabilistic schemes for quantum repeaters particularly find applications in QKD systems of mid-to-long distances, which makes them worthy of analytical scrutiny. In this Chapter, we compare DLCZ with one of its

favorite successors, the SPS protocol [37], which relies on single photon sources. Using a general system-level approach, which encompasses many relevant physical sources of imperfection in both systems, we provide a realistic account of their performance in terms of their secret key generation rates per logical memory used. This measure not only quantifies performance, but it also accounts for possible costs of implementation.

The SPS protocol attempts to resolve one of the key drawbacks in the original DLCZ protocol: multi-photon emissions. DLCZ uses atomic ensembles as QMs, which lend themselves to multi-photon emissions. This leads to obtaining not-fully-entangled states, hence resulting in lower key rates when used for QKD. To tackle this issue, in the SPS protocol, entanglement is distributed by ideally generating single photons, which will either be stored in QMs, or directed toward a measurement site. Whereas, in principle, the SPS protocol should not deal with the multi-photon problem, in practice, it is challenging to build on-demand single photon sources that do not produce any multi-photon components. A fair comparison between the two systems is only possible when one considers different sources of non-idealities in both cases, as we will pursue in this Chapter.

The SPS protocol is one of the many proposed schemes for probabilistic quantum repeaters. In [81], authors provide a review of all such schemes and compare them in terms of the average time that it takes to generate entangled states, of a certain *fidelity*, between two remote memories. Their conclusion is that in the limit of highly efficient memories and detectors, the top three protocols are the SPS protocol and two others that rely on entangled/two photon sources [54, 82]. In more practical regimes, however, the SPS protocol seems to have the best performance per memory/mode used. In this Chapter, we therefore focus on the SPS protocol, and will investigate, under practical assumptions, whether the above conclusion remains valid in the context of QKD systems.

This Chapter is structured as follows. In Sec. 4.2, we outline the contributions of this Chapter. In Sec. 4.3, we review the SPS protocol and we describe the entanglement swapping operation and how it is possible to share a secret key with a QKD measurement. We also describe how we model the memory decay and dephasing. In Sec. 4.4, we describe how we analytically calculate the secret key rate for the setups under study in the repeater and no-repeater cases. In Sec.

4.5, we present the numerical results of the key rate versus setup's parameters and we compare the performance of the SPS protocol with the DLCZ protocol. Finally, in Sec. 4.6, we draw our conclusions.

4.2 This chapter's contribution

The work presented in this Chapter is distinct from previous related work in its focusing on the performance of "QKD" systems over quantum repeaters. In [56], authors have adopted the general measure of fidelity to find the average time of entanglement generation. Whereas their approach provides us with a general insight into some aspects of quantum repeater systems, it cannot be directly applied to the case of QKD. In the latter, the performance is not only a function of the entanglement generation rate, but also the quantum bit error rate caused by using non-ideal entangled states. To include both these issues, here, we adopt the secret-key generation rate per memory as the main figure of merit, by which we can specify the optimal setting of the system and its performance in different regimes of operation.

Another key feature of our work is to use a *normalized* figure of merit to compare the DLCZ and SPS protocols. In practice, to obtain a sufficiently large key rate in such probabilistic systems, one must use multiple memories and/or modes in parallel (see Sec. 2.8). In order to account for the cost of the system, in our analysis, we provide a normalized key rate per memory and/or mode. We calculate the dependence of the secret key generation rate on different system parameters when resolving or non-resolving detectors are used. In particular, we find the optimal values for relevant system parameters if loss, double-photon emissions and dark counts are considered. Moreover, we account for the dephasing and the decay of memories in our analysis, which, we believe, is unprecedented. In our setups, we assume ensemble-based QMs are in use.

4.3 SPS protocol for quantum repeaters

In this section, we review the SPS protocol for quantum repeaters and model relevant system components. The entanglement swapping and the QKD mea-

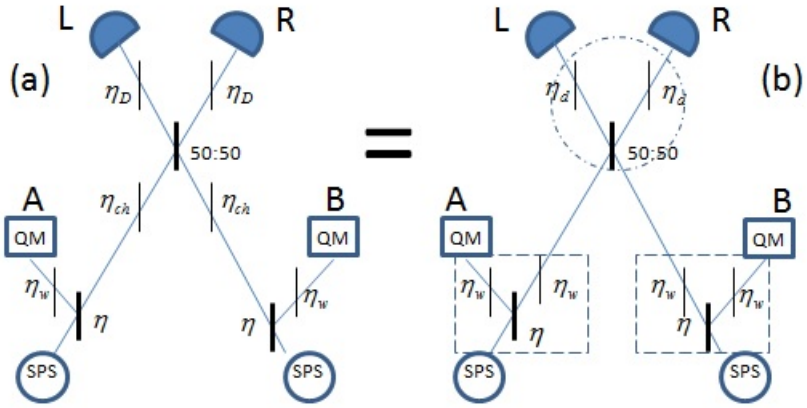

Figure 4.1: A schematic model for the SPS scheme. In (a) the memories' writing efficiencies, the path loss and the detectors' efficiencies are represented by fictitious beam splitters with transmission coefficients η_w; η_{ch} and η_D, respectively. In (b), an equivalent model is represented, where we have grouped beam splitters in the form of butterfly modules; see Fig. 2.8. Here, $\eta_{ch}\eta_D = \eta_w\eta_d$.

surement are described for such a setup.

4.3.1 SPS setup

In Section 2.9.3 we described how the SPS protocol works. As shown in Fig. 2.5(b) Alice and Bob, separated by a distance L, are provided each with an ideal SPS and a QM. They both send a photon to a beam splitter of transmissivity η, which can deflect the photon to a QM or will let the photon go through. A BSM is then performed on the travelling fields and a click on one of the two photodetectors will project the state shared in the QMs into a Bell state plus a spurious vacuum state, which will be ruled out in the post-selection process. Alice and Bob can use two such entangled states, in a QKD measurement, to extract a secure key bit.

For a proper analysis of the system, it is important to account for setup inefficiencies, which are present in real implementations. In Fig. 4.1(a), we model the memory writing efficiency, the channel transmissivity, and the detectors quantum efficiency by introducing fictitious beam splitters with, respectively, transmissivities η_w, η_{ch}, and η_D. In our analysis, we use an equivalent setup, as shown in

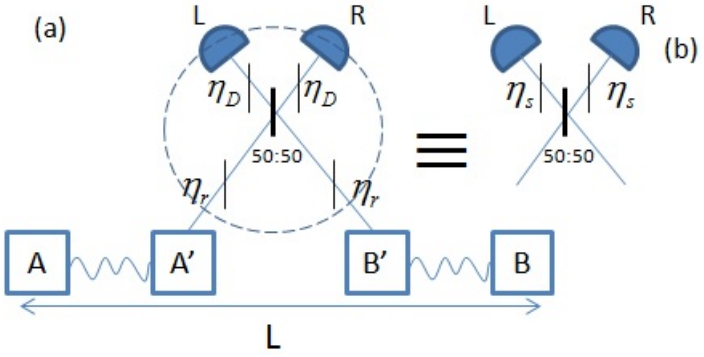

Figure 4.2: (a) Entanglement connection between two entangled links $A - A'$ and $B' - B$. The memories A' and B' are read out and the resulting photons are combined on a 50:50 beam splitter. A click on one of the detectors projects A and B into an entangled state. The retrieval efficiencies and quantum efficiencies are represented by fictitious beam splitters with transmission coefficient η_r and η_D, respectively. (b) The equivalent butterfly transformation to the measurement module, where $\eta_s = \eta_r \eta_D$.

Fig. 4.1(b), where beam splitters have been rearranged such that $\eta_{ch}\eta_D = \eta_w \eta_d$, provided that $\frac{\eta_{ch}\eta_D}{\eta_w} < 1$. We can then recognize similar building blocks, which we referred to as butterfly modules, in Section 2.10. Each of the two butterfly operators at the bottom will be labeled by $B_{\eta,\eta_w} = B^{a,b}_{\eta,\eta w,\eta w,1,1}$ and the butterfly operator in the upper part will be labeled by $B_{0.5,\eta_d} = B^{a,b}_{0.5,\eta_d,\eta d,1,1}$. In Appendix B, we derive the input-output relationships of each butterfly operator. After we establish entanglement either we perform directly a QKD measurement to obtain a raw key bit or we use a quantum repeater setup followed by QKD measurements. In the following section we will describe the entanglement swapping operation and how it is possible to extract a key for such a setup.

4.3.2 Entanglement swapping and QKD measurement

Figure 4.2(a) shows the entanglement swapping setup for the DLCZ and the SPS protocols. Entanglement is established between QM pairs $A-A'$ and $B'-B$ using either of protocols. A partial Bell-state measurement (BSM) on photons retrieved from the middle QMs A' and B' is then followed, which upon success, leaves A and B entangled. The BSM is effectively performed by a 50:50 beam splitter and single-photon detectors. To include the effects of the atomic-to-photonic

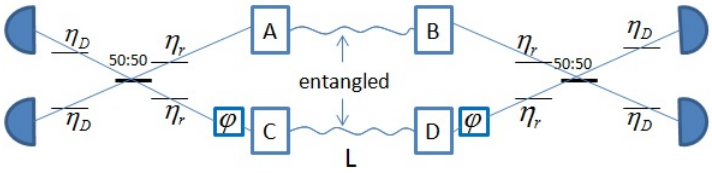

Figure 4.3: QKD measurements on two entangled pairs. Two pairs of memories, A-B and C-D, each share an entangled state. Memories are read out and the resulting photons are combined at a beam splitter and then detected. Different QKD measurements can be performed by choosing different phase shift values, φ, of 0 and $\pi/2$.

conversion efficiency and the photodetectors' quantum efficiency, we introduce two fictitious beam splitters with transmission coefficients η_r and η_D, respectively. All photodetctors in Fig. 4.2 will then have unity quantum efficiencies. Note that the parameter η_r also includes the memory decay during the storage time. The 50:50 beam splitter and the two fictitious beam splitters in Fig. 4.2(a) constitutes again a butterfly module, which can be simplified as in Fig. 4.2(b), with $\eta_s = \eta_r \eta_D$.

Alice and Bob use two butterfly operations to generate a raw key bit, as shown in Fig. 4.3. After generating entangled pairs over a distance L, Alice and Bob retrieve the states of memories and perform a QKD measurement on the resulting photons. They apply a random relative phase shift, φ, of either 0 or $\pi/2$, between their two fields. They will later, at the sifting stage, only keep data points where the same phase value is used by both parties. They then turn their sifted keys into a secure key by using privacy amplification and error reconciliation techniques. Eavesdroppers can be detected by following the BBM92 [17] or the Ekert protocol [18].

As mentioned in Sec. 4.1, previous analyses only provide the fidelity or the time required for a successful creation of an entangled state [37]. Instead, in Sec. 4.4, we will calculate the secret key generation rate for the SPS scheme and compare it with that of the DLCZ protocol reported in [61].

In our forthcoming analysis, we consider the multiple-memory configuration of Fig. 2.4(a), but our results are extensible to the case of Fig. 2.4(b) by accounting for the relevant prefactor. We use atomic-ensemble QMs, and we allow for memory decay and dephasing as explained next.

4.3.3 Memory decay and dephasing

Quantum memories are expected to decay and dephase while storing quantum states. In this Chapter, we model these two processes independently. The decay process, with a time constant T_1, can be absorbed in the retrieval efficiency of memories. If the retrieval efficiency immediately after writing into the memory is given by η_0, after a storage time T, the retrieval efficiency is given by $\eta_r = \eta_0 \exp(-T/T_1)$. Different memories in the multiple-memory setup of Fig. 2.4(a) undergo different decay times. In our analysis, we consider the worst case scenario where all memories have decayed for $T = L/c$, which is only applicable to the far-end memories. Under this assumption, η_r can be treated as a constant at all stages of entanglement swapping.

We model the memory dephasing via a dephasing channel, by which the probability of dephasing after a period T is given by $e_d = [1 - \exp(-T/T_2)]/2$. In the context of the QKD protocol in Fig. 4.3, this phase error is equivalent to the misalignment error in a conventional polarization-based BB84 protocol and has mostly the same effect. In our analysis, we neglect the effect of dephasing at the middle stages, and only consider its effect on the far-end memories used for the QKD protocol. Again, for the multiple-memory setup of Fig. 2.4(a), the relevant storage time is given by $T = L/c$ [58].

In the following section, we highlight the steps needed to find the secret key rate of the SPS protocol in the no-repeater and repeater cases.

4.4 Key rate analysis

In this section, the secure key generation rate for the SPS scheme proposed in [37] is calculated. In the case of no repeater nodes, using (2.9), the key rate will be bound by:

$$R_1 = \max\left[(1 - 2\,h(E_Q))\,\frac{P_S\,(L)}{2L/c}\,Q_{\text{click}}/2,\,0\right], \tag{4.1}$$

where Q_{click} is the probability of creating a sifted key bit by using two entangled pairs, E_Q is the QBER, and $P_S(L)$ is the probability of a successful entanglement generation over a length L. Here, we assume a biased basis choice to avoid an

extra factor of two reduction in the rate [42]. The full derivation of Q_{click} is given in Appendix B and is outlined below. The QBER,

$$E_Q = \frac{Q_{\text{EE}}}{Q_{\text{click}}}, \tag{4.2}$$

where Q_{EE} is the probability that Alice and Bob assign different bits to their sifted keys, is given in Appendix B as well.

From Eq. (2.9), the key rate in the one-node repeater case is lower bounded by

$$R_2 = \max\left[(1 - 2\,h(E_Q))\,\frac{P_S\,(L/2)}{2L/c}\,P_M\,Q_{\text{click}}/2,\,0\right], \tag{4.3}$$

where P_M is the probability of a successful BSM in an entanglement swapping operation.

As was shown in Sec. 4.3, the SPS scheme relies on simultaneous generation of single photons in two remote sites. Most practical schemes for the generation of single photons, however, suffer from the possibility of multiple-photon emissions. To address this issue, in this section, we consider non-ideal photon sources with nonzero probabilities for two-photon emissions, and find the secret key generation rates of Eqs. (4.1) and (4.3).

Suppose our photon sources emit one photon with probability $1-p$ and two photons with probability p. We, therefore, have the following input density matrix for the initial state of l and r sources in Fig. 4.1(a)

$$\rho_{lr}^{(in)} = \rho_l^{(in)} \otimes \rho_r^{(in)}, \tag{4.4}$$

where

$$\rho_j^{(in)} \equiv (1-p)\,|1\,\rangle_{jj}\,\langle 1| + p|2\,\rangle_{jj}\,\langle 2| \quad , \quad j = l,\, r. \tag{4.5}$$

In a practical regime of operation, $p \ll 1$; hence, in our following analysis, we neglect $O\,(p^2)$ terms corresponding to the simultaneous emission of two photons by both sources.

4.4.1 No-repeater case

In this section, we describe how we obtain parameters P_S, Q_{click}, and R_{QKD} for the setup in Fig. 4.1(a) and QKD measurements as in Fig. 4.3. The initial

density matrix in (4.4) goes through several butterfly modules, which has been described in Sec. 4.3. We can then find, ρ_{ALBR}, the joint state of the memories A and B and the optical modes entering detectors L and R in Fig. 4.1(b) by applying the butterfly operation three times, as follows

$$\rho_{ALBR} = B_{0.5,\eta_d}\left(B_{\eta,\eta_w}\left(\rho_l^{(in)}\right) \otimes B_{\eta,\eta_w}\left(\rho_r^{(in)}\right)\right). \tag{4.6}$$

According to the SPS protocol, a click on exactly one of the detectors L or R, in Fig. 4.1(b), would herald the success of entanglement distribution. This process can be modeled by applying proper measurement operators considering whether PNRDs or NRPDs are used. In this Chapter, we will use both kind of detectors, and label the corresponding measurement operator by M_{LR} in both cases. In the case of PNRDs, $M_{LR} = M_{LR}^{R}$, as in Eq. (2.13), and for NRPDs, $M_{LR} = M_{LR}^{NR}$, as given by Eq. (2.14).

After the measurement, the resulting joint state, ρ_{AB}, of quantum memories is given by:

$$\rho_{AB} = \frac{\mathrm{tr}_{L,R}\left(\rho_{ALBR} M_{LR}\right)}{P}, \tag{4.7}$$

where

$$P = \mathrm{tr}\left(\rho_{ALBR} M_{LR}\right) = \frac{P_S\left(L\right)}{2} \tag{4.8}$$

is the probability that the conditioning event M_{LR} occurs. The last equality is due to the symmetry assumption.

For QKD measurements, we assume two pairs of memories, A-B and C-D, are given in an initial state similar to that of Eq. (4.7). We use the scheme described in Fig. 4.3 to perform QKD measurements. For simplicity, we assume both users use zero phase shifts; other cases can be similarly worked out in our symmetric setup. In Fig. 4.3, the retrieval efficiency and the quantum detectors efficiency are represented by fictitious beam splitters with, respectively, transmission coefficient η_r and η_D. It is again possible to remodel the setup in Fig. 4.3 as shown in Fig. 4.2(b), and use the butterfly operation $B_{0.5,\eta_s}$, where $\eta_s = \eta_r\eta_D$. The density matrix right before photodetection in Fig. 4.3 is then given by $B_{0.5,\eta_s}\left(B_{0.5,\eta_s}\left(\rho_{AB} \otimes \rho_{CD}\right)\right)$, where one of the B-operators is applied to modes A and C, and the other one to modes B and D. Using this state, we find Q_{click} and E_Q as outlined in Appendix B. We have now all the ingredients to find the secret key rate of Eq. (4.1)

4.4.2 Repeater case

First, we consider the repeater setup with nesting level one in Fig. 4.2(a). We use the structure of Fig. 4.1(a) to distribute entanglement between A-A' and B'-B memories. The initial joint state of the system, $\rho_{AA'BB'} = \rho_{AA'} \otimes \rho_{BB'}$, can then be found, using Eq. (4.7), as described in the previous section. We then apply a BSM by reading memories A' and B' and interfering the resulting optical modes at a 50:50 beam splitter. Success is declared if exactly one of the detectors in Fig. 4.2(a) clicks. This can be modeled by applying measurement operators in Eqs. (2.13) and (2.14) , which results in

$$\rho_{AB} = \frac{\mathrm{tr}_{LR}\left(M_{LR}\rho'_{ALBR}\right)}{P_L}, \tag{4.9}$$

where $\rho'_{ALBR} = B_{0.5,\eta_s}\left(\rho_{AA'BB'}\right)$, where L and R represent the input modes to the photodetectors. Note that, in Fig. 4.2, the detectors have ideal unity quantum efficiencies. Moreover,

$$P_L = \mathrm{tr}\left(M_{LR}\rho'_{ALBR}\right) = P_M/2 \tag{4.10}$$

is the probability that only the left detector clicks in the BSM module of Fig. 4.2. A click on the right detector has the same probability by symmetry.

In order to find the secret key generation rate, we will follow similar steps to the no-repeater case. That is, we apply the butterfly operation to find relevant density matrices, from which Q_{click} and E_Q can be obtained. Now we can find the secret key rate given in Eq. (4.3). Using the same approach, and by using Eq. (4.3), we find the secret key generation rate for higher nesting levels. The details of which, have, however, been omitted.

4.5 Numerical results

In this section, we present numerical results for the secret key generation rate of the SPS protocol, versus different system parameters, in the no-repeater and repeater cases, and we compare them with that of the DLCZ protocol. Unless otherwise noted, we use the nominal values summarized in Table 4.1 for all the results presented in this Chapter.

η_w	0.5
η_D	0.3
η_0	0.7
d_c	10^{-6} per pulse
L_{att}	25 km
c	$2 \cdot 10^5$ km/s
T_1 (T_2)	∞

Table 4.1: Nominal values used in this Chapter.

4.5.1 SPS key rate versus system parameters

Source transmission coefficient

Figure 4.4 shows the secret key generation rate per memory, R_{QKD}, versus the source transmission coefficient η of the setup of Fig. 4.1(a), at $p = 0.001$ and $L = 250$ km. It can be seen that there exist optimal values of η for both repeater and no-repeater systems. Table 4.2 summarizes these optimum values for different nesting levels. The optimal value of η for the no-repeater system is higher than the repeater ones, and that is because of the additional entanglement swapping steps in the latter systems. Another remarkable feature in Fig. 4.4 is that the penalty of using NRPDs, versus PNRDs, seems to be little at $p = 10^{-3}$. PNRDs better show their advantage at higher values of p when double-photon terms become more evident.

The existence of an optimal value for η arises from a competition between the probability of entanglement distribution P_S, which grows with η, and P_{click}, which decreases with η. This has been demonstrated in the inset of Fig. 4.4. The latter issue is mainly because of the vacuum component in Eq. (2.12). In the case of the repeater system, P_M also decreases with η for the same reason, and that is why the optimal value of η is lower for repeater systems.

The optimum values of η in Fig. 4.4 are interestingly almost identical to the value of η that minimizes the total time for a successful creation of an entangled state, as prescribed in [37]. It is because, at a fixed distance, the QBER term in Eqs. (4.1) and (4.3) is mainly a function of the double-photon probability and the dark count rate, and it does not considerably vary with η. More generally, the

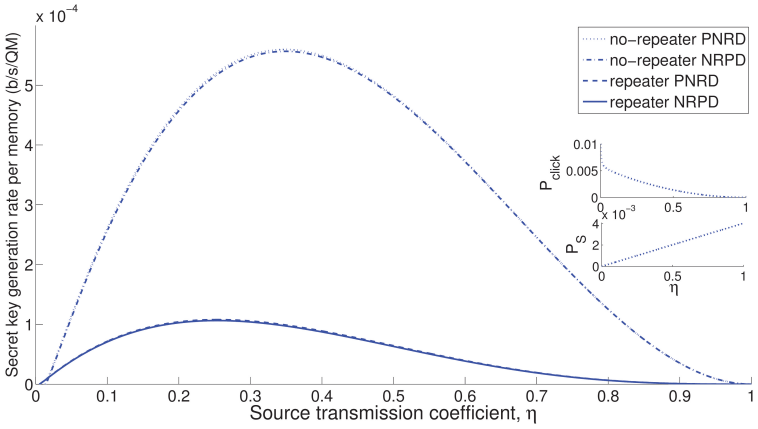

Figure 4.4: R_{QKD} versus the source transmission coefficient η for the PNRDs and NRPDs in the no-repeater and one-node repeater cases. Here, $p = 0.001$, $L = 250$ km, and $n = 1$ for the repeater system; other parameters are listed in Table 4.1.

nesting level	PNRD	NRPD
0	0.35	0.34
1	0.28	0.27
2	0.21	0.20*
3	0.12	0.11*

Table 4.2: Optimal values of η, at $p = 0.001$ and $L = 250$ km, for repeater and no-repeater systems, when PNRDs or NRPDs are used. The figures with an asterisk are approximate values.

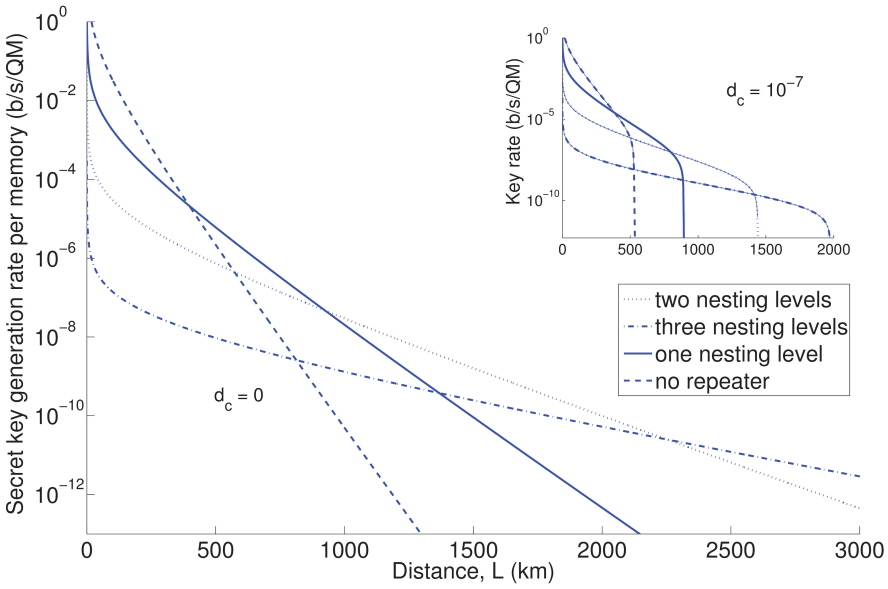

Figure 4.5: Key rate versus distance for up to three nesting levels at two different dark count rates at $p = 10^{-4}$. All other values are listed in Tables 4.1 and 4.2.

optimum values of η remain constant as in Table 4.2 so long as the error terms are well below the cut-off threshold in QKD.

Nesting levels and crossover distance

Figure 4.5 depicts the normalized secret key generation rate versus distance for different nesting levels. At $d_c = 0$, the slope advantage, proportional to $P_S(L/2^n)$, for higher nesting levels is clear in the figure. Because of additional entanglement swapping stages, the no-path-loss rate at $L = 0$ is, however, lower for higher nesting levels. That would result in crossover distances—at which one system outperforms another—once we move from one nesting level to its subsequent one. The crossover distance has architectural importance and will specify the optimum distance between repeater nodes.

The crossover distance is a function of various system parameters. As shown in the inset of Fig. 4.5, positive dark count rates can considerably change the crossover distance. By including dark counts in our analysis, there will be a cutoff security distance for each nesting level. By increasing the dark count rate,

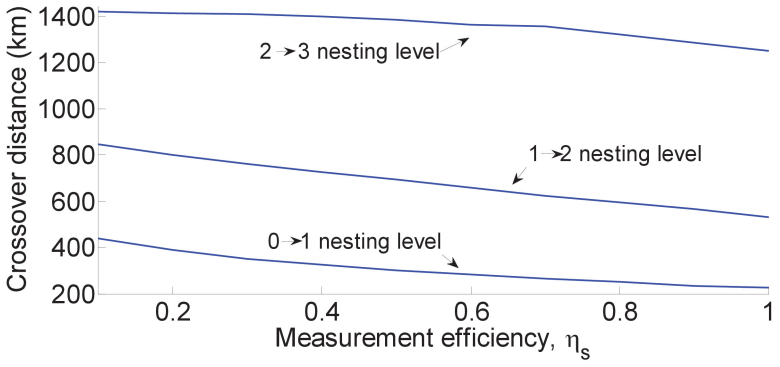

Figure 4.6: The crossover distance, at which a repeater system with nesting level n outperforms a system with nesting level $n-1$, as a function of measurement efficiency $\eta_s = \eta_r \eta_D$, at $p = 10^{-4}$. All other parameters are taken from Tables 4.1 and 4.2 except for the dark count, which is 10^{-7}.

these cutoff distances will decrease and become closer to each other. That would effectively reduce the crossover distance. At dark count rates as high as $d_c = 10^{-6}$, the superiority of 3 over 2 nesting levels at long distances would almost diminish as they both have almost the same cutoff distances.

The crossover distance will decrease if component efficiencies go up. This has been shown in Fig. 4.6 when the crossover distance is depicted versus measurement efficiency. The latter directly impacts the BSM success probability, P_M, and that is why the larger its value the lower the crossover distance. Larger values of η_w also reduce the vacuum component, thus enhancing the chance of success at the entanglement swapping stage.

It can be noted in Fig. 4.6 that, even for highly efficient devices, the optimum distance between repeater nodes would tend to lie at around 150-200 km. For instance at $L = 1000$ km, and with the nominal values used in this Chapter, the optimum nesting level is 2, which implies that the distance between two nodes of the repeater is 250 km. This could be a long distance for practical purposes, such as for phase stabilization, and that might require us to work at a suboptimal distancing. The latter would further reduce the secret key generation rate. Our result is somehow different from what is reported in [81, 83], albeit one should bear in mind the different set of assumptions and measures used therein.

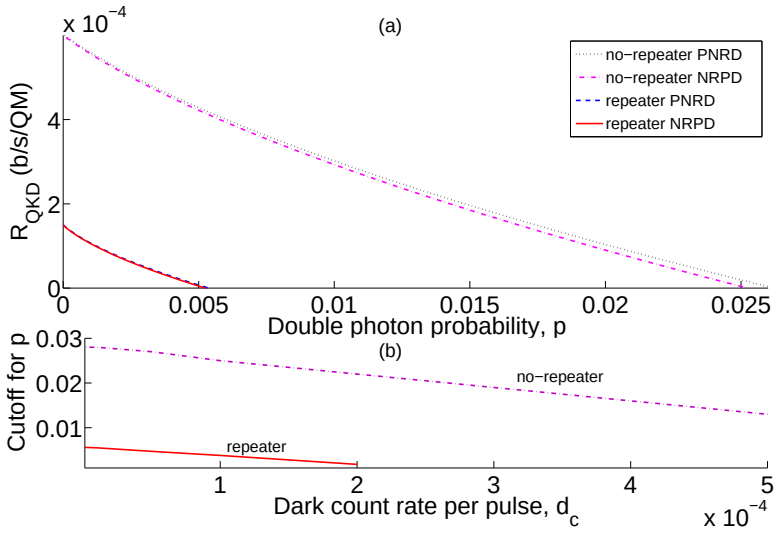

Figure 4.7: (a) Key rate versus double-photon probability, p, using PNRDs and NRPDs in the no-repeater and one-node repeater cases. (b) Cutoff double-photon probability, at which the key rate becomes zero, versus the dark count rate d_c. The higher the dark count rate, the less room for multi-photon errors. All graphs are at $L = 250$ km.

Double-photon probability

Figures 4.7 show the secret key generation rate for the SPS protocol, at the optimal values of η listed in Table 4.2, versus the double-photon probability p in the no-repeater and repeater cases. It can be seen that, in both cases, there exists a cutoff probability at which R_{QKD} becomes zero. This point corresponds to the threshold QBER of 11% from the Shor-Preskill security proof. In the case of QMs with sufficiently long coherence times, as is the case in Fig. 4.7, the QBER in our system stems from two factors: dark count and double-photon probability. The former is proportional to d_c/η_d and it comes into effect only when the path loss is significant. The latter, however, affects the QBER at all distances. To better see this issue, in Fig. 4.7(b), the cutoff probability is depicted versus the dark count rate. It can be seen that the cutoff probability linearly goes down with d_c, which confirms the additive contribution of dark counts and two-photon emissions to the QBER.

The cutoff probability at $d_c = 0$ deserves a particular attention. As can be seen in Fig. 4.7(b), for the no-repeater system, the maximum allowed value

nesting level	cutoff double-photon probability
0	2.5×10^{-2}
1	5.0×10^{-3}
2	1.8×10^{-3}
3	2.1×10^{-4}

Table 4.3: Cutoff double-photon probabilities when PNRDs are used for different nesting levels. The parameter values used are listed in Tables 4.1 and 4.2 .

of p is about 0.028 for PNRDs and 0.026 for NRPDs. This implies that the QBER in this case, at $d_c = 0$, is roughly given by $4p$. This can be verified by finding the contributions from two- and single-photon components in Eq. (4.5). We can then show that the QBER, at the optimal value of η in Table 4.2, is roughly given by $3(1+\eta)p \approx 4p$. Similarly, in the repeater case, one can show that each BSM almost doubles the contribution of two-photon emissions to the QBER. Considering that four pairs of entangled states is now needed, and that the chance of making an error for an unentangled pair is typically 1/2, the QBER is roughly given by $4 \times 2 \times 3(1+\eta)p/2 \approx 16p$, which implies that, to the first-order approximation, the maximum allowed value for p is about $0.11/16 = 0.0068$. Figure 4.7(a) confirms this result, where the cutoff probability is about 0.0056 for the PNRDs and 0.0054 for the NRPDs, corresponding to $E_Q \approx 20p$.

With a similar argument as above, one may roughly expect a factor of 4-to-5 increase in the QBER for each additional nesting level. This implies that for a repeater system with nesting level 3, we should expect a QBER around $500p$ just because of the double-photon emission. Table 4.3 confirms our approximation by providing the actual cutoff figures for different nesting levels. We discuss the practical implications of this finding later in this section.

Memory dephasing

Figure 4.8(a) shows the secret key generation rate per memory for the SPS protocol with NRPDs versus distance for two different values of the dephasing time, T_2, at $p = 10^{-3}$. It is clear that, by reducing the coherence time, the security distance drops to shorter distances. Whereas, at $T_2 = 100$ ms, the key rate remains

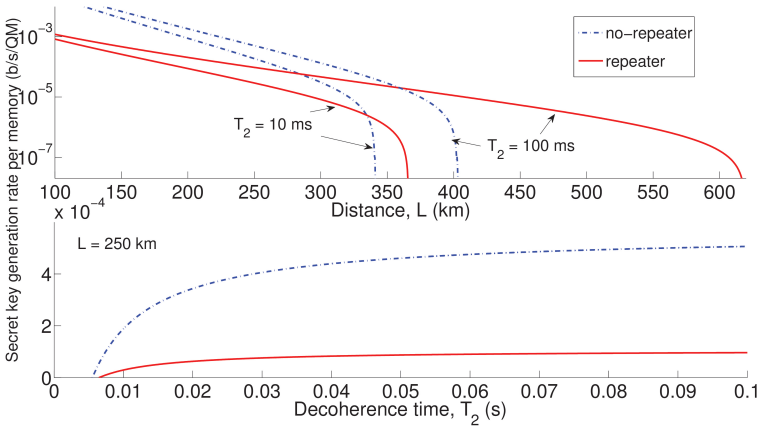

Figure 4.8: (a) The secret key generation rate versus distance for two values of decoherence time, $T_2 = 10$ ms and 100 ms. In (b) the secret key rate is plotted as a function of T_2 at $L = 250$ km. In both graphs, $p = 10^{-3}$.

the same as that of Fig. 4.5(b), at $T_2 = 10$ ms, both repeater and non-repeater systems would fall short of supporting distances over 360 km.

Figure 4.8(b) shows the secret key generation rate per memory versus T_2 at $L = 250$ km. There is a minimum required coherence time of around 5 ms below which we cannot exchange a secure key. This point corresponds to the 11% QBER mainly caused by the dephasing process. In fact, at this point, we have $E_Q \approx e_d = (1 - \exp[-L/(cT_2)])/2 = 0.11$, which implies that the maximum distance supported by our protocol is about $cT_2/4$. To be operating on the flat region in the curves shown in Fig. 4.8(b), one even requires a higher coherence time. In other words, the minimum required coherence time to support a link of length L is on the order of $10L/c$. This is in line with findings in [58]. Although not explicitly shown here, the same requirements are expected to be as well applicable to other QKD systems that rely on quantum repeaters.

4.5.2 SPS versus DLCZ

Figure 4.9 compares the secret key generation rate for the SPS protocol, found in this Chapter, with that of the DLCZ protocol as obtained in [61]. In both systems, we have assumed $d_c = 0$. All other parameters are as in Table 4.1. In both systems, we use the optimal setting in the PNRD case. The conclusion

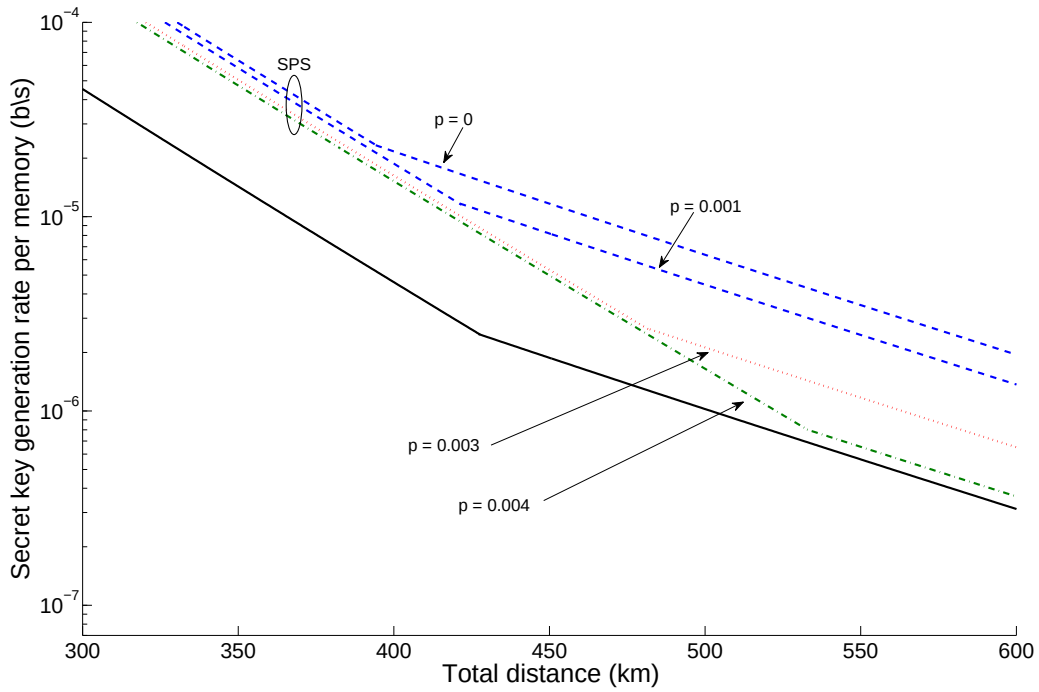

Figure 4.9: Comparison between the DLCZ and SPS protocols using PNRDs. For both systems, the better of repeater or non-repeater system is used. Both systems operate at their optimal setting: For the SPS protocol, the optimum value of η is used; for the DLCZ protocol, the optimum value of p_c is used. By varying the double-photon probability, p, in the SPS protocol, we find that the maximum p at which SPS outperforms DLCZ is around $p = 0.004$. In all curves, $d_c = 0$. All other parameters are taken from Tables 4.1 and 4.2.

would be similar if one uses NRPDs, as seen in all numerical results presented in this Chapter. For the SPS protocol, the optimal setting corresponds to the values of η in Table 4.2. In the DLCZ protocol, the adjustable parameter is the excitation probability p_c. Note that, whereas in the SPS protocol, the rate decreases monotonically with p, in the DLCZ protocol, it peaks at a certain value of p_c. That is because, in the SPS protocol, we use an on-demand source of photons, whereas in the DLCZ protocol, the heralding probability is proportional to p_c so is the ratio between double-photon and single-photon probabilities. The optimum value for the excitation probability is given by $p_c = 0.0243$ in the no-repeater case and $p_c = 0.0060$ in the one-node repeater case [61]. Note that the analysis in [61] accounts for all multi-excitation components in the initial state of the system. In all curves in Fig. 4.9, we have used the better of the repeater and no repeater systems at each distance. Our results show that the SPS protocol offers a higher key rate per memory than the DLCZ for on-demand single-photon sources with double-photon probabilities of 0.004 or lower. The advantage is however below one order of magnitude in most cases.

A key assumption in the results obtained above is the use of on-demand sources in the SPS protocol. The less-than one-order-of-magnitude difference between the two protocols can then be easily washed away if one uses single-photon sources with less than roughly 50% efficiencies. This means that the conventional methods for generating single photons, such as parametric downconversion or quantum dots, may not yet be useful in the SPS protocol. The partial memory-readout technique could, still, be a viable solution. In this scheme, we drive a Raman transition, as in the DLCZ protocol, in an atomic ensemble, such that with some probability p a Stokes photon is released. If we detect such a photon, then we are left with an ensemble, which can be partially read out with probability η to resemble the first part of the SPS protocol. One should, however, note that with limitations on the cutoff probability to be on the order of 10^{-4}–10^{-5}, it may take quite a long time to prepare such a source-memory pair. For instance, if the required p is 10^{-4}, and the efficiency of the collection and detection setup is 0.1, even if we run the driving pulse at a 1 GHz rate, it takes on average 0.1 ms to prepare the initial state. This time is comparable to the time that it takes for light to travel 100 km, which is on the same order of magnitude that we run our

cyclic protocol in Fig. 2.4(a). Considering a particular setup parameters, it is not then an obvious call to which of the DLCZ or SPS protocols performs better, and that underlines the importance of our theoretical analysis.

4.6 Conclusions

In this Chapter, we analyzed the SPS protocol proposed in [37] in terms of the secret key generation rate that it could offer in a QKD-over-repeater setup. This protocol belongs to a family of probabilistic quantum repeaters, and perhaps one of their best, inspired by the DLCZ proposal [72]. Our aim was to compare the SPS protocol, for QKD applications, with the original DLCZ protocol, as reported in [61], in a realistic scenario. To this end, we considered various sources of imperfections in our analysis and obtained the optimal regime of operation as a function of system parameters. We accounted for double-photon probabilities at the source and realized that, under Shor-Preskill's security-proof assumptions, its value should not exceed 0.11/4, in a direct-link scenario, and 0.11/20 in a one-node repeater case. We would expect the same scaling, if not worse, at higher nesting levels, which implied that for a repeater setup of nesting level 3, the double-photon probability must be on the order of 10^{-4} or lower. That would be a challenging requirement for on-demand single-photon sources needed in the SPS protocol. Under above circumstances, the advantage of the SPS protocol over the DLCZ would be marginal and would not exceed one order of magnitude of key rate in bit/s per memory. In our analysis, we also accounted for memory dephasing and dark counts. Our results showed that the minimum required coherence time for a link of length L is roughly given by $4L/c$, where c is the speed of light in the channel. The crossover distance at which we have to move up the nesting-level ladder varies for different system parameters. The optimum distancing between repeater nodes can nevertheless be typically as high as 150 km to 200 km depending on the measurement efficiency among other parameters. We noticed that, within practical regimes of operation, there would only be a minor advantage in using resolving photodetectors over more conventional threshold detectors. We emphasized that, because of using a normalized figure of merit

in our analysis, our results would be applicable to multi-memory and/or -mode scenarios.

The SPS quantum repeater protocol, while it enables us to reach large distances, requires the end users to have quantum memories in order to exchange a secret key. In order to simplify the equipment at the user's and to be able to exchange a key over long distances, we can use an MDI-QKD protocol combined with a quantum repeater setup. We will present this new scheme in the next Chapter.

Chapter 5

Long-Distance Trust-Free Quantum Key Distribution

5.1 Introduction

Future quantum communications networks will enable secure key exchange among remote users. They ideally rely on user friendly access protocols in conjunction with a reliable network of core nodes [84–86]. For economic reasons, they need to share infrastructure with existing and developing classical optical communication networks, such as passive optical networks (PONs) that enable fiber-to-the-home services [77, 87]. The first generation of quantum key distribution (QKD) networks are anticipated to rely on a *trusted* set of core nodes [88, 89]. This approach, although the only feasible one at the moment, may suffer from security breaches over the long run. In the future generations of quantum networks, this trust requirement can be removed by relying on entanglement in QKD protocols [31, 32, 90]. This can be facilitated via using the recently proposed measurement-device-independent QKD (MDI-QKD) [1, 73, 91, 92] at the access nodes of a PON [93] and quantum repeaters at the backbone of the network, as we consider in this Chapter. The former enables easy access to the network via low-cost optical sources and encoders, whereas the latter may rely on high-end technologies for quantum memories and gates. Both systems, however, rely on entanglement swapping, which makes them naturally merge together. More importantly, in

neither systems would we need to trust the intermediary nodes that perform Bell-state measurements (BSMs).

In this Chapter, we study the feasibility of such a *trust-free* hybrid scheme by finding the relationship between the achievable secret key generation rate as a function of various system parameters. We remark that this setup does not provide full device-independence but it removes the trust requirement from the intermediary network nodes that perform measurement operations. Our work provides insights into the feasibility of such systems in the future. Our scheme relies on conventional quantum repeaters, where quantum memories are entangled over large distances via successive entanglement swapping operations. Moreover, users can use imperfect single-photon sources or lasers.

MDI-QKD is an attractive candidate for the access part of quantum networks. First, it provides a means to secure key exchange without trusting measurement devices. This is a huge practical advantage considering the range of attacks on the measurement tools of QKD users [94–97]. Moreover, at the users' ends, it only requires optical encoders driven by weak laser pulses. That not only makes the required technology for the end users much simpler, but it also implies that the costly parts of the network, including detectors and quantum memories, are now shared between all networks users, and are maintained by service providers. One final advantage of MDI-QKD is its reliance on entanglement swapping, which makes its merging with quantum repeaters, also relying on the same technique, straightforward. This will help us develop quantum networks in several generations, where the compatibility of older, e.g. trusted-node, and newer, e.g., our trust-free, networks can be easily achieved.

In this Chapter, we focus on the probabilistic setups for quantum repeaters, and, among all possible options, we use the SPS protocol we studied in Ch. 4 [37]. In the previous Chapter, we compared the performance of the SPS protocol in the context of QKD, with several other alternatives, once imperfections in the SPSs are accounted for. We found that under realistic assumptions, this protocol is capable of providing the best (normalized) key rate versus distance behavior as compared to other protocols. The particular setup that we are going to consider in this Chapter is then a phase-encoded MDI-QKD setup, whose reach and rate

are improved by incorporating a repeater setup, as above, in between the two users.

We assume the multiple-memory configuration for the repeater system. It is worth noting that the easiest way to improve rate-vs-distance behavior is to add two quantum memories in the MDI-QKD setup as we discussed in Ch. 3 [2, 68, 98]. For the right setup and sets of devices, this approach will almost double the distance one can exchange secret keys without trusting middle nodes, but it is not scalable the same way that quantum repeaters are. It, nevertheless, provides a practical route toward building scalable quantum-repeater-based links.

This Chapter is structured as follows. In Sec. 5.2, we outline the contributions of this Chapter. In Sec. 5.3, we describe the trust-free QKD link setup. In Sec. 5.4, we describe how we analytically calculate the secret key rate for the setup under study when users are provided with imperfect SPSs and with coherent sources. In Sec. 5.5, we present the numerical results of the key rate versus the distance in two regimes of operation. Finally, in Sec. 5.6, we draw our conclusions.

5.2 This chapter's contribution

In this Chapter, we analytically determine the secret key rate of the phase-encoded MDI-QKD setup with quantum repeaters when users are provided with lasers, which emit coherent states, SPSs. For both sources, depending on the number of memories in use, we consider two regimes of operation: repeater-limited regime, if the number of memories is large, and source-limited regime, when the number of memories is small. We will give more details about these two regimes in the next section. Finally, we determine the crossover distance versus the memory reading efficiency, which takes into account the amplitude decay in the memories.

5.3 Setup description

In this section we first introduce the general idea behind our trust-free architecture and, then, explain the particular MDI-QKD and quantum-repeater protocols

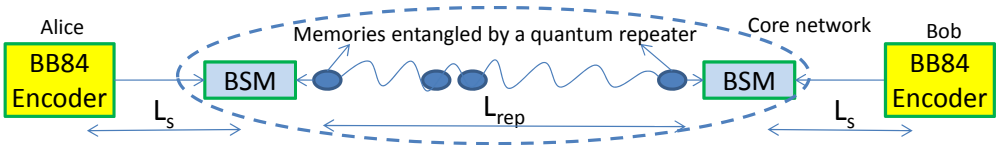

Figure 5.1: A general scheme for trust-free QKD links. Entangled states are created between internal nodes of the core network using quantum repeaters. The two BSMs will then enable an end-to-end MDI-QKD protocol.

considered for its implementation. Let us first consider the ideal scenario considered in Fig. 5.1. In this scheme, by using quantum repeaters, we distribute (polarization) entanglement between two memories apart by a distance L_{rep}. This operation is part of the core network and is facilitated by the service provider. On the users' end, each user is equipped with a BB84 encoder, which sends polarization-encoded single photons to a BSM module at a short distance L_s from its respective source. This resembles the access part of the network, where the BSM module is located at the nearest service point to the user. For each transmitted photon by the users, we need an entangled pair of memories to be read, i.e., their states need to be transferred into single photons. These photons will then interact with the users' photons at the two BSMs in Fig. 5.1.

The setup of Fig. 5.1 effectively enables an enlarged MDI-QKD scheme. In MDI-QKD, the two photons sent by Alice and Bob are directly interacting at a BSM module [1]. Here, by the use of entangled memories, it is as if the Alice's photon is being *teleported* to the other side, and will interact with the Bob's photon at the second BSM. The overall effect is, nevertheless, the same, and once Alice and Bob consider the possible rotations in the memory states corresponding to the obtained BSM results, they can come up with correlated or anti-correlated bits for their sifted keys. Post processing is then performed to convert these sifted keys to secret keys.

The same idea as in Fig. 5.1 can be implemented via phase-encoding techniques as shown in Fig. 5.2. Here, for simplicity, we have considered the dual-rail setup. The equivalent, and more practical, single-rail setup can also be achieved by time multiplexing as shown in [73]. In Fig. 5.2, the quantum repeater ideally leaves memories A_i-B_i, for $i = 1, 2$, in the state $|\psi_{\text{ent}}\rangle_{A_iB_i} = |0\rangle_{A_i}|1\rangle_{B_i} + |1\rangle_{A_i}|0\rangle_{B_i}$,

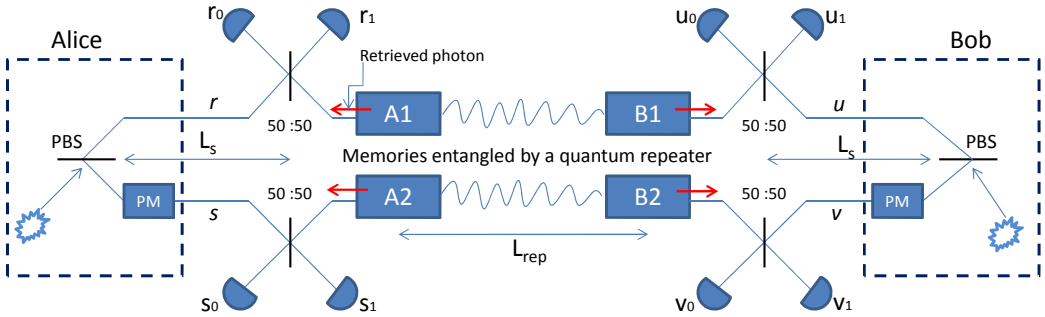

Figure 5.2: Schematic diagram for a trust-free QKD link based on phase encoding. Memories are entangled using the SPS repeater protocol. Here, PBS stands for polarizing beam splitter and PM stands for phase modulator.

where we have neglected normalization factors, and $|n\rangle_K$ represents n excitations in memory K. The implicit assumption is that the memory is of ensemble type so that it can store multiple excitations [71]. The phase encoding that matches this type of entangled states is as follows. Alice and Bob encode their states either in the z or in the x basis. Alice encodes her bits in the z basis by sending, ideally, a photon in the r or in the s mode. This can be achieved by sending horizontally or vertically polarized pulses to the polarizing beam splitter (PBS) at the encoder. The same holds for Bob and his u and v modes. As for the x basis, we can send a $+45°$-polarized signal through the PBS to generate a superposition of r (u) and s (v) modes for Alice (Bob) state. Alice (Bob) encodes her (his) bits by choosing the phase value of the phase modulator (PM), ϕ_A (ϕ_B), to be either 0 or π.

The BSMs used in the scheme of Fig. 5.2 are probabilistic ones. They will be successful if exactly two detectors, one from the top branch, and one from the bottom one, click. We recognize two types of detection. For the Alice's side (and, similarly, for the Bob's side), type I refers to getting a click on r_0-s_0 or on r_1-s_1. Type II refers to the case when r_0-s_1 or r_1-s_0 click. In order to get one bit of sifted key, Alice and Bob must use the same basis and both BSMs in Fig. 5.2 must be successful. Depending on the results of these BSMs and the chosen basis by the two parties, Alice and Bob may end up with correlated or anti-correlated bits, where in the latter case, Bob will flip his bit. Table 5.1 summarizes the bit assignment procedure for our scheme. Note that these BSMs can be performed by untrusted parties.

Basis	Alice BSM	Bob BSM	Bit assignment
z	type I/II	type I/II	Bob flips his bit
x	type I (II)	type I (II)	Bob keeps his bit
x	type I (II)	type II (I)	Bob flips his bit

Table 5.1: Bit assignment protocol depending on the results of the two BSMs.

The repetition rate for our scheme is a function of several factors. In order to do a proper BSM, for each photon sent by the users, there must be *two* entangled pairs of memories ready to be read. In principle, the fastest that we can repeat our scheme is the minimum of the maximum source repetition rate, R_S, and half the entanglement generation rate of the quantum repeater, $R_{\text{rep}}/2$. In the multiple-memory configuration of Fig. 2.4(a) and in the limit of $NR_{\text{ent}}(L)/c \gg 1$, R_{rep} is given by

$$R_{\text{rep}}(L) = N_{\text{QM}} R_{\text{ent}}(L), \tag{5.1}$$

where $N_{\text{QM}} = 2^{n+1}N$ is the total number of logical memories in Fig. 2.4(a).

We therefore consider two regimes of operation. If $R_S > R_{\text{rep}}/2$, we then run our encoders at a rate equivalent to $R_{\text{rep}}/2$ and will look at the achievable key rate per QM used. We refer to this as the repeater-limited regime. If $R_S < R_{\text{rep}}/2$, i.e., when for every photon sent, there will be more than two entangled pairs ready, then we run our scheme at the rate R_S and will look at the key rate per transmitted pulse as a figure of merit. We refer to this scenario by source-limited regime.

In the following, we describe the quantum repeater protocol used in our scheme as well as different types of (imperfect) sources that users may use. Later, we look at the achievable key rates once certain imperfections are considered in our setup.

5.3.1 Source imperfections

In our work, we consider two types of sources for the end users. The first type, which we will use as a point of reference for comparison purposes, is an imperfect

SPS, with the following output state

$$\rho_j = (1-p)\,|1\rangle_{jj}\langle 1| + p\,|2\rangle_{jj}\langle 2|, \quad j = A,\, B, \tag{5.2}$$

where p is the probability to emit two, rather than one, photons. In practical regimes of operation, $p \ll 1$, hence, in our analysis, we neglect the simultaneous emission of two photons by both sources. The second type of source considered is a phase-randomized coherent source. In both cases, we use the decoy-state technique by either varying p or the intensity. In the case of the coherent sources, Alice (Bob) will send $\mu = |\alpha|^2$ ($\nu = |\beta|^2$) photons on average for her (his) main signal states. Other values will be used for decoy pulses. Our analysis here only considers the case when there are infinitely many decoy states in use, although in practice we expect to achieve the same performance by using just a small number of decoy states [91].

5.3.2 Quantum repeater setup

We use the SPS repeater protocol, which was analyzed in Chapter 4. We consider the SPS protocol with imperfect SPSs as in Fig. 5.2 for establishing entanglement on each elementary link. Then, using entanglement swapping operations, we extend the entanglement distance up to two nesting levels in a multiple-memory configuration. By considering writing and reading efficiencies for the QMs in use, respectively, denoted by η_w and η_r, we use the results of the previous Chapter to find the relevant density matrices, $\rho_{A_iB_i}$ for $i = 1, 2$, for memories entangled by the SPS protocol for different values of p and for different nesting levels n. The amplitude decay of QMs can then be modeled with η_r. Other sources of imperfections considered throughout the Chapter are the path loss given by $\eta_{\text{ch}}(l) = \exp(-l/L_{\text{att}})$, photodetectors' quantum efficiency, η_D, and photodetectors' dark count per pulse given by d_c.

We describe in the following section the procedure we use to find the secret key rate for such a hybrid scheme.

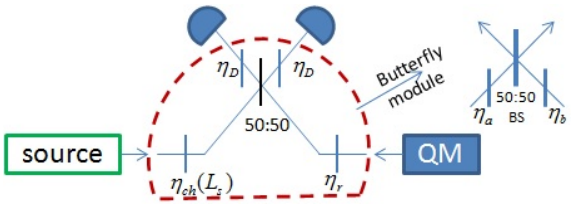

Figure 5.3: BSM module with generic transmission coefficient represented by fictitious beam splitters. In our setup, η_a is the path loss; η_b is the reading efficiency and η_D is the detection efficiency.

5.4 Secret key generation rate

In this section, we find the secret key generation rate, R_{QKD}, per logical memory used, for the scheme of Fig. 5.2 under the normal mode of operation when no eavesdropper is present. We consider two types of sources as discussed in Sec. 5.3.1.

5.4.1 Imperfect SPSs

Here, Alice and Bob each use an SPS with the output state as given by Eq. (5.2) in their encoder. In the limit of an infinitely long key and a sufficiently large number of QMs, their normalized secret key generation rate per employed memory is lower bounded by

$$\begin{aligned} R_{\mathrm{QKD}} &= \frac{\min(R_S, R_{\mathrm{rep}}/2)}{N_{\mathrm{QM}}} \\ &\times \max\left\{Q_{11}^{z}\left(1-h\left(e_{11}^{x}\right)\right)-Q_{pp}^{z} f\, h\left(E_{pp}^{z}\right), 0\right\} \end{aligned} \tag{5.3}$$

Appendix C provides us with the full derivation of the relevant terms in Eq. (5.3). Our general approach to find these terms is as follows. For any basis $\Phi = x, z$ and any possible encoded state $\rho_{\mathrm{enc}}^{\Phi} = \rho_{rs} \otimes \rho_{uv}$ by Alice and Bob, the initial state of the system including entangled memories A_1-B_1 and A_2-B_2 is given by

$$\rho_{\mathrm{in}}^{\Phi} = \rho_{\mathrm{enc}}^{\Phi} \otimes \rho_{A_1B_1} \otimes \rho_{A_2B_2} \tag{5.4}$$

where $\rho_{A_iB_i}$ has been obtained in Ch. 4. Once memories are read, their states will be transferred to photonic states, which we denote by the same label as their original memories. In that case, optical fields corresponding to modes r and A_1, as well as the other three pairs of modes in Fig. 5.2, would undergo through the

setup shown in Fig. 5.3, where $\eta_a = \eta_r \eta_D$ and $\eta_b = \eta_{\text{ch}}(L_s)\eta_D$. The equivalent sub-module in Fig. 5.3 is what we refer to as an asymmetric butterfly module (see Fig. 2.7(c)), whose operation is denoted by $B^{ab}_{\eta_a \eta_b} = B^{a,b}_{0.5,\eta_a,\eta_b,1,1}$ when it acts on two incoming modes a and b. In Appendix A, we have derived the output states of a butterfly module for relevant number states at its input. Using those results, we can then find the pre-measurement state right before the photodetection at the BSM modules by

$$\rho^{\Phi}_{\text{out}} = B^{rA_1}_{\eta_a \eta_b} \otimes B^{sA_2}_{\eta_a \eta_b} \otimes B^{uB_1}_{\eta_a \eta_b} \otimes B^{vB_2}_{\eta_a \eta_b}(\rho^{\Phi}_{\text{in}}). \tag{5.5}$$

Note that we have already accounted for the quantum efficiency of photodetectors in our butterfly modules. The probability for a particular pattern of clicks on detectors r_i, s_j, u_k, and v_l, for $i, j, k, l = 0, 1$, is given by

$$P_{r_i s_j u_k v_l}(\rho^{\Phi}_{\text{enc}}) = \text{tr}\left(\rho^{\Phi}_{\text{out}} M_{r_i} M_{s_j} M_{u_k} M_{v_l}\right), \tag{5.6}$$

where for $x = r, s, u, v$

$$M_{x_0} \equiv M^{NR}_{x_0 x_1} \tag{5.7}$$

is the measurement operator to get a click on detector x_0 but not on x_1 as explained in Eq. (2.14). One can define a similar operator $M_{x_1} \equiv M^{NR}_{x_1 x_0}$, when x_1 clicks, but no x_0. The relevant terms in Eq. (5.3) can now be calculated by using Eq. (5.6) as shown in Appendix C.

5.4.2 Coherent sources

In this section we replace the SPSs with lasers sources and use the decoy-state technique to exchange secret keys. This is a more user friendly approach as the complexity of the required equipment for the end users would be minimized. In the limit of infinitely many decoy states, infinitely long key, and sufficiently large number of memories, the secret key generation rate per logical memory used is lower bounded by

$$\begin{aligned} R_{\text{QKD}} &= \frac{\min(R_S, R_{\text{rep}}/2)}{N_{\text{QM}}} \\ &\times \max\left\{Q^z_{11}\left(1 - H\left(e^x_{11}\right)\right) - Q^z_{\mu\nu} f\, H\left(E^z_{\mu\nu}\right), 0\right\}, \end{aligned} \tag{5.8}$$

where $Q^z_{\mu\nu}$ is the probability of a successful click pattern in the z basis when Alice and Bob send phase-randomized coherent pulses, respectively, with mean photon number $\mu = |\alpha|^2$ and $\nu = |\beta|^2$ and $E^z_{\mu\nu}$ is the QBER in the z basis in the same scenario.

The procedure to find $Q^z_{\mu\nu}$ and $E^z_{\mu\nu}$ is the same as what we outlined in Eqs. (5.4)-(5.6). The only difference here is that in our butterfly modules, we now need to know the output of the module to coherent states in one input port, for the signal coming from the users, and number states in the other, representing the state of QMs. Table C.1 in Appendix C provides us with the input-output relations for a range of relevant input states. We can then find the relevant terms of the key rate, as shown in Appendix C.

5.5 Numerical results

In this section, we present numerical results for the secret key generation rate of our long-haul trust-free QKD link versus different system parameters. We look at two regimes of operation; the *source-limited* regime when memories are abundant and we are slowed down by source rates, i.e., $2R_S < R_{\text{rep}}$, versus the *repeater-limited* regime when the rate limitations come from the quantum repeater side, i.e., $2R_S > R_{\text{rep}}$. In the latter case, we should still satisfy the condition $NR_{\text{ent}}(L)L/c \gg 1$ in order that Eq. (5.1) remains valid. We have used Maple 15 to analytically derive expressions for Eqs. (5.3) and (5.8). Unless otherwise noted, we use the nominal values summarized in Table 3.1.

The first thing to obtain is the optimum intensity for our decoy-state coherent state scheme. Let us assume that in the symmetric scenario, as considered in this section, Alice and Bob both use the same intensity value $\mu = |\alpha|^2 = \nu$ for their coherent signal states. Figure 5.4 shows the secret key generation rate per pulse versus $|\alpha|$ for (a) different values of d_c and (b) different values of p of the quantum repeater at $L_{\text{rep}} = 100$ km. We assume that $2R_S < R_{\text{rep}}$ and the plotted curves represent $R_{\text{QKD}}N_{\text{QM}}/R_S$ in Eq. (5.8). It can be seen in both figures that $|\alpha| = 1$ almost gives us the maximum rate in most scenarios. The optimal value is to some extent a function of d_c as can be seen in Fig. 5.4(a). By increasing d_c, the optimal intensity slightly decreases. Dark count represents the main source of

η_w	0.78
η_D	0.93
η_r	0.87
d_c	10^{-9}
L_{att}	25 km
c	$2 \cdot 10^5$ km/s
T_1 (T_2)	∞
p	10^{-4}
Distance between user and measurement apparatus, L_S	5 km
f	1.16

Table 5.2: Nominal values used in our numerical results.

error in the z basis, therefore, when d_c increases, the tolerance for the multiple-photon terms in a coherent state decreases, hence the maximum allowed value of $|\alpha|$ will go down as well. This leads to a slightly shifted curve and therefore lower values for the optimal values of $|\alpha|$. On the contrary, $E^z_{\mu\nu}$ is not affected much by the double-photon probability p and there is not much difference in the optimal intensity when p increases as shown in Fig. 5.4(b). We also obtain the same optimal values of $|\alpha|$ for nesting levels one and two in the repeater-limited regime. Throughout this section, we then use $|\mu| = |\nu| = 1$ in our calculations.

5.5.1 Rate versus distance

Figures 5.5 and 5.6 show the secret key generation rate, at the optimal value of intensity, versus the total distance, $L = 2L_s + L_{\text{rep}}$, between Alice and Bob. In both figures, we assume L_s is a fixed short distance resembling the length of the access network. We vary L_{rep} then to effectively increase the link distance. Figure 5.5 shows the secret key generation rate per transmitted pulse in the source-limited regime, whereas Fig. 5.6 represents the key rate per logical memory used in the repeater-limited regime. In both cases we consider SPSs at $p = 10^{-4}$ as well as coherent decoy states. The difference in the performance of the systems relying on these sources, as expected, is low, and that again confirms the possibility, and practicality, of using the decoy-state technique for end-user

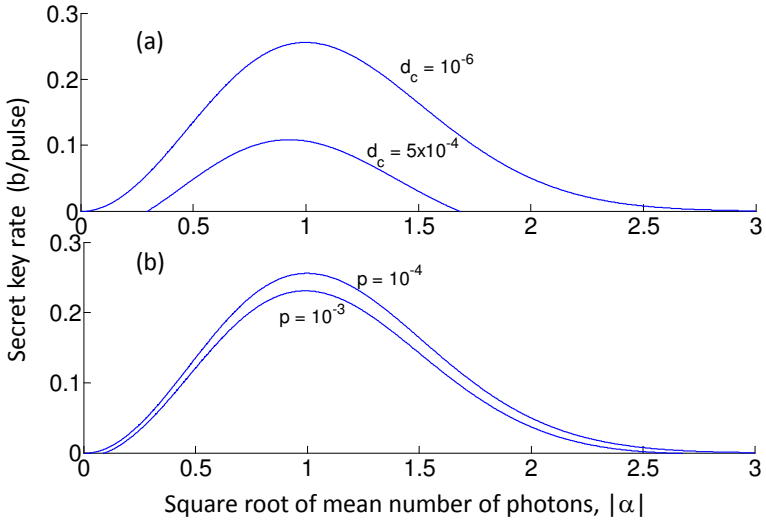

Figure 5.4: Secret key generation rate per pulse versus $|\alpha| = |\beta|$ for different values of (a) the dark count and (b) the repeater's double photon probability. Here, $L_{\text{rep}} = 100$ km and the other values are as in Table 5.2.

devices. The cut-off security distance, i.e., the distance beyond which secure key exchange is not possible, almost doubles every time we increase the nesting level so long as memories decoherence rates are correspondingly low. This distance at $n = 0$ is about 800 km, similar to the no-memory case for the parameter values used and at $n = 1$ and $n = 2$, respectively, reaches around 1500 km and 2500 km. Security distances are slightly higher for the single-photon than coherent-state sources.

The slope of the curves in Fig. 5.5 is different than that of Fig. 5.6. In Fig. 5.5 curves are almost flat until they reach their cut-off distances. That has two reasons. First, in the source-limited regime, R_{QKD} is proportional to the constant R_S, whereas, it scales with R_{ent}, which exponentially decays with L_0 [99], in the repeater-limited regime. Second, and this is common in both figures, in the absence of the decoherence, the fidelity of the entangled states generated by our probabilistic repeater effectively reaches a constant value once we increase the distance [61]. That means that the double-photon-driven error terms in the key rate are almost fixed until dark count becomes significant and the rate goes down.

The implications on the achievable key rate is also different in the two figures.

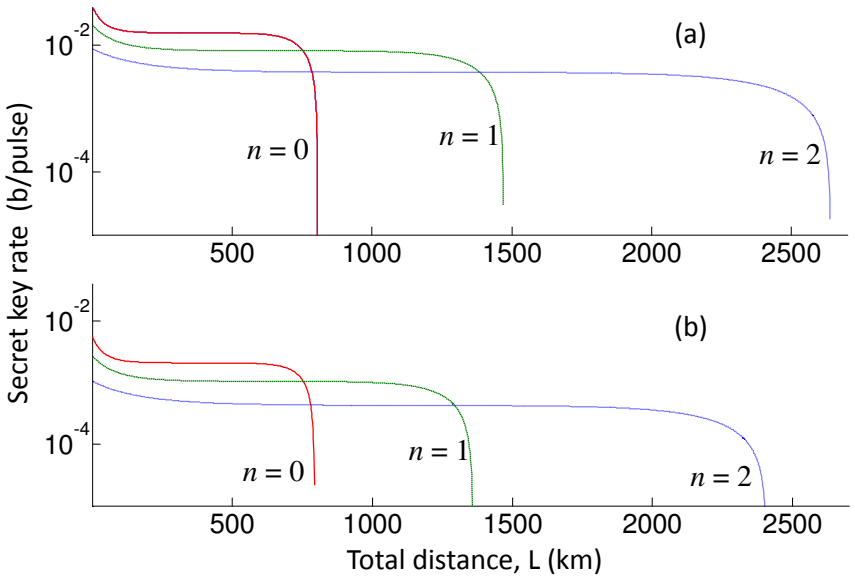

Figure 5.5: Secret key generation rate per transmitted pulse, in the source-limited regime, versus distance when (a) imperfect SPSs and (b) decoy coherent states are used.

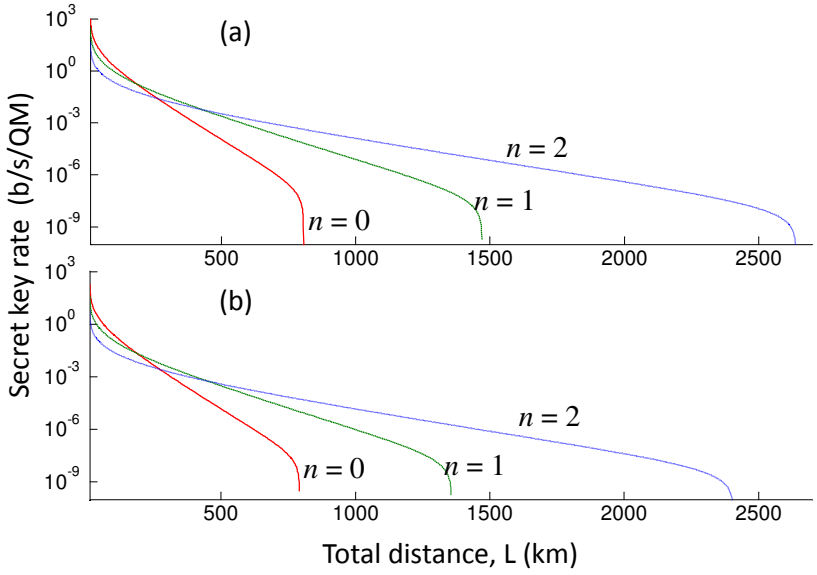

Figure 5.6: R_{QKD}, in the repeater-limited regime, versus distance when (a) imperfect SPSs and (b) decoy coherent states are used.

Largest distance (km)	zero nesting level	one nesting level	two nesting levels
imperfect single photon source	800	1460	2640
coherent source	790	1355	2400

Table 5.3: Largest achievable distances for zero, one and two nesting levels when imperfect single photon and coherent source are used for the inefficiencies values listed in Tab. 5.2.

In Fig. 5.5, at a nominal distance of $L = 1000$ km and a source rate of $R_S = 1$ GHz, the key rate is in the region of Mb/s. The assumption $2R_S < R_{\text{rep}}$, however, implies that we need something on the order of 10^{15} QMs in our core network to work in the source-limited regime, which seems, at the moment, quite impractical. In the repeater-limited regime, we still need many memories to obtain a decent rate. For instance, at $L = 1000$ km, we would need around 1 billion QMs to get a key rate on the order of kb/s. This is still a huge number of resources for the current technology of QMs. This is in fact the same number of memories in use in our classical computers, which was perhaps inconceivable a few decades ago. Progress in solid-state QMs is much needed to meet the above requirements.

5.5.2 Crossover distance

The different slopes in Figs. 5.5 and 5.6 result in appreciably different values for crossover distances, i.e., the distances where one nesting level outperforms its previous one. In the source-limited regime, in Fig. 5.5, the curve for $n = 1$ outperforms that of $n = 0$ for L greater than around 750 km. The crossover distance to nesting level 2 is then around 1400 km. These are quite large distances, which imply that L_0, the spacing between adjacent nodes in our quantum repeater, could be as large as 700 km. This sparse location of memories in the system has some advantages in the sense that resources are more or less centralized, rather than distributed, but at the same time it imposes harder conditions on maintaining phase and polarization stability over such long distances. In the repeater-limited regime of Fig. 5.6, the nodes are much closer as now the crossover distance is around/below 500 km. This implies that the optimum architecture of our core

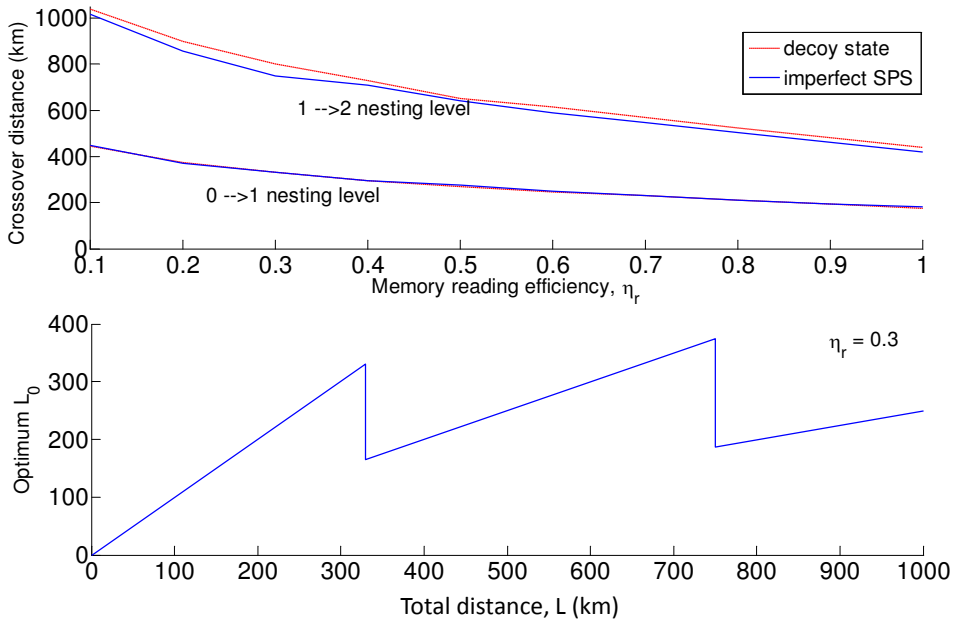

Figure 5.7: (a) Crossover distance versus QM's recall efficiency in the repeater-limited regime. (b) Optimum spacing L_0 between adjacent nodes of a quantum repeater at $\eta_r = 0.3$.

network relies on, among other things, how many QMs are available at the time of development.

The crossover distance is also a function of the efficiency of various system parameters. In Fig. 5.7(a), we have looked at the crossover distance as a function of the recall efficiency, η_r, in the repeater-limited regime. This is particularly important, because η_r implicitly accounts for the amplitude decay in memories. As expected, the crossover distance decreases with the recall efficiency as there would be less of rate reduction because of the BSM operation. Figure 5.7(b) shows this effect on the optimal value of L_0. It can be seen that at $\eta_r = 0.3$ the optimal spacing is much wider than what can be obtained from Fig. 5.6 at $\eta_r = 0.87$. It can be seen that the curve for optimal L_0 is non-continuous as we have limited our study to the case when the number of segments in a repeater setup is a power of 2. By developing new repeater protocols for arbitrarily number of segments, one can get a smoother curve for optimal L_0. At $\eta_r = 0.3$, L_0 is on average around 250 km for the set of parameters as in Table 5.2.

5.6 Conclusions

In this Chapter we combined MDI-QKD with a quantum repeater setup in order to obtain a long-distance key exchange scheme without the need to trust any of the intermediate nodes or measurement tools. This trust-free network could be used in future generations of quantum networks, where the easy cost-efficient access to the network would be facilitated by laser-based encoders and the repeater technology, at the backbone, would be maintained by the service provider. We considered a particular entanglement distribution scheme for our quantum repeater, which relied on imperfect single-photon sources. We merged memories entangled by this probabilistic repeater setup with photons sent and phase encoded by the two users via two BSM modules. We showed that it would be possible to exchange secret keys up to over 2500 km using repeaters with two nesting levels. It turned out that in order to get a key rate on the order of 1 kb/s, one may need to employ and control billions of memories at the core network. We also showed that the network architecture depends on the number of memories at stake. In the limit of infinitely many memories, the repeater nodes would be sparsely located, although each node may contain a large number of memories. Our results showed how challenging it would be to build trust-free quantum communication networks.

Chapter 6

Conclusions

In this thesis we have addressed the impact of imperfect ensemble-based quantum memories on the performance of several QKD and quantum repeater systems through the analysis of the secret key rate. We have meticulously considered major sources of non-idealities in real implementation of such systems.

We started with analyzing the effects of multiple excitations of QMs on the memory-assisted MDI-QKD system, which is supposed to beat conventional no-memory QKD links in rate and distance. We found that multiple excitations deteriorate the performance of the memory-assisted MDI-QKD system to the extent that they can no longer beat their no-memory counterparts.

Then, we considered a probabilistic quantum repeater setup, whose entanglement distribution is performed by the single-photon source protocol (SPS protocol). Whereas the first probabilistic quantum repeater protocol (DLCZ) is strongly affected by multiple excitations in QMs, the main limitation of the SPS protocol comes from using not perfect single photon sources. Therefore, we compared the two protocols in a practical scenario, and we determined the range of values for the double photon probability for which the SPS protocol outperforms the DLCZ protocol. This advantage is conditional on having on-demand single photon sources. However, we estimated the maximum distance achievable in a quantum repeater setup for a few nesting levels and we also determined the crossover distance for the system under consideration.

Finally, we combined MDI-QKD protocol with a quantum repeater setup. This trust-free network has the advantage of not relying on the security of mea-

surement devices and its architecture enables future generations of quantum networks to provide easy access to their users. We showed that it would be possible to exchange secret keys up to over 2500 km using repeaters with two nesting levels. It turned out that in order to get a key rate on the order of 1 kb/s, one may need to employ and control billions of memories at the core network. Our results showed how challenging it would be to build trust-free quantum communications networks.

Future directions of research that I am planning to pursue include:

- considering quantum repeater setups that do not rely on quantum memories. In Sec. 2.7, I mentioned two deterministic quantum repeaters, which can reach very high key rates. While the performance is very high, their requirements are still to hard to meet. I will aim at relaxing some constraints in order to have more feasible quantum repeater setups.

- comparing a probabilistic quantum repeater protocol with satellite QKD, which is the other main approach to reach larger distances. In [100], authors analyze the performance of low Earth orbit satellite quantum communication, by considering several sources of errors. Satellite QKD seems to be an appealing option for long-distance quantum communications, although such sources of errors may constitute an obstacle to a feasible implementation. A comparison between quantum repeaters and satellite QKD can shed light on which of the two approaches is more practicable in the imminent future.

- considering different source states (cat-states) in an MDI-QKD setup that are less affected by channel loss. Channel loss is the main obstacle to reach long distances. Cat states seem to be very resilient to channel loss. I will investigate a quantum repeater setup when cat-states are used as sources by calculating the key rate as the main figure of merit.

Appendix A

A.1 MDI-QKD with imperfect sources: Key rate parameters

In this Appendix we will derive the terms in Eq. (3.11) for the setup of Fig. 3.2, considering path loss, quantum efficiency η_d, dark count rates d_c, double-photon probability p, and misalignment probability e_d assuming that no eavesdropper is present. This provides us with an estimate of how well the system performs under normal conditions. In Eq. (3.11), Y_{11}^z and e_{11}^x have already been calculated in [73]. Here, we will derive the other two terms Q_{pp}^z and E_{pp}^z. In the z basis, a successful click event at the BSM module is corresponded to different key bits at Alice's and Bob's ends. We can therefore separate the input states that result in correct inference of bits versus those causing errors. The input states that result in correct inference of bits are those that correspond to sending different bits by Alice and Bob given by

$$\rho_C^{(\text{in})} = [\rho_{r_A}(p) \otimes \rho_{s_B}(p) + \rho_{s_A}(p) \otimes \rho_{r_B}(p)]/2, \tag{A.1}$$

whereas

$$\rho_E^{(\text{in})} = [\rho_{r_A}(p) \otimes \rho_{r_B}(p) + \rho_{s_A}(p) \otimes \rho_{s_B}(p)]/2 \tag{A.2}$$

results in erroneous decisions. In above equations, $r_{A(B)}$ and $s_{A(B)}$ subscripts, respectively, refer to the r and s optical modes of Alice (Bob) in Fig. 3.2. Note that terms corresponding to $O(p^2)$ are neglected in Eqs. (A.1) and (A.2). Each of the above states undergoes a state transformation according to the butterfly

module in Fig. 2.8(c). The input-output relationships for this butterfly operation are given in Table A.1 for a range of input states of interest. The output states, for the input states as in Eqs. (A.1) and (A.2), are then given by

$$\rho_K^{(\text{out})} = B_{\eta_a,\eta_b}^{r_A r_B} \otimes B_{\eta_a,\eta_b}^{s_A s_B}(\rho_K^{(\text{in})}), \quad K = C, E \tag{A.3}$$

where $\eta_a = \eta_{\text{ch}}(L_A)\eta_D$, $\eta_b = \eta_{\text{ch}}(L_B)\eta_D$, $B_{\eta_a,\eta_b}^{r_A r_B} = B_{0.5,\eta_a,\eta_b,1,1}^{r_A r_B}$ and $B_{\eta_a,\eta_b}^{s_A s_B} = B_{0.5,\eta_a,\eta_b,1,1}^{s_A s_B}$, (see Fig. 2.7).

With the above output states in hand, one just needs to apply the relevant measurement operators to find all probabilities of interest. In particular, by denoting the probability that detectors r_i and s_j, $i, j = 0, 1$, click by

$$P_{r_i s_j}^{(K)} = \text{tr}(\rho_K^{(\text{out})} M_{r_i} M_{s_j}), \quad K = C, E, \tag{A.4}$$

the probability that an acceptable click pattern occurs in the z basis, Q_{pp}^z, is given by

$$Q_{pp}^z = Q_C^z + Q_E^z \tag{A.5}$$

where

$$Q_K^z = \left(P_{r_0 s_0}^{(K)} + P_{r_1 s_1}^{(K)} + P_{r_0 s_1}^{(K)} + P_{r_1 s_0}^{(K)}\right)/2, \quad K = C, E. \tag{A.6}$$

Finally, E_{pp}^z is given by

$$E_{pp}^z = \frac{Q_{EE}^z}{Q_{pp}^z} \tag{A.7}$$

where $Q_{EE}^z = e_d Q_C^z + (1 - e_d) Q_E^z$. More generally, for any input state $\rho^{(\text{in})} = \rho_{r_A r_B s_A s_B}$, and for total transmissivities η_A and η_B for, respectively, Alice's and Bob's photons, we can define a gain parameter $Q^\beta(\eta_A, \eta_B; \rho_{r_A r_B s_A s_B})$ to represent the success probability, in basis $\beta = x, z$, for the BSM operation in Fig. 3.2. For any such input state, the probabilities of getting a click on detectors r_i and s_j, $i, j = 0, 1$, is given by

$$P_{r_i s_j}(\rho^{(\text{in})}) = \text{tr}(\rho^{(\text{out})} M_{r_i} M_{s_j}), \tag{A.8}$$

where

$$\rho^{(\text{out})} = B_{\eta_A,\eta_B}^{r_A r_B} \otimes B_{\eta_A,\eta_B}^{s_A s_B}(\rho^{(\text{in})}). \tag{A.9}$$

ρ_{AB}	$B^{AB}_{\eta_a,\eta_b}(\rho_{AB})$
$\|10\rangle\langle 10\|$	$\frac{\eta_a}{2}\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_a)\|00\rangle\langle 00\|$
$\|01\rangle\langle 01\|$	$\frac{\eta_b}{2}\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_b)\|00\rangle\langle 00\|$
$\|11\rangle\langle 11\|$	$\frac{1}{2}(\eta_a+\eta_b-2\eta_a\eta_b)\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right) + (1-\eta_a)(1-\eta_b)\|00\rangle\langle 00\|$ $+\frac{\eta_a\eta_b}{2}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|20\rangle\langle 20\|$	$(1-\eta_a)^2\|00\rangle\langle 00\| + \frac{\eta_a^2}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$ $+\eta_a(1-\eta_a)\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right)$
$\|02\rangle\langle 02\|$	$(1-\eta_b)^2\|00\rangle\langle 00\| + \frac{\eta_b^2}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$ $+\eta_b(1-\eta_b)\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right)$
$\|21\rangle\langle 21\|$	$(1-\eta_a)\left[\eta_a(1-\eta_b)+\frac{\eta_b}{2}(1-\eta_a)\right]\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right)$ $+\eta_a\left[\frac{\eta_a}{4}(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$ $+(1-\eta_a)^2(1-\eta_b)\|00\rangle\langle 00\| + \frac{3}{8}\eta_a^2\eta_b\left(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|\right)$
$\|12\rangle\langle 12\|$	$(1-\eta_b)\left[\eta_b(1-\eta_a)+\frac{\eta_a}{2}(1-\eta_b)\right]\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right)$ $+\eta_b\left[\frac{\eta_b}{4}(1-\eta_a)+\eta_a(1-\eta_b)\right]\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$ $+(1-\eta_b)^2(1-\eta_a)\|00\rangle\langle 00\| + \frac{3}{8}\eta_a\eta_b^2\left(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|\right)$
$\|10\rangle\langle 01\|$	$\frac{1}{2}\sqrt{\eta_a\eta_b}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right)$
$\|01\rangle\langle 10\|$	$\frac{1}{2}\sqrt{\eta_a\eta_b}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right)$
$\|11\rangle\langle 20\|$	$(1-\eta_a)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|11\rangle\langle 02\|$	$(1-\eta_a\eta_c)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|20\rangle\langle 11\|$	$(1-\eta_a)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|02\rangle\langle 11\|$	$(1-\eta_a)\sqrt{\frac{\eta_a\eta_b}{2}}\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right) + \frac{\eta_a\sqrt{\eta_a\eta_b}}{2\sqrt{2}}\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|20\rangle\langle 02\|$	$\frac{\eta_a\eta_b}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|02\rangle\langle 20\|$	$\frac{\eta_a\eta_b}{4}\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)$
$\|21\rangle\langle 12\|$	$+\frac{3}{8}\eta_a\eta_b\sqrt{\eta_a\eta_b}\left(\|30\rangle\langle 30\| - \|03\rangle\langle 03\|\right)$ $+\sqrt{\eta_a\eta_b}(1-\eta_a)(1-\eta_b)\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right)$ $+\frac{\eta_c^2}{2}\sqrt{\eta_a\eta_b}\left[\eta_a(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|12\rangle\langle 21\|$	$+\frac{3}{8}\eta_a\eta_b\sqrt{\eta_a\eta_b}\left(\|30\rangle\langle 30\| - \|03\rangle\langle 03\|\right)$ $+\eta_c\sqrt{\eta_a\eta_b}(1-\eta_a)(1-\eta_b)\left(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|\right)$ $+\frac{\eta_c^2}{2}\sqrt{\eta_a\eta_b}\left[\eta_a(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|\right)$
$\|22\rangle\langle 22\|$	$(1-\eta_a)^2(1-\eta_b)^2\|00\rangle\langle 00\| + +\frac{3}{8}\eta_a^2\eta_b^2\left(\|40\rangle\langle 40\| + \|04\rangle\langle 04\|\right)$ $+(1-\eta_a)(1-\eta_b)\left[\eta_a(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|\right)$ $+\frac{3}{4}\eta_a\eta_b\left[\eta_a(1-\eta_b)+\eta_b(1-\eta_a)\right]\left(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|\right)$ $+\frac{1}{4}\left[\eta_a^2(1-\eta_b)^2+\eta_b^2(1-\eta_a)^2\right]\left(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|\right)\|$

Table A.1: The input-output relationship for the asymmetric butterfly module of Fig. 2.8(c). For the sake of brevity, here, we have only included the terms that provide us with nonzero values after applying the measurement operation. More specifically, we have removed all *asymmetric* density matrix terms, such as $|10\rangle\langle 01|$ or $|01\rangle\langle 10|$, for which the bra state is different from the ket state, from the output state.

With the above notation, we obtain

$$Q^{\beta}(\eta_A, \eta_B; \rho^{(\text{in})}) = P_{r_0 s_0}(\rho^{(\text{in})}) + P_{r_1 s_1}(\rho^{(\text{in})}) \\ + P_{r_0 s_1}(\rho^{(\text{in})}) + P_{r_1 s_0}(\rho^{(\text{in})}). \tag{A.10}$$

The total gain for the basis $\beta = x, z$ is then given by

$$Q^{\beta}(\eta_A, \eta_B) = \sum_{\text{all input states } \rho} Q^{\beta}(\eta_A, \eta_B; \rho) \Pr(\rho) \tag{A.11}$$

Similarly, we also define $Q_C^{\beta}(\eta_A, \eta_B)$ to be the probability to get a successful BSM *and* Alice and Bob end up with correct inference of their bits:

$$Q_C^{\beta}(\eta_A, \eta_B) = \sum_{\text{all input states } \rho} \sum_{\substack{\text{all correct detection} \\ \text{pairs } (r_i, s_j) \text{ for input } \rho}} P_{r_i s_j}(\rho) \Pr(\rho). \tag{A.12}$$

Likewise, $Q_E^{\beta}(\eta_A, \eta_B) = Q^{\beta}(\eta_A, \eta_B) - Q_C^{\beta}(\eta_A, \eta_B)$ denotes the probability to get a successful BSM and Alice and Bob end up with incorrect inference of their bits. Finally, error terms can be defined as $e^{\beta} Q^{\beta} = Q_E^{\beta}$ calculated at the point (η_A, η_B). We use the above relationships in the next section.

A.2 MDI-QKD with imperfect memories: Key rate parameters

In this section we will derive the terms in Eq. (3.20) for the setup of Fig. 3.7, considering path loss, quantum efficiency η_D, dark count rates d_c, excitation probability p of the memories, and memories' amplitude decay assuming that no eavesdropper is present. We will follow the same procedure as in Appendix A.1 to separate the terms that result in error versus correct key bits. The general idea is to find the post-measurement density matrix of memories for any relevant input state upon a successful side-BSM event. Once both sets of memories are loaded, we apply the middle BSM operation and find relevant probabilities of interest.

The setup of Fig. 3.7 can be thought of three asymmetric MDI-QKD setups, where memories link them together. The first and second systems are those

that are involved with the loading process. They include the photons entangled with memories, e.g. P_1 and P_2 on Alice side, with those sent by the users. The third one is centered around the middle BSM and the photons retrieved from the memories. Here we use the general notation introduced in Eqs. (A.8)-(A.12) to calculate the relevant gain and error parameters. In order to do so, we need to first find the input state for the final stage of BSM. For any input state $\rho_A^{(\mathrm{in})}$ sent by Alice, we can find the post-measurement state $\rho_A^{(\mathrm{pm})}(r_i, s_j; \rho_A^{(\mathrm{in})})$ of the memories A_1 and A_2 upon a click on detectors r_i and s_j, for $i, j = 0, 1$, as follows

$$\rho_A^{(\mathrm{pm})}(r_i, s_j; \rho_A^{(\mathrm{in})}) = \frac{\mathrm{tr}_{P_1,P_2,r_A,s_A}(\rho_A^{(\mathrm{out})} M_{r_i} M_{s_j})}{\mathrm{tr}(\rho_A^{(\mathrm{out})} M_{r_i} M_{s_j})}, \tag{A.13}$$

where

$$\rho_A^{(\mathrm{out})} = B^{r_A P_1}_{\eta_a,\eta_D} \otimes B^{s_A P_2}_{\eta_a,\eta_D}(\rho_A^{(\mathrm{in})} \otimes \rho_{P_1}\rho_{P_2}), \tag{A.14}$$

where $\eta_a = \eta_{\mathrm{ch}}(L/2)\eta_D$ and $\rho_{P_i} = \mathrm{tr}_{A_1}(|\psi\rangle_{A_1P_1}\langle\psi|)$, for $i = 1, 2$. Similarly, one can find the post-measurement state for B_1-B_2 memories and denote it by $\rho_B^{(\mathrm{pm})}(r_m, s_n; \rho_B^{(\mathrm{in})})$ once detectors r_m and s_n, for $m, n = 0, 1$, click on the side BSM of Bob. The final parameter we need from the loading stage is the loading probability, i.e., the probability to get a successful side BSM which is given by

$$P_{\mathrm{load}} = Q^z(\eta_{\mathrm{ch}}(L/2)\eta_D, \eta_D; |10\rangle_{r_A s_A}\langle 10| \otimes \rho_{P_1}\rho_{P_2}). \tag{A.15}$$

In order to apply the middle BSM on the post-measurement states $\rho_A^{(\mathrm{pm})}$ and $\rho_B^{(\mathrm{pm})}$, One must consider the random nature of the loading process. Given that one set of the memories can be loaded earlier than the other, the former will undergo some amplitude decay before being read for the final BSM. That would result in an imbalanced middle BSM, where the reading efficiency for one memory could be lower than that of the other. To fully capture this random storage time, following the analysis and notations used in [2], let us consider two geometric random variables N_A and N_B corresponding to the number of attempts until Alice memories (A_1, A_2) and Bob memories (B_1, B_2) are, respectively, loaded. Therefore, the number of rounds needed to load both sets of memories will be given by $\max\{\mathrm{N_A}, \mathrm{N_B}\}$. The effective reading efficiency for memories $K = A, B$

will then be given by

$$\eta_{rK} = \begin{cases} \eta_{r0}, & \text{if memory K is late} \\ \eta_r\left(t = |N_A - N_B|T\right), & \text{if memory K is early} \end{cases}, \tag{A.16}$$

where T is the repetition period for the protocol, determined by the writing time into memories.

With all above considerations in mind, we obtain

$$Y_{11}^{\mathrm{QM}} = \frac{1}{N_L(P_{\mathrm{load}}, P_{\mathrm{load}}) + N_r} \mathrm{E}\left\{Q^z\left(\eta_{rA}\eta_d,\, \eta_{rB}\eta_d\right)\right\} \tag{A.17}$$

where $\mathrm{E}\{\cdot\}$ is the expectation value operator with respect to N_A and N_B; Q^z is the total gain in Eq. (A.11), where the input states ρ in the sum cover all possible post-measurement states that can be obtained for different states sent by Alice and Bob; and $N_L = \mathrm{E}\{\max(\mathrm{N_A}, \mathrm{N_B})\}$ and N_r are obtained in [2].

Similarly, the QBER terms in Eq. (3.20) can be obtained from the following

$$e_{11;\beta}^{\mathrm{QM}} \mathrm{E}\left\{Q^\beta\left(\eta_{rA}\eta_D,\, \eta_{rB}\eta_D\right)\right\} = \mathrm{E}\left\{Q_E^\beta\left(\eta_{rA}\eta_D,\, \eta_{rB}\eta_D\right)\right\}, \quad \beta = x, z, \tag{A.18}$$

where, again, the sum in Eq. (A.12) are taken over all possible post-measurement states obtained from Eq. (A.13).

Finally, to calculate the expected value terms in the above equations, one

needs to use the following relationships:

$$
\begin{aligned}
S_{A<B}(\delta) &= \frac{P_A P_B (1-P_B) e^{-\delta}}{[1-(1-P_A)(1-P_B)]\,[1-(1-P_B)e^{-\delta}]} \\
S_{B<A}(\delta) &= \frac{P_A P_B (1-P_A) e^{-\delta}}{[1-(1-P_A)(1-P_B)]\,[1-(1-P_A)e^{-\delta}]} \\
\mathrm{E}\{\eta_{rA}\} &= \eta_{r0}\left(\frac{P_B}{1-(1-P_A)(1-P_B)} + S_{A<B}(T/T_1)\right) \\
\mathrm{E}\{\eta_{rB}\} &= \eta_{r0}\left(\frac{P_A}{1-(1-P_A)(1-P_B)} + S_{B<A}(T/T_1)\right) \\
\mathrm{E}\{\eta_{rA}\eta_{rB}\} &= \eta_{r0}^2 P_0\left(\frac{1}{1-(1-P_A)e^{-T/T_1}} + \frac{1}{1-(1-P_B)e^{-T/T_1}} - 1\right) \\
\mathrm{E}\{\eta_{rA}^2\} &= \eta_{r0}^2\left(\frac{P_B}{1-(1-P_A)(1-P_B)} + S_{A<B}(2T/T_1)\right) \\
\mathrm{E}\{\eta_{rB}^2\} &= \eta_{r0}\left(\frac{P_A}{1-(1-P_A)(1-P_B)} + S_{B<A}(2T/T_1)\right) \\
\mathrm{E}\{\eta_{rA}^2\eta_{rB}\} &= \eta_{r0}^3\left(P_0 + S_{B<A}(T/T_1) + S_{A<B}(2T/T_1)\right) \\
\mathrm{E}\{\eta_{rA}\eta_{rB}^2\} &= \eta_{r0}^3\left(P_0 + S_{A<B}(T/T_1) + S_{B<A}(2T/T_1)\right) \\
\mathrm{E}\{\eta_{rA}^2\eta_{rB}^2\} &= \eta_{r0}^4 P_0\left(\frac{1}{1-(1-P_A)e^{-T/T_1}} + \frac{1}{1-(1-P_B)e^{-T/T_1}} - 1\right),
\end{aligned}
\tag{A.19}
$$

where $P_A = P_B = P_{\mathrm{load}}$ is the loading probability for Alice and Bob's memories.

Appendix B

In this Appendix, we find input-output relationships for the butterfly module in Fig. 2.7(a) and 2.7(b). We do this in the number-state representation, only for the relevant input states in Eq. (4.6).

Table B.1 provides the output state for the butterfly operation $B_{\eta,\eta_w} = B_{\eta,\eta_w,eta_w,1,1}$ when there is exactly one or two photons at one of the input ports. These are the only relevant terms in the input states in Eqs. (4.4) and (4.5). Using Table B.1, we find $B_{\eta,\eta_w}(\rho_l^{(in)}) \otimes B_{\eta,\eta_w}(\rho_r^{(in)})$, to be used in Eq. (4.6).

The last operation required in Eq. (4.6) is the symmetric butterfly operation $B_{0.5,\eta_d}$. Table B.2 lists the input-output relationships for all relevant input terms in our system for the more general operation $B_{0.5,\eta_x}$. Note that by choosing $\eta_x = \eta_s$, we can use the same relationships for the measurement modules used in entanglement swapping and QKD of Figs. 4.2 and 4.3, respectively. For the sake of brevity, in Table B.2, we have only included the terms that provide us with nonzero values after applying the measurement operation. More specifically, we

ρ_{in}	$B_{\eta,\eta_w}(\rho_{in})$
$\|10\rangle\langle 10\|$	$\eta\eta_w\|01\rangle\langle 01\| + \eta_w\sqrt{\eta(1-\eta)}(\|10\rangle\langle 01\| + \|01\rangle\langle 10\|)$ $+\eta_w(1-\eta)\|10\rangle\langle 10\| + (1-\eta_w)\|00\rangle\langle 00\|$
$\|20\rangle\langle 20\|$	$(1-\eta_w)^2\|00\rangle\langle 00\| + 2\eta\eta_w(1-\eta_w)\|01\rangle\langle 01\| + \eta\eta_w^2(1-\eta)(\|20\rangle\langle 02\| + \|02\rangle\langle 20\|)$ $+2\eta_w(1-\eta_w)\sqrt{\eta(1-\eta)}(\|10\rangle\langle 01\| + \|01\rangle\langle 10\|) + \eta^2\eta_w^2\|02\rangle\langle 02\|$ $+\eta_w^2(1-\eta)\sqrt{2\eta(1-\eta)}(\|20\rangle\langle 11\| + \|11\rangle\langle 20\|)$ $+2\eta_w(1-\eta)(1-\eta_w)\|10\rangle\langle 01\| + \eta_m^2(1-\eta)^2\|20\rangle\langle 20\|$ $+\eta\eta_w^2\sqrt{2\eta(1-\eta)}(\|02\rangle\langle 11\| + \|11\rangle\langle 02\|) + 2\eta\eta_w^2(1-\eta)\|11\rangle\langle 11\|$

Table B.1: The input-output relationship for the B_{η,η_w} butterfly of Fig.2.7(a).

have removed all *asymmetric* density matrix terms, such as $|10\rangle\langle 01|$ or $|01\rangle\langle 10|$, for which the bra state is different from the ket state, in the output state.

B.1 Derivation of key rate parameters for the SPS quantum repeater protocol

In this section, we find the gain and the QBER for the QKD scheme of Fig. 4.3. Let us assume that the memory pairs AB and CD are already entangled via the no-repeater or the one-node repeater scheme described in Sections 4.4.1 and 4.4.2. In the case of SPS protocol, their state is, respectively, given by Eqs. (4.7) and (4.9). The density matrix right before photodetection in Fig. 4.3 is then given by $\rho_{ABCD} = B_{0.5,\eta_s}\left(B_{0.5,\eta_s}\left(\rho_{AB}\otimes\rho_{CD}\right)\right)$, where one of the B-operators is applied to modes A and C, and the other one to modes B and D. Using Table B.2, we can calculate the exact form of ρ_{ABCD}.

The most general measurement on the modes entering the photodetectos of Fig. 4.3, namely, A, B, C, and D, can be written in terms of the following measurement operators:

$$M_{abcd} = |a\rangle_{AA}\langle a|\otimes|b\rangle_{BB}\langle b|\otimes|c\rangle_{CC}\langle c|\otimes|d\rangle_{DD}\langle d| \tag{B.1}$$

for PNRDs, where a, b, c, $d = 0, 1$ and $|k\rangle_K$ represents a Fock state for the optical mode $K = A, B, C, D$. In the case of NRPDs, we only need to replace $|1\rangle_{KK}\langle 1|$ with $(I_K - |0\rangle_{KK}\langle 0|)$, where I_K is the identity operator for mode K.

Similarly, we can define the corresponding probabilities to the above measurement operators as follows

$$P_{abcd} = Tr\left(\rho_{ABCD}M_{abcd}\right). \tag{B.2}$$

The explicit forms for Q_{click} and E_{Q} are then given by

$$Q_{\text{click}} = Q_C + Q_E \tag{B.3}$$

and

$$Q_{\text{EE}} = e_d Q_C + (1-e_d)Q_E, \tag{B.4}$$

ρ_{in}	$B_{0.5,\eta_x}(\rho_{in})$
$\|10\rangle\langle 10\|$	$\frac{\eta_x}{2}(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)\|00\rangle\langle 00\|$
$\|01\rangle\langle 01\|$	$\frac{\eta_x}{2}(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)\|00\rangle\langle 00\|$
$\|11\rangle\langle 11\|$	$\eta_x(1-\eta_x)(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^2\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|)$
$\|20\rangle\langle 20\|$	$\eta_x(1-\eta_x)(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^2\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}\|11\rangle\langle 11\|$ $+\frac{\eta_x^2}{4}(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|)$
$\|02\rangle\langle 02\|$	$\eta_x(1-\eta_x)(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^2\|00\rangle\langle 00\| + \frac{\eta_x^2}{2}\|11\rangle\langle 11\|$ $+\frac{\eta_x^2}{4}(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|)$
$\|21\rangle\langle 21\|$	$\frac{3}{2}\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^3\|00\rangle\langle 00\|$ $+\frac{5}{4}\eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|) + \frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|)$ $+\frac{1}{8}\eta_x^3(\|21\rangle\langle 21\| + \|12\rangle\langle 12\|) + \frac{\eta_x^2}{2}(1-\eta_x)\|11\rangle\langle 11\|$
$\|21\rangle\langle 21\|$	$\frac{3}{2}\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + (1-\eta_x)^3\|00\rangle\langle 00\|$ $+\frac{5}{4}\eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|) + \frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|)$ $+\frac{1}{8}\eta_x^3(\|21\rangle\langle 21\| + \|12\rangle\langle 12\|) + \frac{\eta_x^2}{2}(1-\eta_x)\|11\rangle\langle 11\|$
$\|10\rangle\langle 01\|$	$\frac{1}{2}\eta_x(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|)$
$\|01\rangle\langle 10\|$	$\frac{1}{2}\eta_x(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|)$
$\|11\rangle\langle 20\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|11\rangle\langle 02\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|20\rangle\langle 11\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|02\rangle\langle 11\|$	$\frac{\sqrt{2}}{2}\eta_x(1-\eta_x)(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \frac{1}{2\sqrt{2}}\eta_x^2(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$
$\|21\rangle\langle 12\|$	$\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$ $+\frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| - \|03\rangle\langle 03\|) + \frac{1}{8}\eta_x^3(\|12\rangle\langle 12\| - \|21\rangle\langle 21\|)$
$\|12\rangle\langle 21\|$	$\eta_x(1-\eta_x)^2(\|10\rangle\langle 10\| - \|01\rangle\langle 01\|) + \eta_x^2(1-\eta_x)(\|20\rangle\langle 20\| - \|02\rangle\langle 02\|)$ $+\frac{3}{8}\eta_x^3(\|30\rangle\langle 30\| - \|03\rangle\langle 03\|) + \frac{1}{8}\eta_x^3(\|12\rangle\langle 12\| - \|21\rangle\langle 21\|)$
$\|22\rangle\langle 22\|$	$(1-\eta_x)^4\|00\rangle\langle 00\| + 2\eta_x(1-\eta_x)^3(\|10\rangle\langle 10\| + \|01\rangle\langle 01\|) + \eta_x^2(1-\eta_x)^2\|11\rangle\langle 11\|$ $+\frac{3}{2}\eta_x^3(1-\eta_x)(\|30\rangle\langle 30\| + \|03\rangle\langle 03\|) + \frac{1}{2}\eta_x^3(1-\eta_x)(\|21\rangle\langle 21\| + \|12\rangle\langle 12\|)$ $\frac{5}{2}\eta_x^2(1-\eta_x)^2(\|20\rangle\langle 20\| + \|02\rangle\langle 02\|) + \frac{3}{8}\eta_x^4(\|40\rangle\langle 40\| + \|04\rangle\langle 04\|) + \frac{1}{4}\eta_x^4\|22\rangle\langle 22\|$

Table B.2: The input-output relationship for a symmetric butterfly module of Fig.2.7(b). The notation used is similar to that of Table B.1.

where e_d is the dephasing (misalignment) error, and

$$Q_C = \begin{cases} (1-d_c)^2(P_{1100}+P_{0011}+d_c(P_{1000}+P_{0100}+P_{0010}+P_{0001})+2d_c^2P_{0000}), \text{ PNRD} \\ \left(\frac{d_c^2}{2}-d_c+1\right)(P_{1100}+P_{0011})+d_c(1-\frac{d_c}{2})(P_{1001}+P_{0110}) \\ +\frac{d_c}{2}(2-d_c)(P_{1000}+P_{0100}+P_{0010}+P_{0001})+\frac{d_c^2}{2}(2-d_c)^2P_{0000} \\ +\frac{1}{2}(P_{1110}+P_{1101}+P_{0111}+P_{1011})+\frac{d_c}{2}(2-d_c)(P_{1010}+P_{0101})+\frac{1}{2}P_{1111}, \text{ NRPD} \end{cases} \tag{B.5}$$

is the probability that Alice and Bob assign identical bits to their raw keys if there is no misalignment, and

$$Q_E = \begin{cases} (1-d_c)^2(P_{1001}+P_{0110}+d_c(P_{1000}+P_{0100}+P_{0010}+P_{0001})+2d_c^2P_{0000}), \text{ PNRD} \\ \left(\frac{d_c^2}{2}-d_c+1\right)(P_{1001}+P_{0110})+\frac{d_c}{2}(2-d_c)(P_{1000}+P_{0100}+P_{0010}+P_{0001}) \\ +\frac{d_c^2}{2}(2-d_c)^2P_{0000}+\frac{1}{2}(P_{1110}+P_{1101}+P_{0111}+P_{1011}) \\ +\frac{d_c}{2}(2-d_c)(P_{1100}+P_{1010}+P_{0011}+P_{0101})+\frac{1}{2}P_{1111}, \text{ NRPD} \end{cases} \tag{B.6}$$

is the probability that they make an erroneous bit assignment in the absence of misalignment.

Appendix C

C.1 Derivation of the key rate terms for MDI-QKD and quantum repeater protocol

In this Appendix, we derive the key rate terms in Eqs. (5.3) and (5.8) under the normal mode of operation when no eavesdropper is present. We use the formulation developed in Eqs. (5.4)-(5.6) to obtain $\Gamma^z_{11} = Y^z_{11}$, $\epsilon^x_{11} = e^x_{11}$, $\Gamma^z_{pp} = Q^z_{pp}$, $\epsilon^z_{pp} = E^z_{pp}$, $\Gamma^z_{\mu\nu} = Q^z_{\mu\nu}$, and $\epsilon^z_{\mu\nu} = E^z_{\mu\nu}$, where new unifying notations Γ and ϵ are used in this section.

Let $\rho^{\Phi}_{\text{enc}}(mn)$ denote the output state of Alice and Bob's encoders for, respectively, sending bits m and n, for $m, n = 0, 1$, in basis Φ. With the above notation, the probability that an acceptable click pattern occurs in basis Φ, $\Gamma^{\Phi}_{\gamma\delta}$, is given by

$$\Gamma^{\Phi}_{\gamma\delta} = \sum_{i,j,k,l,m,n=0,1} P_{r_i s_j u_k v_l}(\rho^{\Phi}_{\text{enc}}(mn))/4, \tag{C.1}$$

where $\gamma = \delta = 1$ refers to the case when Alice and Bob are sending exactly one photon each; when $\gamma = \delta = p$, imperfect SPSs are used and when $\gamma = \mu$ and $\delta = \nu$ coherent states with mean photon number μ and ν, are, respectively, in use. In above, some of the successful click patterns would result in errors in the end, while the other in correct sifted key bits. By separating these two components, we obtain

$$\Gamma^{\Phi}_{\gamma\delta} = \Gamma^{\Phi}_{\gamma\delta;C} + \Gamma^{\Phi}_{\gamma\delta;E}, \tag{C.2}$$

where $\Gamma^{\Phi}_{\gamma\delta;C(E)}$ represents the click terms that result in correct (erroneous) infer-

ρ_{AB}	$\mathrm{tr}\left(M_{x_0} B^{AB}_{\eta_a \eta_b}\left(\rho_{AB}\right)\right)$
$\lvert\alpha 0\rangle\langle\alpha 0\rvert$	$(1-d_c)\left[e^{-\frac{\eta_a}{2}\mu}\left(1-e^{-\frac{\eta_a}{2}\mu}\right)+d_c e^{-\eta_a\mu}\right]$
$\lvert\alpha 1\rangle\langle\alpha 1\rvert$	$(1-d_c)\left[\frac{\eta_b}{2}e^{-\frac{\eta_a}{2}\mu}\left(1+\frac{\eta_a}{2}\mu\right)+e^{-\frac{\eta_a}{2}\mu}\left(1-\eta_b\right)\left(1-e^{-\frac{\eta_a}{2}\mu}\right)\right.$ $\left.+d_c\left(1-\eta_b\right)\left(1-e^{-\eta_a\mu}\right)\right]$
$\lvert\alpha 2\rangle\langle\alpha 2\rvert$	$(1-d_c)\left\{\frac{\eta_b^2}{4}e^{-\frac{\eta_a}{2}\mu}\left[1+\frac{\eta_a^2}{4}\mu^2\left(\frac{1}{2}-8\,e^{-\frac{\eta_a}{2}\mu}\right)+\eta_a\mu\right]\right.$ $+\eta_b e^{-\frac{\eta_a}{2}\mu}\left(1-\eta_b\right)\left(1+\frac{\eta_a}{2}\mu\right)+e^{-\frac{\eta_a}{2}\mu}\left(1-\eta_b\right)^2\left(1-e^{-\frac{\eta_a}{2}\mu}\right)$ $\left.+d_c\left[\frac{\eta_a^2\eta_b^2}{2}e^{-\eta_a\mu}\mu^2+e^{-\eta_a\mu}\left(1-\eta_b\right)^2\right]\right\}$
$\lvert\alpha 1\rangle\langle\alpha 0\rvert$	$(1-d_c)\left(\frac{1}{2}\sqrt{\eta_a\eta_b}\alpha e^{-\frac{\eta_a}{2}\mu}\right)$
$\lvert\alpha 0\rangle\langle\alpha 1\rvert$	$(1-d_c)\left(\frac{1}{2}\sqrt{\eta_a\eta_b}\alpha e^{-\frac{\eta_a}{2}\mu}\right)$
$\lvert\alpha 1\rangle\langle\alpha 2\rvert$	$(1-d_c)\left(\sqrt{\frac{\eta_a\eta_b}{2}}\alpha\left(\frac{\eta_b}{2}-\frac{\eta_a\eta_b}{8}-1\right)\right)$
$\lvert\alpha 2\rangle\langle\alpha 1\rvert$	$(1-d_c)\left(\sqrt{\frac{\eta_a\eta_b}{2}}\alpha\left(\frac{\eta_b}{2}-\frac{\eta_a\eta_b}{8}-1\right)\right)$

Table C.1: The input-output relationship for a butterfly module with coherent states in one input and number states in the other. The column on the right represents the probability that the output state causes a click on detector x_0, but not x_1, where $x = r, s, u, v$ in Fig. 5.2, assuming that detector x_0 measures the left output port and x_1 the right one. The expression $\mathrm{tr}\left(M_{x_1} B^{AB}_{\eta_a,\eta_b}\left(\rho_{AB}\right)\right)$ will give the same results as above for symmetrical input states; a minus sign correction is needed for asymmetrical input states. Here, $\mu = |\alpha|^2$.

ence of bits by Alice and Bob. In the z basis,

$$\Gamma^{z}_{\gamma\delta;C} = \sum_{i,j,k,l,m,n=0,1;m+n=1} P_{r_i s_j u_k v_l}(\rho^{z}_{\mathrm{enc}}(mn))/4 \tag{C.3}$$

and $\Gamma^{\Phi}_{\gamma\delta;E} = \Gamma^{\Phi}_{\gamma\delta} - \Gamma^{\Phi}_{\gamma\delta;C}$. In the x basis,

$$\begin{aligned}\Gamma^{x}_{\gamma\delta;C} = &\sum_{i,k,m,n=0,1;m\oplus n=0} (P_{r_i s_i u_k v_k}(\rho^{x}_{\mathrm{enc}}(mn))/4 \\ &+P_{r_i s_{i\oplus 1} u_k v_{k\oplus 1}}(\rho^{x}_{\mathrm{enc}}(mn))/4\big) \\ + &\sum_{i,k,m,n=0,1;m\oplus n=1} \big(P_{r_i s_i u_k v_{k\oplus 1}}(\rho^{x}_{\mathrm{enc}}(mn))/4 \\ &+P_{r_i s_{i\oplus 1} u_k v_k}(\rho^{x}_{\mathrm{enc}}(mn))/4\big)\,,\end{aligned} \tag{C.4}$$

where $\oplus$ denotes addition modulo two. Finally, all QBER terms can be obtained from the following.

$$\epsilon^{\Phi}_{\gamma\delta} = \frac{\Gamma^{\Phi}_{\gamma\delta;E}}{\Gamma^{\Phi}_{\gamma\delta}}. \tag{C.5}$$

Appendix D

I explain in this Appendix the procedure to find the secret key rate in chapter 3 using Maple 17.

D.1 Finding the initial density matrices in the no heralding memories of the memory-assisted MDI-QKD protocol

In order to determine the coefficients of the density matrices in the quantum memories for the setup of Fig. 3.7, we apply a butterfly module to the state sent by the user and to a specific state read out of the memory. First, Maple accepts as input the tensor product of two density matrices. One is the density matrix corresponding to the state sent by Alice (or Bob) and the other one is the density matrix corresponding to the mixed state produced by reading out the quantum memory (see Eq. 3.1). The output will be a density matrix whose coefficients are given by the results of the butterfly module applied to the incoming modes. Now, we can apply the relevant measurement operators modules to this density matrix to determine the contribution of dark counts as well. The measurement operators pattern has been explained in Sec. 3.7.1. This output will be the initial density matrix in the quantum memories.

Here, I make an example to better understand how the code works. For instance, to find the coefficient of the density matrix corresponding to the state $|10\rangle\langle 10|$, we may multiply it for the incoming state sent by the user. We then couple the corresponding modes going through the same BSM using the "op"

function, which gives a state separated by commas by using the "seq" function. We have to interject commas between kets and bras in order to be input of the butterfly module. This module is a maple procedure which transforms a generic input state into an output state following the relationships of Table B.2. After we apply the butterfly module both in the upper and lower part of the scheme, we generate two outputs which go directly to the measurement operators, which is an NRPD. This operation is done by using the function "coeff" to a specific combination of the two outputs corresponding to a successful BSM. For instance, if only r_0 and s_0 of Fig. 3.7 click, we have

$$\begin{aligned}(1-d_c)^2 \cdot \{&(\textstyle\sum_{i=1}^{n} \text{coeff}\,(out1, |i0\rangle\langle i0|\,))\,(\textstyle\sum_{i=1}^{n} \text{coeff}\,(out2, |i0\rangle\langle i0|\,)) \\ &+d_c\,[\textstyle\sum_{i=1}^{n} \text{coeff}\,(out1, |i0\rangle\langle i0|\,)\,\text{coeff}\,(out2, |00\rangle\langle 00|\,) \\ &+\textstyle\sum_{i=1}^{n} \text{coeff}\,(out2, |i0\rangle\langle i0|\,)\,\text{coeff}\,(out1, |00\rangle\langle 00|\,)] \\ &d_c^2 \cdot \text{coeff}\,(out1, |00\rangle\langle 00|\,)\,\text{coeff}\,(out2, |00\rangle\langle 00|\,)\end{aligned} \tag{D.1}$$

where $out1$ and $out2$ are the outputs after applying the butterfly module corresponding to the upper and lower part of the scheme respectively; d_c is the dark count, and n is the number of photons.

We follow the same procedure to determine the coefficients of the other part of the density matrix.

D.2 Finding Q_E

Once all memories are loaded, we retrieve the states from them and perform a BSM on the resulting modes. Maple accepts as input the tensor product of the density matrices that are in the quantum memories of each side of Fig. 3.7. The output will be the result of the butterfly module applied to the incoming modes. This output is the input for the relevant measurement operators, which follows the click pattern described in Sec. 3.7.1. As output we find the probabilities for a successful click pattern. In the following, I sketch how to find Q_E in the z basis. The procedure to determine the other probabilities follows the same steps. We start by defining two matrices with Maple. In the first matrix, $pq[i, j]$ we store the product of the coefficients of the density matrices of the QMs of Alice and Bob's side respectively. These coefficients have been calculated in the previous section. In the second matrix, we store the product of the states corresponding

to the stored coefficients. We use again the "op" and "seq" functions on this second matrix so that we can apply the butterfly module. In this way, we find two output matrices, $out1[i,j]$ and $out2[i,j]$, which correspond to the outputs of the middle part of the upper and lower BSM of Fig. 3.7. Now, the probability of obtaining a click on the detector labeled with "a" in Fig. 3.7 will be

$$P1_a[i,j] := \sum_{i=1}^{n} \text{coeff}\left(out1[i,j], |i0\rangle\langle i0|_{a_1 b_1}\right) \tag{D.2}$$

as well as the probability of obtaining a click on the detector labeled with "b" in Fig. 3.7 will be

$$P1_b[i,j] := \sum_{i=1}^{n} \text{coeff}\left(out1[i,j], |0i\rangle\langle 0i|_{a_1 b_1}\right). \tag{D.3}$$

and finally, the probability of no-click will be simply

$$P1_{00}[i,j] := \text{coeff}\left(out1[i,j], |00\rangle\langle 00|_{a_1 b_1}\right) \tag{D.4}$$

To find the lower probabilities, $P2_a$, $P2_b$ and $P2_{00}$, we substitute $out1[i,j]$ with $out2[i,j]$ We can now include the contributions coming from the dark count and we find the total probability of a click in the detectors. For example, the total probability of a click in the "a" detector will be

$$P1_{tot}(a)[i,j] = (1-d_c)\left(P1_a[i,j] + d_c \cdot P1_{00}[i,j]\right) \tag{D.5}$$

Similarly we find the total probability of a click in the "b" detector, $P1_{tot}(b)[i,j]$; the total probability of a click in the "c" detector, $P2_{tot}(c)[i,j]$; and the total probability of a click in the "d" detector, $P2_{tot}(d)[i,j]$.

Now, we can find the matrix of the probabilities of a correct click pattern in the "z" basis by multiplying the $pq[i,j]$ matrix with its corresponding probability click pattern

$$\begin{aligned} P^z_{good}[i,j] := \tfrac{1}{2} pg[i,j] \cdot \big(&P1_{tot}(a)[i,j]P2_{tot}(c)[i,j] + P1_{tot}(b)[i,j]P2_{tot}(d)[i,j] \\ &+ P1_{tot}(b)[i,j]P2_{tot}(c)[i,j] + P1_{tot}(a)[i,j]P2_{tot}(d)[i,j]\big). \end{aligned} \tag{D.6}$$

Finally, to find the total probability of a correct click pattern we add each single contribution of $P^z_{good}[i,j]$ using the "add" function. We can now calculate the key rate by substituting the numerical values of the inefficiencies in the probabilities found in this section.

References

[1] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, Mar 2012. 12, 8, 18, 19, 37, 79, 82

[2] C. Panayi, M. Razavi, X. Ma, and N. Lutkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," *New. J. Phys.*, vol. 16, p. 043005, 2013. 13, 10, 20, 37, 38, 39, 57, 81, 101, 102

[3] M. Dusek, N. Lükenhaus, and M. Hendrych, "Quantum cryptography," *Progress in Optics*, vol. 49, pp. 381–454, 2006. 2, 4

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 6, pp. 644–654, 1976. 2

[5] R. L. Rivest, A. Shamir, and L. Adlemann, "A method for obtaining digital signature and public key cryptosystem," *Communication of the ACM*, vol. 2, pp. 120–126, 1978. 3

[6] M. Gardner, "Mathematical Games, A New Kind of Cipher That Would Take Millions of Years to Break," *Sci. Am.*, vol. 237, p. 120, 1977. 3

[7] A. Shamir, *in: Proceedings of CHES'99, WOrcester, MA, USA, Lecture Notes in Computer Science*. Springer, 1999. 3

[8] T. Kleinjung, K. Aoki, A. K. L. J. F., E. Thom, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, "Factorization of a 768-bit rsa modulus," *Lecture Notes in Computer Science*, vol. 6223, pp. 333–350, 2010. 3

[9] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithm problems," *SIAM J.*, vol. 26, pp. 1484–1509, 1997. 3

[10] R. W. Spekkens and T. Rudolph, "Degrees of concealment and bindingness in quantum bit commitment protocols," *Phys. Rev. A*, vol. 65, p. 012310, Dec 2001. 5

[11] D. Gottesman and I. Chuang, "Quantum digital signatures," *arXiv:quant-ph/0105032*, 2001. 5

[12] D. DiVincenzo, D. Leung, and B. Terhal, "Quantum data hiding," *IEEE Transactions on Information Theory*, vol. 48(3), pp. 580–599, 2002. 5

[13] D. Gottesman, "Uncloneable encryption," *Quantum Information and Computing*, vol. 3(6), pp. 581–602, 2003. 5

[14] M. Mosca, A. Tapp, and R. de Wolf, *Private quantum channels*. 2000. 5

[15] M. Adcock and R. Cleve, "A quantum Goldreich-Levin theorem with cryptographic applications," *Lecure Notes in COmputer Science*, vol. 2285, pp. 323–334, 2002. 5

[16] C. H. Bennet and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing." presented at the IEEE International Conference on Computers Systems and Signal Processing, 1984. 6, 12, 58

[17] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992. 6, 63

[18] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991. 7, 12, 17, 58, 63

[19] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bells theorem," *Phys. Rev. Lett.*, vol. 68, p. 557, 1992. 7, 18, 58

[20] J. Bell, "On the einstein podolsky rosen paradox," *Physics*, vol. 1 (3), pp. 195–200, 1964. 7, 18

[21] A. S. J. Clauser, M. Horne and R. A. Holt, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *Phys. Rev. Lett.*, vol. 24, p. 549, 1970. 7

[22] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug 2000. 7

[23] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution wuth imperfect devices," *Quant. Inf. Comp.*, vol. 4, p. 325, 2004. 8

[24] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, 2004. 8

[25] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication.," *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003. 8, 14

[26] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 94, p. 230504, 2005. 15, 16

[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev A*, vol. 72, p. 012326, 2005. 8, 15

[28] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quant. Inf. and Comp.*, vol. 7, p. 073, 2007. 8

[29] V. Makarov and J. Skaar, "Fakes states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," *Quant. Inf. and Comp.*, vol. 8, pp. 0622–0635, 2007.

[30] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Marakov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, pp. 686–689, 2010. 8

[31] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, Mar 2012. 8, 9, 18, 19, 38, 79

[32] E. Biham, B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Phys. Rev. A*, vol. 54, no. 4, p. 2651, 1996. 9, 18, 19, 38, 79

[33] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, p. 802, 1982. 9, 12

[34] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""event-ready-detectors" bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, pp. 4287–4290, Dec 1993. 9

[35] 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.*, vol. 81, pp. 5932–5935, Dec 1998. 9, 12, 22, 58

[36] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature (London)*, vol. 414, p. 413, 2001. 9, 10, 12, 22, 26, 27, 31, 58

[37] N. Sangouard, C. Simon, J. c. v. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, "Long-distance entanglement distribution with single-photon sources," *Phys. Rev. A*, vol. 76, p. 050301, Nov 2007. 10, 23, 26, 27, 29, 30, 31, 58, 59, 63, 64, 68, 77, 80

[38] D. Dieks, "Communication by epr devices," *Phys. Letters A*, vol. 92, p. 271, 1982. 12

[39] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000. 14, 25

[40] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," *IEEE Transactions on Information Theory*, vol. 49, p. 457, 2003. 14

[41] X. Ma, "Quantum cryptography: from theory to practice," 2008. 15

[42] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology*, vol. 18, p. 133, 2005. 16, 65

[43] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, no. 23, p. 230501, 2007. 18, 36

[44] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Letters*, vol. 84, pp. 4729–4732, 2000. 18

[45] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys Rev. A.*, vol. 74, p. 022313, 2006. 18

[46] V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on sarg04, phase-time, dpsk, and ekert protocols," *Quant. Inf. Comput.*, vol. 8, p. 0622, 2008. 18

[47] Inamori, "Security of practical time-reversed epr quantum key distribution," *Algorithmica*, vol. 34, pp. 340–365, 2008. 10.1007/s00453-002-0983-4. 18, 19

[48] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *Eur. Phys. J. D*, vol. 41, p. 599, 2007. 19

[49] K. F. Reim, P. Michelberger, K. C. Lee, J. Nunn, N. K. Langford, and I. A. Walmsley, "Single-photon-level quantum memory at room temperature," *Phys. Rev. Lett.*, vol. 107, p. 053603, Jul 2011. 20, 37

[50] E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussiéres, M. George, R. Ricken, W. Sohler, and W. Tittel, "Broadband waveguide quantum memory for entangled photons," *Nature*, vol. 469, pp. 512–515, Jan. 2011. 20, 37

[51] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "event-ready detectors bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, pp. 4287–4290, Dec. 1993. 21

[52] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nature Photon.*, vol. 6, pp. 771–781, Oct. 2012. 22, 23, 37

[53] K. Azuma, K. Tamaki, and H.-K. Lo, "All photonic quantum repeaters," *arXiv:1309.7207 [quant-ph]*, 2013. 22, 23

[54] Z.-B. Chen, B. Zhao, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, "Fault-tolerant quantum repeater with atomic ensembles and linear optics," *Phys. Rev. A*, vol. 76, p. 022329, Aug 2007. 22, 58, 59

[55] B. Zhao, Y.-A. Chen, . H. Bao, T. Strassel, C.-S. Chuu, X.-M. Jin, J. Schmiedmayer, Z.-S. Yuan, S. Chen, and J.-W. i Pan, "A millisecond quantum memory for scalable quantum networks," *Nat. Phys.*, vol. 5, p. 95, 2009. 22

[56] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar 2011. 22, 60

[57] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, "Quantum repeaters with photon pair sources and multimode memories," *Phys. Rev. Lett.*, vol. 98, p. 190503, May 2007. 23, 27, 58

[58] M. Razavi, M. Piani, and N. Lutkenhaus, "Quantum repeaters with imperfect memories: Cost and scalability," *Phys. Rev. A*, vol. 80, p. 032301, 2009. 24, 25, 38, 64, 74

[59] C. Simon, H. de Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, "Quantum repeaters with photon pair sources and multimode memories," *Phys. Rev. Lett.*, vol. 98, p. 190503, May 2007. 25

[60] M. Razavi, K. Thompson, H. Farmanbar, M. Piani, and N. Lütkenhaus, "Physical and architectural considerations in quantum repeaters," in *Proc. SPIE*, vol. 7236, (San Jose, CA), p. 723603, 2009. 26

[61] J. Amirloo, M. Razavi, and A. Majedi, "Quantum key distribution over probabilistic quantum repeaters," *Phys. Rev. A*, vol. 82, p. 032304, 2010. 28, 29, 31, 58, 63, 74, 76, 77, 90

[62] P. L. Knight and A. Miller, *Measuring the Quantum State of Light, 1st ed., Vol. 1.* (Cambridge University Press), 1997. 32

[63] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022313, 2006. 36

[64] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Experimental demonstration of time-shift attack against practical quantum key distribution systems," *Phys. Rev. A*, vol. 78, p. 042333, 2008. 36

[65] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *FOCS, 39th Annual Symposium on Foundations of Computer Science*, p. 503, IEEE, Computer Society Press, Los Alamitos, 1998. 36

[66] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, no. 4, p. 045021 (25pp), 2009. 36

[67] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Ultrafast and fault-tolerant quantum communication across long distances," *Phys. Rev. Lett.*, vol. 112, p. 250501, Jun 2014. 37

[68] S. Abruzzo, H. Kampermann, and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories," *Phys. Rev. A*, vol. 89, p. 012301, Jan 2014. 37, 81

[69] A. Stute, B. Casabone, P. Schindler, T. Monz, P. O. Schmidt, B. Brandstätter, T. E. Northup, and R. Blatt, "Tunable ionphoton entanglement in an optical cavity," *Nature*, vol. 485, p. 482, May 2012. 39

[70] S. Ritter, C. Nölleke, C. Hahn, A. Reiserer, A. Neuzner, M. Uphoff, M. Mücke, E. Figueroa, J. Bochmann, and G. Rempe, "An elementary quantum network of single atoms in optical cavities," *Nature*, vol. 484, pp. 195–200, April 2012. 39

[71] M. Razavi and J. H. Shapiro, "Long-distance quantum communication with neutral atoms," *Phys. Rev. A*, vol. 73, p. 042303, April 2006. 41, 83

[72] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413 – 418, 2001. 41, 77

[73] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 062319, 2012. 41, 42, 44, 45, 57, 79, 82, 97

[74] F. Marislli, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam *Nature Photonics*, vol. 7, p. 210. 48

[75] M. Hosseini, B. M. Sparkes, G. Campbell, P. K. Lam, and B. C. Buchler *Nat. Commun.*, vol. 2, p. 174, 2011. 48

[76] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," *Opt. Lett.*, vol. 37, pp. 1008–1010, March 2012. 58

[77] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New J. Phys.*, vol. 13, p. 063039, June 2011. 58, 79

[78] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.* , vol. 94, p. 230504, June 2005. 58

[79] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruss, "quantum repeaters and quantum key distribution: Analysis of secret-key rates," *Phys. Rev. A*, vol. 87, p. 052315, 2013. 58

[80] L. Jiang, J. M. Taylor, and M. D. Lukin, "Fast and robust approach to long-distance quantum communication with atomic ensembles," *Phys. Rev. A*, vol. 76, p. 012301, 2007. 58

[81] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar 2011. 59, 71

[82] N. Sangouard, C. Simon, Y.-a. C. B. Zhao, J.-W. P. H. de Riedmatten, and N. Gisin, "Fast and robust approach to long-distance quantum communication with atomic ensembles," *New Journal of Physics*, vol. 77, p. 062301, 2009. 59

[83] M. Razavi, K. Thompson, H. Farmanbar, M. Piani, and N. Lutkenhaus, *Quantum Communications Realized II*. Y. Arakawa and H. Sotobayashi, 2009. 71

[84] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, June 2008. 79

[85] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, pp. 69–72, Sept. 2013.

[86] M. Razavi, "Multiple-access quantum key distribution networks," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 3071–3079, 2012. 79

[87] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Phys. Rev. X*, vol. 2, p. 041010, Nov. 2012. 79

[88] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, p. 075001, 2009. 79

[89] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011. 79

[90] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* , vol. 67, p. 661, 1991. 79

[91] X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 052305, Nov 2012. 79, 85

[92] 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, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, p. 130502, Sep 2013. 79

[93] M. Razavi, N. Lo Piparo, C. Panayi, and D. E. Bruschi, "Architectural considerations in hybrid quantum-classical networks (invited paper)," in *Iran Workshop on Communication and Information Theory (IWCIT)*, (Tehran, Iran), pp. 1–7, 2013. 79

[94] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," *Quant. Inf. Comput.*, vol. 7, p. 073, 2007. 80

[95] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New Journal of Physics*, vol. 11, no. 6, p. 065003 (18pp), 2009.

[96] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, no. 1, p. 013043, 2011.

[97] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, no. 7, p. 073024, 2011. 80

[98] N. Lo Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories," *arXiv:1407.8016*, 2014. 81

[99] N. Lo Piparo and M. Razavi, "Long-distance quantum key distribution with imperfect devices," *Phys. Rev. A*, vol. 88, p. 012332, Jul 2013. 90

[100] J.-P. Bourgoin, E. Meyer-Scott, B. H. B. L. Higgins1, C. Erven, H. Hbel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *Phys. Rev. A*, vol. 15, p. 023006, 2013. 96