Memory-Assisted Measurement-Device-Independent Quantum Key Distribution Systems

by

Christiana Panayi

Submitted in accordance with the requirements for the degree of Doctor of Philosophy

The University of Leeds
School of Electronic and Electrical Engineering
March 2016

Declarations

The candidate confirms that the work submitted is her own, except where work which has formed part of a jointly authored publication 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 (Christiana Panayi). 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 4 of the thesis has appeared in publication as follows:

C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, Memory-assisted measurement-device-independent quantum key distribution *New J. Phys. 16 04300 (2014).* I have analyzed the system by calculating the secret key rate when quantum memories are introduced in the memory-assisted-device-independent quantum key distribution protocol, in terms of coherence time, loading time and key generation rate versus distance.

C. Panayi and M. Razavi, Measurement-device-independent quantum key distribution with imperfect quantum memories. *International Conference on Quantum, Nano and Micro-Technologies, Rome, Italy, Aug. 2012.*

C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, Memory-assisted measurement-device-independent quantum key distribution. *QCrypt 2013, 3rd international conference on quantum cryptography, in Waterloo, Canada, August, 2013.* It has also been presented in the *International Workshop on Quantum Communication Networks, Leeds, UK, January, 2014.*

N. Lo Piparo, C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, Reaching beyond existing quantum key distribution links: How to take advantage of imperfect quantum memories. *QCrypt 2014, 4th international conference on quantum cryptography, in Paris, September, 2014.*

N. Lo Piparo, M. Razavi and C. Panayi, Measurement-device-independent quantum key distribution with ensemble-based memories. *IEEE Journal of Selected Topics in Quantum Electronics vol. 21, article 3, (2015).* I have contributed to the development of EPR based memory-assisted systems.

M. Razavi, N. Lo Piparo, C. Panayi, X. Ma, and N. Lütkenhaus, Quantum Memories in Action. *Invited Paper to Quantum Information and Measurement Conf., Messes Berlin, Berlin Germany (2014).* My contribution to this work is related to how quantum memories, change the performance of the key generation rate in the measurement-device-independent quantum key distribution protocol using EPR sources.

Some of the work in Chapters 3 and 4 of the thesis has appeared in publication as follows:

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

Some of the work in Chapter 5 has appearead in publication as follows:

M. Razavi, C. Panayi, N. Lo Piparo and X. Ma, and N. Lütkenhaus, Recent progress in memory-assisted measurement-device-independent QKD. *Invited talk to Trustworthy Quantum Information, Michigan, USA (2015).*

Acknowledgements

My heartfelt gratitude to Dr. Mohsen Razavi for his invaluable guidance, patience, motivation and knowledge during my studies and his support and understanding on a personal level.

My deepest appreciation goes to Aryana for his unremitting encouragement. Put simply, I have never met anyone who believes in me more. Thank you for making me more than I am.

I would especially like to thank some of my dear friends George Constantinou, Neofytos Ioannou, Electra Eleftheriadou and Shima Ghasemi-Roudsari. We have been friends for many years and your love and support has kept me strong and focused on my goal.

George we have had great memories during our undergraduate studies and kept a wonderful friendship since then. I will always be thankful for the fruitful conversations we had regarding physics and beyond. Neo you have taught me how to take risks and to be bold in my decisions. Electra thank you for being an understanding source of love and Shima thank you for your guidance and standing by me all these years. Nicolo thank you for being such a good friend and a fellow colleague. The discussions we had were fruitful and I am grateful for your help.

Above and beyond all, my indebtedness towards my parents and sisters for their much needed support, patience, understanding, and encouragement in every possible way. Their endless love, priceless, perpetual and indispensable help made all this possible. Evi thank you for always believing in me and being there for me. Caterina I could not be more happy to have you as my supportive and loving sister. My dear mother Nedi, thank you for being a constant source of love, concern and strength all these years. A special thanks to my father Georgios whom has always taught me to go after my dreams, be strong and not let anything get between me and my goals.

This research was supported in part by the European Community's Seventh Framework Programme Grant Agreement 277110 and the UK Engineering and Physical Sciences Research Council Grant No. EP/J005762/1.

Dedicated to my parents and sisters.

Abstract

Quantum key distribution (QKD) is one of the most prominent methods for secure exchange of cryptographic keys between two users. The laws of physics provide it with an immense tool towards secure communications. Although QKD has been proven to reach distances on the order of a few hundreds of kilometers, the transmission rate of the key significantly drops when we go to further distances. One possible solution to this is to build a network of trusted nodes. The trust requirement will however narrow its scope of deployability. In this thesis, we focus on improving the key rate performance of secure communications by introducing imperfect quantum memories (QMs) in a measurement-device-independent (MDI) QKD system.

In this thesis, a protocol with the potential of beating the existing distance records for conventional QKD systems is proposed. It borrows ideas from quantum repeaters by using memories in the middle of the link, and that of MDI-QKD, which only requires optical source equipment at the user's end. For certain fast memories, our scheme allows a higher repetition rate than that of quantum repeaters, thereby requiring lower coherence times. By accounting for various sources of nonideality, such as memory decoherence, dark counts, misalignment errors, and background noise, as well as timing issues with memories, we develop a mathematical framework within which we can compare QKD systems with and without memories. In particular, we show that with the state-of-the-art technology for quantum memories, it is possible to devise memory-assisted QKD systems that, at certain distances of practical interest, outperform current QKD implementations.

To extend this work, we consider a suitable candidate that fullfils the requirements we have set for the QMs, i.e., the ensemble-based QMs. This type of memories, nevertheless, suffers from multiple-excitation effects, which can deteriorate the performance of the memory-assisted MDI-QKD system. As a solution we propose an alternative approach to the memory-assisted MDI-QKD by employing entangled-photon sources. We fully analyse this system by including modulation errors during the state-preparation at a single-photon source. We identify under which regimes of operation this system outperforms present QKD implementations. Overall we obtain a realistic account of what can be done with current technologies in order to improve the performance, in terms of rate versus distance, of QKD systems. Our findings can guide us toward implementing larger quantum networks.

Contents

Abbreviations

Abbreviations used in this thesis	Full expression
BS	Beam splitter
BSM	Bell-state measurement
EPR	Entangled photon source
FSS	Fine-structure-splitting
HQC	Hybrid Quantum-Classical
MDI-QKD	Measurement-device-independent QKD
PBS	Polarising beam splitter
PNS	Photon number splitting
QBER	Quantum bit error rate
QKD	Quantum key distribution
QM	Quantum memory
RSA	Rivest, Shamir and Andleman
SPDC	Spontaneous-parametric-down-conversion
WCP	Weak coherent-pulses

List of Figures

List of Tables

List of Notations

B_{BF}	Butterfly Operator
B_{ent}	Entangling Operator for side-BSM
B_{η}	Beam Splitter Operator with transmissivity η
$B^{\dagger}_{\eta_{\alpha}}$	Alice's Hermitian Conjugate of the transmissivity Beam Splitter Operator
$B^{\dagger}_{\eta_{\beta}}$	Bob's Hermitian Conjugate of the transmissivity Beam Splitter Operator
c	Speed of light in the channel
$\mathrm{E}\{\cdot\}$	Expectation value operator
e^{K}_{BG}	Probability of QM loaded by a background photon conditioned on successful loading
e_d	Total misalignment probability of the channel
e_{deph}	Misalignment due to dephasing
$e^{(A,B)}_{dS}$	Misalignment probabilities for Alice's and Bob's QMs for basis $S = \{X,Z\}$
e_i	QBER for $i-$photon states
E_{μ}	QBER for a phase-randomised coherent state with μ photons on average
$E_{\mu}Q_{\mu}$	Intrinsic error rate for a phase-randomised coherent state with μ photons on average
$E^{\mathrm{QM}}_{\mu\nu;Z}$	QBER in the Z basis after successfully loading both QMs when Alice and Bob use respectively μ and ν on average number of photons
$e_{11;S}$	QBER in basis S=$\{X,Z\}$ between Alice and Bob when single photons are used
$e^{\mathrm{QM}}_{11;S}$	QBER in basis S=$\{X,Z\}$ between Alice and Bob QMs when single photons are used
F	Fidelity of the $i-$photon state
$f1$	Error correction inefficiency
$\lvert H_{xx}\rangle$	Biexciton photon of a quantum dot in horizontal polarization
$\lvert H_{x}\rangle$	Exciton photon of a quantum dot in horizontal polarization
$\lvert H\rangle$	Horizontally polarised photon
$h(x)$	Binary entropy function
$I_0(x)$	Modified Bessel function of the first kind

I	Identity operator
L_{att}	Attenuation length
$M_{D_iD_j}$	Measurement Operator of two detectors in orthogonal polarisations H,V of a successful BSM
N_A	Geometric random variable on Alice's side with success probability η_A
N_B	Geometric random variable on Bob's side with success probability η_B
N_L	Average number of trials to load both memories
N_r	Extra rounds lost due to nonzero reading times of QMs
p_{BG}	Probability of background (unpolarized) photons per pulse
p_{dc}	Probability of dark count
$\|P\rangle$	A polarised photon in a BB84 state
$P_{D_iD_j}$	Probability of a successful BSM where i,j are one of the 4 single photodetectors
q	Basis reconciliation factor
Q_{11}	Probability of a successful BSM if Alice and Bob respectively send single-photon pulses multiplied by the probability of sending single photons
Q_{11}^{QM}	Probability of a successful BSM after successfully loading the QMs with single-photon pulses multiplied by the probability of sending single photons
Q_{AB}^{S}	Probability an acceptable pattern of clicks occurs in the S= $\{X,Z\}$
Q_C	Probability of correct clicks occurs in the basis S= $\{X,Z\}$
Q_E^X	Probability of having a successful pattern of clicks due to errors in the X basis
Q_E^Z	Probability of non-identical bits in Z basis assuming Alice and Bob used the Z basis to encode their bits initially
Q_μ	Probability of a successful BSM conditioned on using μ average number of photons
$Q_{\mu\nu;Z}^{\text{QM}}$	Overall gain when Alice and Bob use pulses with μ and ν average number of photons
Q_i	Overall gain of $i-$photon states
R	Secret key generation rate
R_S	Single-photon repetition rate
T	Repetition period
T_1	QM amplitude decay time
T_2	Coherence or dephazing time of the QM

T_{st}	Average required memory storage time
$\lvert V\rangle$	Vertically polarised photon
Y_i	Conditional probability of detection on Bob's side conditioned that Alice sends i photons
Y_1	Yield of single photons or the probability that Bob gets a click on his measurement devices assuming Alice has sent exactly one photon
Y_{11}	Yield of single photons or the probability of a successful middle BSM assuming Alice and Bob has sent exactly one photon
Y_{11}^{QM}	Rate at which both QMs are loaded with single photons of the same basis and the middle BSM is successful
Y_C	Yield or otherwise conditional probability of identical bits shared by Alice and Bob
Y_E	Yield or otherwise conditional probability of non-identical bits shared by Alice and Bob
Y_{EPR}^{QM}	Yield or otherwise conditional probability that heralds the successful BSM conditioned on the success of the side-BSMs from both Alice's and Bob's sides
γ_{BG}	Background rate per pulse
γ_{dc}	Dark count rate per pulse
μ, ν	Average number of photons for the signal state in decoy state-method
η_a	Channel efficiency of Alice's side
η_b	Channel efficiency of Bob's side
η_A	Success probability for middle-BSM on Alice's side
η_B	Success probability for middle-BSM on Bob's side
η_{ch}	Channel loss efficiency
η_d	Detector efficiency
η_{ent}	Entangling effificiency
η_g	EPR source efficiency
η_{1K}	Probability of successfully loading a directly heralding QM with SPSs for the leg $K = \{A,B\}$
η_{mK}	Effective measurement efficiency for the leg $K = \{A,B\}$
η_{r0}	QM reading efficiency right after loading
η_r	QM reading efficiency
η_w	QM writing efficiency
τ_p	Pulse duration
τ_r	Reading time duration, time between retrieval process until end of the pulse
τ_w	Writing time duration

Chapter 1

Introduction

Communication is one of the most basic and yet most essential part of human beings in their daily lives. It can be verbal exchange of information when discussing on a one-to-one basis or nonverbal by using the technological advancements with the help of networks. This communication could be extended to multiple-users all over the world. An important necessity is how to establish secure communication between two or more parties in long distances and at the same time have high data rates. Another is authentication where users are assured that their communicating party on the other end is who they claim to be. The area that focuses strictly on how to establish these goals is called cryptography. Various methods and techniques based on cryptographic systems have been developed to protect communicating parties from adversaries. Complexity of encryption in some algorithms is what provides the security in communication against potential eavesdroppers, thus making the decryption more difficult. An equally interesting area of cryptography that provides reliable security is quantum cryptography and an application therein, quantum-key-distribution (QKD). In QKD, it is guaranteed that any eavesdropper trying to intercept the secret key can be detected by the users. Despite the unconditional security that it offers, QKD has yet a long way to implement efficient systems that can tolerate loss. The motivation behind my work relies on the implementation of a trustworthy QKD system over long distances with characterised imperfections in our employed devices. In order to describe the work behind this thesis, I will introduce a basic background, which will be used as a guide to the main topics studied in this thesis.

1.1 Cryptography

Cryptography, from the Greek words $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$, meaning secret or hidden and $\gamma\rho\alpha\phi\eta$ meaning writing, is the primary science that studies and develops methods of encryption and decryption of messages, as well as authentication, integrity and non-repudiation in order to establish secure communication.

Looking at the 20th century inventions of cryptography, one of the most outstanding inventions is the *one-time-pad* by Vernam [8]. The principle of this cryptographic algorithm is to translate information, with the help of a secret key, from a plaintext to a sequence of random characters in the alphabet, the so-called ciphertext. This symmetrical stream cipher uses a combination of plaintext and streams of data with the same length. In the binary format, in order to generate the ciphertext, we use the Boolean or otherwise known XOR function: $plaintext \oplus key = ciphertext$ $=> ciphertext \oplus key = plaintext$.

A key is generally used in cryptographic algorithms, for instance, in message authentication codes and digital signature schemes. The transformation from plaintext to ciphertext is called encryption and vice versa is the decryption. With *one-time-pad* the information could be trusted to be transmitted publicly as the only person that could decode the ciphertext must have the secret key. The Vernam cipher has the advantage of providing unconditional security against adversaries with unlimited computational power; however, the distribution of the required key was a complication. The significance of the security that it provides even nowadays is of great importance and we will discuss this further in key distribution.

Another innovative invention was the Enigma [9] machine by A. Schrebious in 1918, which was later on called the rotor machine. The rotating wired wheels could perform a challenging substitution cipher. It was widely used during World War II. The Enigma could have up to 159×10^{18} different cryptographic keys. The fact that this machine could have this enormous numbers of possible keys is what paved the way for Alan Turing to formulate the first electronic computer, which in turn used to decode the Enigma cipher later on. Enigma cipher messages are decoded in a few minutes with the current computational power.

The security of Enigma and similar encryption systems is based on the mathematical complexity of factorising the product of two large prime numbers. Therefore it is required to find different cryptographic systems that their security is resilient to the advancement of technology in computation power.

Cryptography has two main classes of cryptographic protocols, the public or asymmetric-key cryptography and the secret or symmetric-key cryptography. In the next sections, I give a brief description of their main advantages and weaknesses.

1.2 Public-key cryptography

Public key cryptography or otherwise asymmetric cryptography is an invention of W. Diffie and M. Hellman [10]. It is a method of assuring the authenticity and security of the Internet. Public key cryptography is based on sharing initial seed keys that will be used for cryptographic protocols, between two communicants. The user A on one end creates two different keys, hence the term asymmetric, one is public and available to everyone and the second one is a secret key, which is stored in a private place. If someone wishes to communicate with A then he/she has to use the public key to encrypt his/her message and then send it to A, who can decrypt it using her private key. This technique reassures confidentiality. Practically, the public keys are distributed through trusted servers. The secret key can be retrieved with the help of strong computation power since the secret and public key are mathematically related.

RSA cryptosystem was invented by Rivest, Shamir and Andleman [11] and is one of the most widely used examples of algorithms used by public-key cryptography. It is based on the mathematical difficulty of factoring large numbers. In RSA, A picks two large prime numbers, p and q, and announces their product publicly. He/she chooses two large numbers k and l such that (kl - 1) is divisible by (p-1) (q-1). The public key consists of the product $N = pq$ together with the number l; p, q and k make the private key. With N and l, anyone can encrypt a message M by calculating $S = M^l \mod N$. To decipher the encrypted message, A uses his/her private key and calculates $M = S^k \mod N$. Thus in order to break the RSA system, one has to find the prime factors of N, which is a significantly hard computational problem for classical computers.

During the past decades there have been many attempts to break an RSA system [12, 13]. In a recent attack a 768 bit key was cracked by a network of classical computers [14]. With the help of quantum computers, the RSA system will be decrypted in polynomial order time [15]. Therefore the RSA may become entirely outdated for its purpose. A different type of cryptography is studied along with its benefit of the security it provides.

1.3 Secret-key cryptography

Secret-key cryptography or else known as symmetric key are algorithms that use the same cryptographic keys to both encrypt and decrypt a message. However the distribution of the secret key to the two parties constitutes one of the main limitations of secret key cryptography. Today, the key distribution part is done by public-key schemes. The combination of fast secret-key and versatile public-key systems, is at the core of today's secure systems.

Vernam cipher [8], as previously mentioned, is an unbreakable classical cryptographic cipher, secure against eavesdroppers with unlimited computational and technological power. This symmetric cipher, uses a random key to ensure secure communication and uses the same key for both, encrypting and decrypting a message, between two authenticated users. The encryption algorithm E in the binary logic [16] can be written as:

$$E_N(L) = (L_1 + N_1, L_2 + N_2, ..., L_n + N_n) \mod 2. \tag{1.1}$$

where $L = (L_1, L_2, ..L_n)$ represents the message in the form of bits and $N = (N_1, N_2, ..N_n)$ represents the key in the form of random bits or else the secret key bits. The decryption of the message follows the same procedure as in equantion (1.1), on E_N. When applying the $\mod 2$ operation two times then L can be retrieved as follows

$$L = E_N(E_N(L)) = (L_1 + N_1 + N_1, L_2 + N_2 + N_2, ..., L_n + N_n + N_n) \mod 2. \tag{1.2}$$

To establish an unbreakable secure one-time-pad system, three conditions need to be fulfilled: (a) the key length must be equal to the length of the message; (b) the key must be random; (c) it must be used only once (hence the *one-time pad* name) as it was proved by Shannon in 1949 [17] from the information theory point of view. Even though, all of the three conditions are fulfilled, the main limitation of the Vernam cipher, is the distribution of the key when one user is in distance from the other. Public-key cryptography can be compromised as mentioned in Sec 1.2. However, quantum key distribution (QKD) can be used as a solution to this problem. It offers to detect an eavesdropper if he/she retains an unacceptable amount of information of the secret key, as it will be explained next.

1.4 Quantum key distribution

QKD is based on the laws of quantum mechanics and it establishes a cryptosystem secure against any attempt by adversaries to compromise the communication without the knowledge of the two autenticated users. Protocols based on the quantum mechanics principles have unbreakable security, unlike classical cryptography, even against an eavesdropper with unlimited computational power. The basic principle behind QKD is the use of non-orthogonal quantum states. Its security is based on the Heisenberg uncertainty principle, which states that a measured system will be altered if someone attempts to learn information about the non-orthogonal states with certainty and this eavesdropper would be eventually detected. In classical physics, an eavesdropper cannot be traced, since the information can be encoded into any properties of a classical object and can be accessed without changing the current state of the object [16]. Unlike the classical systems, the quantum ones, with the usage of non-orthogonal quantum states as information carriers, can reassure the inviolability of the channel. Since the information is encoded into non-orthogonal states, it cannot be split, read or copied without disturbing the system in a detectable way [16].

Nonetheless QKD cannot prevent possible attempts for interception from adversaries; it only offers the detection of any eavesdropper, namely, Eve. Any attempt of Eve to gain information would result in discrepancies. Therefore with the help of post-processing techniques, the key is either made secure or discarded and the two legitimate users repeat the protocol for a new key to be generated.

There are different QKD protocols in practise. Here, I briefly explain major categories of protocols pertinent to this thesis. Further detailed description of these protocols will appear in Chapter 2.

1.4.1 Prepare-and-measure protocols

One of the pioneering protocols of the prepare-and-measure category is BB84 [1] (see Figure 1.1). In prepare-and-measure protocols, one user has the encoder side and the other has the decoder. In BB84 Alice sends a polarised single photon, encoded, in one of the two random chosen bases. Following this, Bob measures it respectively to determine its polarization. This procedure is repeated multiple times until they have an adequately long string of bits. In the sifting process Bob shares his chosen basis for measurement, publicly. Thus they keep the bits that share the same basis and discard the rest. If Eve attempts to intercept the communication, e.g. the photon transmitted by Alice, then she will introduce discrepancies that can be detected in the generated sifted keys.

In prepare-and-measure schemes, e.g., BB84 [1], they commonly rely on the transmission of single photons between two parties. According to the *no-cloning* theorem [18] there cannot be exact copies of an arbitrary quantum state without violating the laws of quantum mechanics. Thus the security of any protocol using single photons is guaranteed by the *no-cloning* theorem [18]. Nevertheless the implementation of single photon sources faces many difficulties. In recent years many solutions have been proposed to overcome this drawback. One of the proposals is to, instead of ideal single-photon sources, use weak laser pulses that emit coherent states. These coherent states consist of vacuum components and multiphoton components, which can cause adverse results in the performance of a QKD protocol. When the source emits more than a single photon this leads to a compromised security as the so-called photon number splitting (PNS) attack

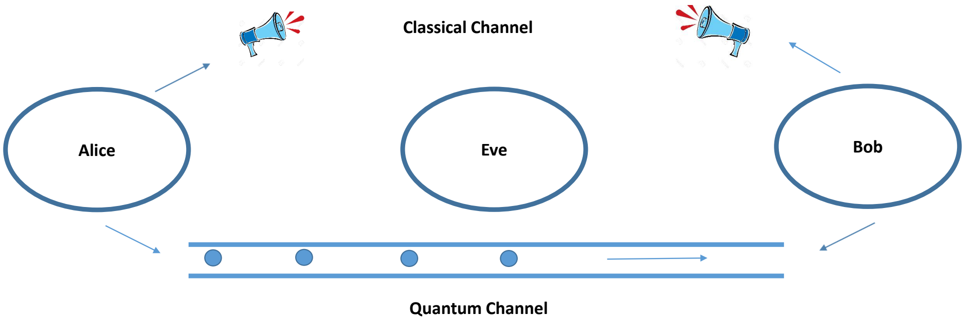


Figure 1.1: A prepare-and-measurement QKD protocol such as BB84 [1].
Alice transmits single encoded photons to Bob through a quantum channel and they both publicly announce the bases they used. Eve represents any eavesdropper trying to intercept the communication.

[2] (see Figure 1.2) offers Eve the possibility to obtain information of the key without being traced. However, under certain conditions, a secure key can still be established even under the PNS attack as proven in GLLP [19], but with a significant reduction of the secret key. In PNS, the rate is scaled as ${\eta_{ch}}^2$, whereas the single photon source rate is scaled as η_{ch}, where η_{ch} is the transmittance of the quantum channel.

Other solutions to the PNS attack, since the ideal single photon sources are not available, are the modified BB84 [20] protocol where the key rate scales as ${\eta_{ch}}^{3/2}$, or using decoy state protocols [21] where Alice randomly sends two types of pulses, one is used for extracting the key and the other are the so called decoy states, which are used for detection of any eavesdropper. Decoy state based protocols can be used against PNS attacks as Eve will not be able to discriminate between the signal and decoy pulses. I will be giving a further description of this in Chapter 2.

1.4.2 Entanglement based protocols

Another category of equally important protocols is based on entanglement. Quantum entanglement is a property that applies only in quantum physics thus a property that cannot be used in classical physical systems. Two systems are considered entangled when their joint quantum state cannot be described as a convex sum of separable states. The most famous QKD protocols based on entanglement are Ekert91 [3] (see Figure 1.3) and BBM92 [22]. Assuming that the entangled particles are photons and one of them is measured in the rectilinear basis, and has been found to have a horizontal polarization then it is expected that the other photon will have a known polarization, conditioned that it is measured in the same basis. However, if the second photon is

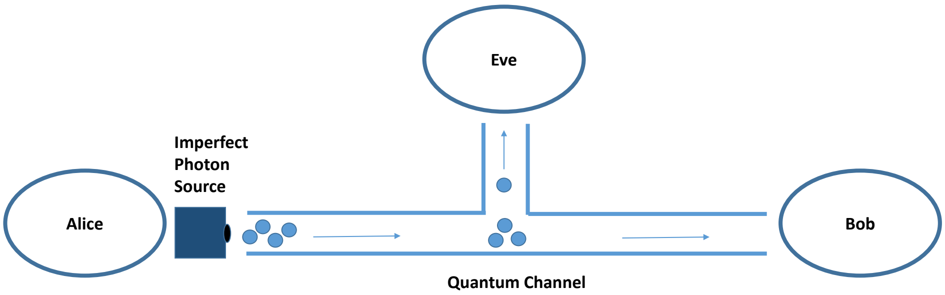


Figure 1.2: This protocol depicts a PNS attack [2].
In the case of an imperfect single-photon source, the PNS attack takes place in a typical QKD protocol as shown above.

measured in a different basis, e.g. circular, then it will have either right or left circular polarization. Ekert, in his paper [3], proved that the security of a two-qubit protocol is based on Bell's inequality [23], an inequality which states that some correlations can be predicted by quantum mechanics but cannot be recreated by the local hidden variable theory. John Clauser, et. al. introduced the CHSH inequality [24], with the following classical constraints 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 (b) and a' (b') represent detector settings on Alice and Bob's side, respectively. The four combinations are tested separately in experiments. The terms $E(a,b)$ are the quantum correlations of the particle pairs. Quantum correlation is the expectation value of the product of the "outcomes" of the experiment. In quantum mechanics, the mathematical formalism predicts that S has a maximum value of $2\sqrt{2}$, which is greater than 2 therefore CHSH violations are confirmed by the theory of quantum mechanics. Thus, if an adversary attempts to intercept the entangled pairs shared by Alice and Bob, he or she will break the quantum correlation of the two particles, resulting in a non-violation of Bell's inequality.

While in entanglement-based QKD protocols, users do not need to trust the source, their measurement devices are still prone to many attacks by Eve. This has particularly been demonstrated experimentally by modifying the Bob's detector setup in commercial products. These attacks include the time-shift attack, remapping and blinding attacks [25, 26, 27, 28, 29, 30]. In these

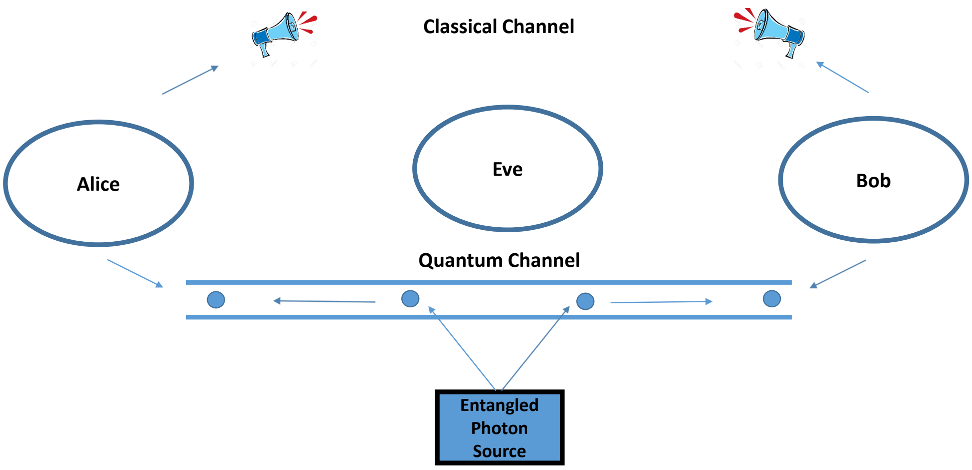


Figure 1.3: This protocol depicts an entanglement based protocol such as the Ekert91 [3].

An entanglement photon source placed between Alice and Bob, emits a pair of entangled photons, one to each user through a quantum channel. As in the BB84 they discuss their measurement results publicly.

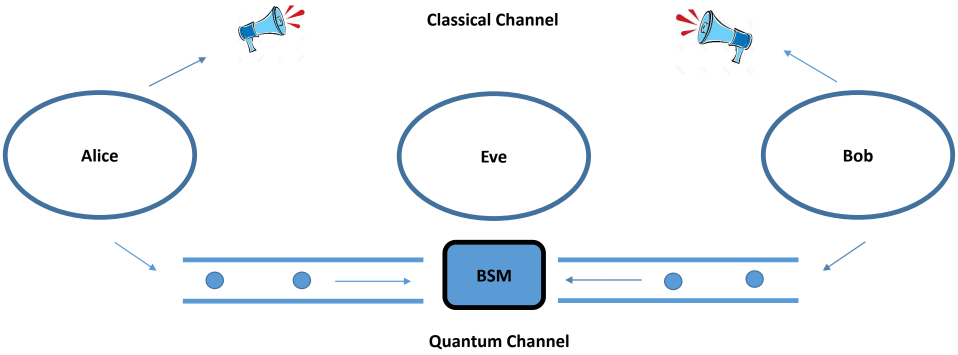


Figure 1.4: A generalised MDI-QKD protocol [4].

Alice and Bob both emit single photons through a quantum channel to the middle of their link to perform Bell-state-measurement (BSM). The BSM module could be handled by Eve and the secret key generated can still be secure.

attacks, Eve exploits the flaws of the detectors to her benefit to gain information about the key. Hence, the measurement devices, apart from being of a high value, are not necessarily reliable for the secure operation of a QKD protocol. There is, however, a counterproposal to overcome this limitation [31, 32] as we explain next.

1.4.3 Measurement-device-independent QKD protocols

In an alternative approach to BB84 [1] and Ekert91 [3], a different generation of protocols was proposed, the measurement-device-independent (MDI) [4] QKD. Below there is a brief description of this protocol.

In the MDI-QKD (see Figure 1.4) a reversed EPR-based [33] QKD security proof is combined with BB84 source states. The main idea is that Alice and Bob would effectively share entangled states pair in their own laboratory using the teleportation trick. A more detailed description of MDI-QKD follows in Section 2.6.

In MDI-QKD type of protocols, the main goal is to close the gap between theory and practice with varying degrees of success, as detection devices, which are the most prone to various attacks. MDI-QKD has proved to be more tolerant against device inefficiencies (i.e. detection) and low channel loss and yet provide secure keys. Additionally the MDI-QKD is resilient against side-channel attacks on detector setups, such as the time-shift attack [34, 35], the re-mapping attack [36] and the blinding attack [37]. Moreover, it improves the security distance over QKD protocols that use conventional laser diodes [4].

In a practical implementation of a QKD protocol, there are various imperfections, such as the detection efficiency, dark counts in photodetectors, imperfect sources and channel loss. All these inefficiencies contribute to a constrained performance of a QKD protocol. This is usually measured by the corresponding rate at which the two users can establish a secret key, i.e. the secret key generation rate. In this thesis, I use the secret key generation rate as the main figure of merit for comparing the performance of different systems considered here.

Despite all commercial and experimental achievements in QKD [38, 39, 40, 41, 42], reaching arbitrarily long distances is still a remote objective. Because QKD relies on single photons to generate secret keys, this would impose numerous problems when long-distance communications is concerned. Limitations such as the channel loss restricts the distance of communications significantly. The fundamental solution to this problem, i.e., quantum repeaters, that is is known for over a decade. From early proposals by Briegel *et al.* [43] to the latest no-memory version by Munro *et al.* [44], quantum repeaters, typically rely on highly efficient quantum gates comparable to what we may need for future quantum computers. While the progress on that ground may take some time before such systems become functional, another approach based on *probabilistic* gate operations was proposed by Duan and coworkers [45], which could offer a simpler way of implementing quantum repeaters for moderate distances of up to around 1000 km. The latter systems require quantum memory modules with high coupling efficiencies to light *and* with coherence times exceeding the transmission delays, which are yet to be achieved together. In this thesis, we propose a protocol that, although is not as scalable as quantum repeaters, for certain classes of memories, to some extent, relaxes, the harsh requirements on memories' coherence times, thereby paving the way for the existing technologies to beat the highest distance records achieved for no-memory QKD links [38]. The idea behind our protocol was presented in [46], and, independently, it has also been used in [47]. This thesis proposes additional practical schemes and rigorously analyzes them under realistic conditions.

Our protocol relies on concepts from quantum repeaters, on the one hand and MDI-QKD on the other. The original MDI-QKD [4] relies on sending encoded photons by the users to a middle site at which a Bell-state measurement (BSM) is performed. This BSM can be done by an untrusted party, e.g., the service provider, which makes MDI-QKD resilient to detector attacks, e.g., time-shift, remapping, and blinding attacks [25, 26, 27, 28, 29, 30]. The security is then guaranteed by the reverse EPR protocol [33]. In our scheme, by using two quantum memories at the middle site, we first store the state of the transmitted photons in the memories, and perform the required BSM, only when both memories are loaded. This way, similar to quantum repeaters, we achieve a rate-versus-distance improvement as compared to the MDI-QKD schemes proposed in [4, 48], or other conventional QKD systems that do not use quantum memories.

There is an important distinction between our protocol and a conventional quantum repeater system. In a typical quantum repeater link, which relies on initial entanglement distribution among neighboring nodes, the repeat period for the protocol is mainly dictated by the transmission delay for the shortest segment of the repeater system [49, 50]. In our scheme, however, the repeat period is constrained by the writing time, including the time needed for the herald/verification process, into memories. This implies that using sufficiently fast memories, one can run our scheme at a faster rate than that of a quantum repeater, thereby achieving higher key generation rates, as compared to conventional QKD links, and at lower coherence times, as compared to probabilistic repeater systems. This increase in clock rate is what our proposal shares with the recently proposed third generation of quantum repeaters, which use quantum error correction codes to compensate for loss and errors, thus also being able to speed up the clock rate to local processing times [44]. The need for long coherence times remains one of the key challenges in implementing the first generations of quantum repeaters before the latest no-memory quantum repeater proposals can be implemented.

The above two benefits would offer a midterm solution to the problem of long-distance QKD. While our scheme is not scalable the same way that quantum repeaters are, it possibly allows us to use the existing technology for quantum memories to improve the performance of QKD systems. In the absence of fully operational quantum repeater systems, our setup can fill the gap between theory and practice and will become one of the first applications of realistic quantum memories in quantum communications.

It is worth mentioning that the setups we propose here are compatible with different generations of hybrid quantum-classical (HQC) networks [51]. In such systems, home users are not only able to use broadband data services, but they can also use quantum services such as QKD. MDI-QKD offers a user-friendly approach to the access part of such networks as the end users only require source equipment. Whereas, in the first generation of HQC networks, the service provider may only facilitate routing services for quantum applications, in the future generations, probabilistic, deterministic, and eventually no-memory quantum repeaters constitute the quantum core of the network. In each of these cases, our setups are extensible and compatible with forthcoming technologies for HQC networks.

1.5 Thesis overview and outline

In this thesis, I will depict examples of how we can use the idea of MDI-QKD with quantum memories (QMs) to achieve longer distances. Memory-assisted MDI-QKD requires milder conditions on memory devices thus making this protocol more feasible in the short term. In order to analyze this protocol, the inefficiencies of each module has to be taken into consideration. The reason is that these inefficiencies can affect the performance of the protocol itself, represented by its key generation rate. These inefficiencies include the channel loss, the detector efficiency, dark counts and decoherence in QMs. There will be an analytical explanation on how the key generation rate versus distance is obtained in each case. I will find the secret key rate as a function of many system parameters, for comparison on how the system is affected in each case. The thesis is structured as follows:

- In Chapter 2, I will review the relevant background including QKD protocols.
- In Chapter 3, I will analyse the performance of MDI-QKD, using single-photon sources that include modulation errors. I will show how the performance of the MDI-QKD protocol is affected by such errors.

- In Chapter 4, I will study how the addition of QMs in the MDI-QKD improves the key generation rate versus distance. By considering many sources of imperfection for the QMs I will set a specific set of requirements that need to attain in order for the memory-assisted MDI-QKD to outperform other conventional no-memory QKD systems.

- In Chapter 5, I will extend my analysis by considering a memory-assisted MDI-QKD with imperfect EPR sources. This protocol offers the ability to use a wider range of QMs that do not necessarily herald the storage of a photon.

- In Chapter 6, I will summarise my work and present a few topics for future research.

Chapter 2

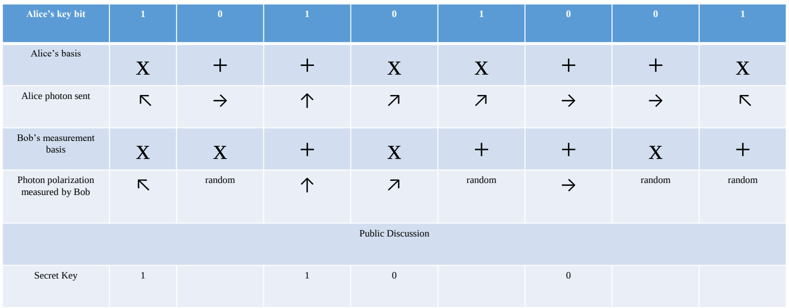
Background

2.1 Introduction

This Chapter gives a brief description of what is necessary to have as a background in order to understand the technical contribution of this thesis. This includes the review of a few QKD protocols relevant to the topics discussed in this thesis. I will begin with the primary prepare-and-measure protocol, BB84 [1], and that of enanglement-based, the Ekert protocol [3] for exchanging secret keys. I will continue with the decoy-state method, which allows for usage of weak laser pulses instead of ideal single photons in QKD. I will compare these main QKD protocols in terms of their secret key generation rates. Also I describe the original MDI-QKD [4], which is at the core of our work.

2.2 BB84 protocol

The benchmark of QKD is the well known BB84 [1], which was proposed by Charles Bennet and Gilles Brassard in 1984. BB84 protocol is based on the exchange of secret information with the use of non-orthogonal states. In this protocol, Alice is the sender and Bob is the receiver and they wish to communicate through a quantum channel, e.g., an optical fibre or free space. An authenticated public channel is also required. In BB84 Alice transmits a key bit by encoding a single photon in one of the four polarisation states. In doing so she chooses randomly between one of the two conjugate bases, namely, the rectilinear and diagonal. She assigns bit *0* to the horizontally (or 45^0) polarised photons and bit *1* to vertical (or -45^0) polarisation. Eve cannot tell with certainty to which photons Alice has assigned bit *0* or bit *1*. At the receiver, Bob also chooses one of the bases randomly and performs a polarisation measurement. After this, through an authenticated public channel, Alice and Bob announce to each other the choice of their bases for each bit of the key they measured. They both discard all key bits for which their bases do not agree, which could be around half of the message as seen in Figure 2.1. This procedure is called sifting. The post-processing procedure, i.e., the error correction and privacy amplification, is the next step in order to remove all the discrepancies in their keys and reduce any information that might be in Eve's knowledge. If there is an eavesdropper, then the percentage of the correct key bits drops to less than a certain threshold in which case they abort the protocol and try again. The discrepancy rate between the sifted keys of Alice and Bob is called quantum bit error rate (QBER). If the QBER is below a certain level, (between 11% [52] and 20% [53]) privacy amplification can be used to reduce Eve's knowledge of the key at the price of reducing the key length.



Alice's key bit	1	0	1	0	1	0	0	1
Alice's basis	X	+	+	X	X	+	+	X
Alice photon sent	↖	→	↑	↗	↗	→	→	↖
Bob's measurement basis	X	X	+	X	+	+	X	+
Photon polarization measured by Bob	↖	random	↑	↗	random	→	random	random
Public Discussion								
Secret Key	1		1	0		0		

Figure 2.1: Schematic description of the BB84 protocol.
Alice transmits randomly generated key bits. She chooses randomly between rectilinear and diagonal bases, to send a single photon. Bob measures all the photons after he received them from Alice, choosing randomly between the same two polarisation bases. After this, through an authenticated public channel, Alice and Bob announce to each other the choice of their bases for each bit of the key they measured. That would result in a sifted key shared between Alice and Bob.

As mentioned earlier, the security of the BB84 protocol relies primarily on the use of single photons due to the no cloning theorem [18]. Alice requires an ideal single photon source to transmit her information to Bob. Nonetheless the implementation of perfect single photon sources is currently practically impossible. Usually the single-photon sources produce multiphoton components, thus making them susceptible to eavesdropping attacks such as the photon-number-splitting (PNS) attack [2]. In the PNS attack, if there are more than one photon transmitted through the pulse in the channel, Eve can split off the extra photons and transmit the remaining single photons to Bob. Eve can therefore store with the help of a QM these extra photons and she measures it in the correct basis once Bob measures his and Alice announces her chosen basis publicly. In this way Eve can gain part of the information on the secret key thus compromising the security of the protocol. In the followng section, I will describe a solution to the PNS attack with the use of weak laser pulses instead of single photons in QKD.

2.3 Decoy-state method

The decoy-state [21] is proposed as a solution to minimise the effects of the security loophole for attacks such as the PNS in the BB84 protocol if the quantum information carriers are composed of multiphoton components. The use of lasers to send pulses of weak coherent states, to substitute single photons, makes the protocol more employable for a practical application. A weak coherent state source consists of multiphoton components, which will be explained below. In the decoy-state method [21], Alice sends two types of states: the signal states, for the key generation only, and, the decoy states, for detecting the presence of any eavesdropper. In the combination of the decoy state with the BB84, Alice chooses to send Bob the signal states and the decoy states with different intensities. We consider that Y_i known as the yield, is the conditional probability of a detection on Bob's side, conditioned that Alice sends i photons. More specifically the yield of the i-photon states Y_i mainly comes from two parts, the background and the true signal. Assuming that the background counts Y_0 are independent of the signal photon detection, then Y_i is given by:

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \tag{2.1}$$

Because Eve cannot discriminate between the signal and decoy states to extract the key, we have that the yield Y_i and QBER e_i of $i-$photon states is given respectively by

$$\begin{aligned} Y_i(decoy) &= Y_i(signal), \\ e_i(decoy) &= e_i(signal). \end{aligned} \tag{2.2}$$

In order to estimate Y_i and e_i terms by legitimate users, we can assume that an infinite number of decoy states are sent. For all pulses with intensity μ we have the overall gain Q_μ and the overall intrinsic error rate due to background noise of μ photon states is $E_\mu Q_\mu$ given by

$$Q_\mu = \sum_{i=0}^{\infty} Q_i, \tag{2.3}$$

and

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} \exp(-\mu), \tag{2.4}$$

where Q_i is the gain of $i-$photon states given by:

$$Q_\mu = Y_i \frac{\mu^i}{i!} \exp(-\mu). \tag{2.5}$$

If there are infinitely many intensities, then theoretically we can estimate the overall gain and QBER for the single photons Q_1 and e_1 with a good precision. It is proven that the least required amount of decoy states that can be used in practice is one or two [54]. According to the infinite decoy-state QKD protocol [55] the basic steps are:

- Alice transmits signal and decoy states to Bob, who in turn measures them in the two conjugate bases.
- Alice announces publicly the pulses she used for decoy states and they determine all the gains of signals and of decoy states.
- Alice and Bob compare all the bases used for the decoy states in order to find the QBER.
- Error correction and privacy amplification follows, in order to find the final secret key generated.

The key rate formula for the decoy-state procotol in the BB84 technique is derived by Lo *et. al.* from [56]. For infinitely many decoy states and long keys, the key rate has a lower bound given by:

$$R \geq q[Q_1[1-h(e_1)] - Q_\mu f h(E_\mu)], \tag{2.6}$$

where q is the basis reconciliation factor, f is the error correction inefficiency, and the binary entropy function $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. The error correction inefficiency denotes the ineneffciency of the error correction scheme, i.e., the ratio between the actual cost of error correction and its minimum value obtained by the Shannon's theorem, assumed to be constant and equal to $f = 1.16$. E_μ is the overall QBER for coherent photon states with μ average photon number. In the case of the BB84 scheme the reconciliation factor equals to $1/2$ due to the fact that half of the time Alice and Bob do not agree on the chosen basis. In Equation (2.6), we can assume $q = 1$ if the efficient [57] QKD scheme is used. The key rate formula of Equation (2.6) with $q = 1$ will be further used in Chapter 4. In the following subsection (2.4) I give a brief mathematical analysis for the key generation rate of the BB84 protocol.

2.4 BB84 Key Rate analysis

In this section we summarize the secret key generation rate for the efficient BB84 protocol [57] shown in Figure (2.2). In Figure (2.2), Alice is the transmitter sending pulses in either the rectilinear or diagonal basis and Bob is the receiver, which decodes the message. They communicate through an optical channel of distance L.

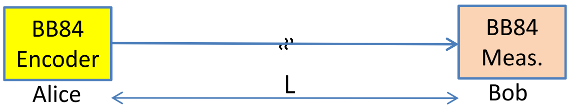


Figure 2.2: The setup for the BB84 protocol.

With a clock rate of R_S, the secret key generation rate is lower bounded by

$$R_{\text{BB84}} = R_S Y_1 [1 - h(e_1) - f h(e_1)], \tag{2.7}$$

in the single-photon case, and

$$R_{\text{BB84}} = R_S [Q_1 (1 - h(e_1)) - f Q_\mu h(E_\mu)], \tag{2.8}$$

in the (infinitely many) decoy-state case, where μ is the average number of photons for the signal state, which is dominantly used. In Equation (2.7), Y_1 is the yield of single photons, or the probability that Bob gets a click on his measurement devices assuming that Alice has sent exactly one photon, including the dark counts and is given by

$$Y_1 = Y_C + Y_E = 1 - (1 - \eta)(1 - p_{\text{dc}})^2, \tag{2.9}$$

where $\eta = \eta_{\text{ch}}(L)\eta_d$, with $n_{ch}(L) = \exp(-L/L_{\text{att}})$ being the loss or a channel with attenuation length L_{att}, η_d being the detector efficiency, and p_{dc} is the dark count rate per pulse. In Equation (2.9)

$$Y_C = (1 - p_{\mathrm{dc}}/2)(\eta + (1-\eta)p_{\mathrm{dc}}) \text{ and } Y_E = p_{\mathrm{dc}}[(1-\eta)(1-p_{\mathrm{dc}}/2) + \eta/2] \tag{2.10}$$

correspond, respectively, to the terms that, in the absence of misalignment, result in identical (Correct) versus non-identical (Error) bits shared by Alice and Bob. The QBER for the single photon case, e_1, is the same for both bases and is given by

$$e_1 = \frac{Y_E}{Y_1} \tag{2.11}$$

and the overall intrinsic error rate is given by

$$\begin{aligned} e_1 Y_1 &= e_d Y_C + (1-e_d) Y_E = e_0 Y_1 - (e_0 - e_d)(Y_C - Y_E) \\ &= e_0 Y_1 - (e_0 - e_d)\eta(1 - p_{\mathrm{dc}}), \end{aligned} \tag{2.12}$$

where $e_0 = 1/2$ and e_d is the total misalignment probability for the channel.

Similarly, in Equation (2.8),

$$\begin{gathered} Q_1 = Y_1 \mu e^{-\mu}, \\ Q_\mu = Q_C + Q_E = 1 - e^{-\eta\mu}(1-p_{\mathrm{dc}})^2, \\ Q_C = (1-p_{\mathrm{dc}}/2)(1 - e^{-\eta\mu} + e^{-\eta\mu} p_{\mathrm{dc}}), \\ Q_E = p_{\mathrm{dc}}[e^{-\eta\mu}(1-p_{\mathrm{dc}}/2) + (1-e^{-\eta\mu})/2], \end{gathered} \tag{2.13}$$

are the corresponding gain terms [56] for the overall gain of single photon states Q_1, of all pulses with intensity μ Q_μ, and the overall error probability Q_E. The overall intrinsic error rate is given by

$$\begin{aligned} E_\mu Q_\mu &= e_0 Q_\mu - (e_0 - e_d)(1 - e^{-\eta\mu})(1 - p_{\mathrm{dc}}), \qquad (2.14) \\ e_0 &= 1/2, \end{aligned}$$

and the overall QBER E_μ is given by

$$E_\mu = \frac{Q_E}{Q_\mu}. \tag{2.15}$$

The decoy-state technique can be used when the signals are driven by the users. In the following section, a different approach to exchanging secret keys is proposed, where the decoy-state method cannot be applied. Despite this, the next approach has an equal importance as the BB84 for the QKD.

2.5 Ekert protocol

An alternative approach to BB84 was introduced by Ekert in 1991, using entangled photon pairs [3]. This protocol relies on three properties of quantum entanglement. First is the fact that entangled states are perfectly correlated, second is the quantum non-locality and the last is the detection of eavesdroppers, whose attempts destroy these correlations.

Unlike the BB84, Alice and Bob in the Ekert protocol are now both receivers, connected to a central source that creates entangled photons sending one to Alice and one to Bob. The source could be untrusted (Eve could handle it) but the protocol is set in a way that the source emits pairs of polarisation singlet states [58] as

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle). \tag{2.16}$$

Next Alice and Bob choose one out of the three coplanar axes for a polarization measurement. Alice's and Bob's orientation analyzers represent a basis and are given accordingly by:

$$\phi_A = 0^\circ, 45^\circ, 90^\circ \tag{2.17}$$

and

$$\phi_B = 45^\circ, 90^\circ, 135^\circ. \tag{2.18}$$

If their bases match then their results will be anti-correlated. For instance if Alice measures vertical polarization then Bob will measure horizontal polarization and vice versa. If they choose different bases, then the results will be random.

Public discussion follows to exchange the bases that Bob and Alice chose. They discard the random results in order to establish the sifted key. For the results that match to prove their entanglement they must violate the Bell inequality [23]. One key feature of this protocol is its immunity against source attacks. If Eve tries to manipulate the source to her own advantage, she introduces errors, detectable by Alice and Bob, whose data will now be uncorrelated. In such a case Alice and Bob acknowledge Eve's presence and abort the protocol.

Many protocols succeeded the Ekert protocol relying on the security that entangled states provide. An example of these protocols is the BBM92 [22] that was proposed by Bennett, Brassard and Mermin and it is an entanglement-based form of the BB84 protocol. More proposed protocols that share the same idea was the time-reversed EPR protocol [32, 33] and the device-independent one [59]. The modified BB84 with entangled photons has been experiementally constructed [60].

The main drawbacks that both prepare-and-measure protocols and entanglement-based protocols face are the multiple attacks that can be performed on the measurement devices [61]. These attacks significantly reduce the security of the protocol itself. As an alternative to prepare-and-measure and entanglement-based protocols, measurement-device-independent (MDI-QKD) was proposed by Lo, Curty and Qi [4]. In the proposed protocol the measurement devices could be in the hands of untrusted parties. It relies on entanglement swapping and the time-reverse EPR [33] protocol. The decoy-state protocol can also be used giving it another benefit. In the next section, the key features of this protocol are described.

2.6 MDI-QKD protocol

In MDI-QKD [4] a reverse EPR-based QKD security proof [33] is combined with the BB84 source states to remove all the side-channel attacks in detectors automatically. Additionally in the current protocol, the decoy-state technique, which was described in Section 2.3, can be applied, using weak coherent pulses (WCPs) that are generated by a laser, as a source. The main idea is that Alice and Bob would effectively share entangled states in their own laboratory using the teleportation trick.

Figure 2.3 shows the setup. Alice and Bob prepare photons in one of the four possible BB84 polarisation states and in the measurement site a Bell state measurement is performed. The measurement device consists of linear optical elements as seen in Figure 2.3 with a $50-50$ beam splitter (BS), which on each end has a polarising beam splitter (PBS), and on each of the PBS output arms there is a single-photon detector. The measurement device is on the hands of an untrusted party called Eve. Eve announces which detectors click. The procedure is repeated several times by Alice and Bob. After the bases that were chosen are publicly announced through a public channel, Alice and Bob compare their results and discard the ones that their bases do not match and use the rest for key generation after error correction and privacy amplification. The security of the MDI-QKD relies on the time-reverse EPR protocol, therefore the measurement device module does not need to be trusted.

MDI-QKD offers several advantages over other QKD schemes. It removes all the side-channel attacks in detectors automatically since all the measurements can be done by Eve [33]. This is a benefit over the standard BB84 [1] and Ekert [3] protocols, where either Alice or Bob, or both

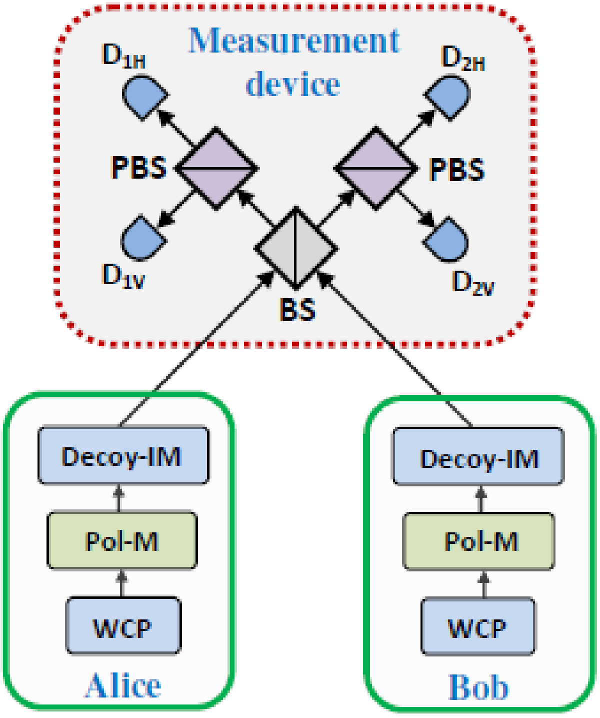


Figure 2.3: The MDI-QKD set up [4]
The main idea is that Alice and Bob send either single photons or phase-randomized weak coherent pulses in one of the four possible BB84 polarisation states [1] and send them to an untrusted relay (Eve) placed in the middle. This relay setup performs partial BSM. On each end of the $50-50$ beam splitter (BS), there are two polarising beam splitters (PBS) that on each arm have a single-photon detector. A successful BSM associates with two clicks and identifies two of the four Bell states.

parties must perform some measurements. The transmission distance in MDI-QKD could reach almost double the distance used in conventional BB84 setups. Also the key generation rate is as good as the ones that use entangled photon pairs. Additionally MDI-QKD does not require a near unity detection efficiency, but, using post-selection, unsuccessful BSMs can be removed without compromising the security. To summarise, MDI-QKD is attractive for practical implementation and fully effective against any side channel attacks on detectors. An analysis of the key rate of MDI-QKD follows next.

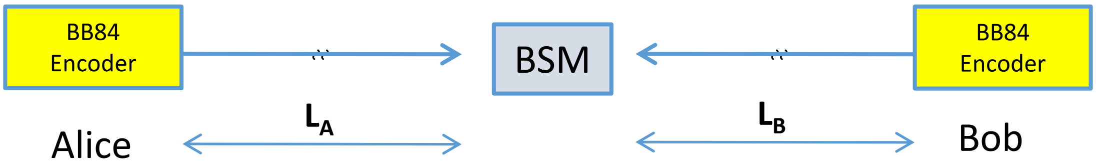


Figure 2.4: The MDI-QKD using two single-photon source encoders.

2.6.1 MDI-QKD key rate analysis

The secret key generation rate for the MDI-QKD scheme of Figure 2.4 is lower bounded by [48]

$$R_{\mathrm{MDI-QKD}} = R_S Y_{11}[1 - h(e_{11;X}) - fh(e_{11;Z})], \tag{2.19}$$

in the single-photon case, where Y_{11} is the conditional probability of successful middle BSM conditioned that Alice and Bob have sent exactly a single photon at the beginning using the same basis, R_S is the single photon repetition rate. The QBER in X and Z basis are given by $e_{11;X}$ and $e_{11;Z}$ when Alice and Bob use exactly single photons.

$$R_{\mathrm{MDI-QKD}} = R_S[Q_{11}(1 - h(e_{11;X})) - fQ_{\mu\nu;Z}h(E_{\mu\nu;Z})], \tag{2.20}$$

in the decoy-state case, where μ (ν) is the average number of photons for signal states sent by Alice (Bob). The QBER in the Z basis becomes $E_{\mu\nu;Z}$ when using μ (ν) as the average number of photons for signal states instead of single photons. Here, Q_{11} is the overall probability of a successful BSM if Alice and Bob, respectively, send pulses with μ and ν average number of photons and is given by

$$Q_{11}(\eta_a, \eta_b) = \mu\nu e^{-\mu-\nu} Y_{11}(\eta_a, \eta_b) \tag{2.21}$$

where $\eta_a = \eta_{\mathrm{ch}}(L_A)\eta_d$ and $\eta_b = \eta_{\mathrm{ch}}(L_B)\eta_d$ are transmission coefficients of each leg with lengths, L_A and L_B, respectively in Figure 2.4, and [48]

$$\begin{gathered}
Y_{11}(\eta_a, \eta_b) = (1 - p_{\mathrm{dc}})^2 \left[\tfrac{\eta_a \eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)p_{\mathrm{dc}} + 4(1-\eta_a)(1-\eta_b)p_{\mathrm{dc}}^2\right], \\
e_{11;X}(\eta_a, \eta_b, e_d)Y_{11}(\eta_a, \eta_b) = e_0 Y_{11}(\eta_a, \eta_b) - (e_0 - e_d)(1 - p_{\mathrm{dc}})^2 \eta_a \eta_b / 2, \\
e_{11;Z}(\eta_a, \eta_b, e_d)Y_{11}(\eta_a, \eta_b) = e_0 Y_{11}(\eta_a, \eta_b) - (e_0 - e_d)(1 - p_{\mathrm{dc}})^2 (1 - 2p_{\mathrm{dc}}) \eta_a \eta_b / 2
\end{gathered} \tag{2.22}$$

with e_d being the total misalignment probability. In the scheme of Figure 2.4, $e_d = e_{dA}(1-e_{dB}) + e_{dB}(1-e_{dA})$, where $e_{dA}(e_{dB})$ is the misalignment parameter for Alice (Bob) channel.

Similarly, using the results obtained in [48], we have

$$\begin{aligned} Q_{\mu\nu;Z} &= Q'_C + Q'_E \\ E_{\mu\nu;Z}Q_{\mu\nu;Z} &= e_d Q'_C + (1-e_d)Q'_E, \end{aligned} \tag{2.23}$$

where

$$\begin{aligned} Q'_C &= 2(1-p_{\mathrm{dc}})^2 e^{-\mu'/2}\left[1-(1-p_{\mathrm{dc}})e^{-\eta_a\mu_a/2}\right]\left[1-(1-p_{\mathrm{dc}})e^{-\eta_b\mu_b/2}\right] \\ Q'_E &= 2p_{\mathrm{dc}}(1-p_{\mathrm{dc}})^2 e^{-\mu'/2}[I_0(2x)-(1-p_{\mathrm{dc}})e^{-\mu'/2}]. \end{aligned} \tag{2.24}$$

In the above Equations, $I_0(x)$ is the modified Bessel function of the first kind and

$$x \quad = \sqrt{\eta_a\mu\eta_b\nu}/2, \tag{2.25}$$

$$y \quad = (1-p_{\mathrm{dc}})e^{-\frac{1}{4}(\eta_a\mu+\eta_b\nu)}, \tag{2.26}$$

$$\mu' \quad = \eta_a\mu+\eta_b\nu. \tag{2.27}$$

2.7 Memory-assisted MDI-QKD

In this thesis, we extend the idea of an MDI-QKD protocol, to achieve longer distances, with the use of QMs. QMs can be located next to the BSM module in order to reduce the effect of channel loss on the key rate. The key advantage of our proposed memory-assisted MDI-QKD as compared to the original MDI-QKD, is its higher resilience to channel loss and dark count.

In our protocol, Alice and Bob, at a rate R_S, send BB84 encoded pulses to the middle station (dashed box in Figure (2.5)). At the QMs, for each incoming pulse, we either apply a loading process by which we can store the state of the photons into memories and verify it, or use the indirectly heralding scheme of Figure (2.5(b)). Once successful for a particular QM, we stop the loading procedure on that QM, and wait until both memories are loaded, at which point, a BSM is performed on the QMs. The BSM results are sent back to Alice and Bob, and the above procedure is being repeated until a sufficient number of raw key bits is obtained. The rest of the protocol is the same as that of MDI-QKD. Sifting and postprocessing will be performed on the raw key to

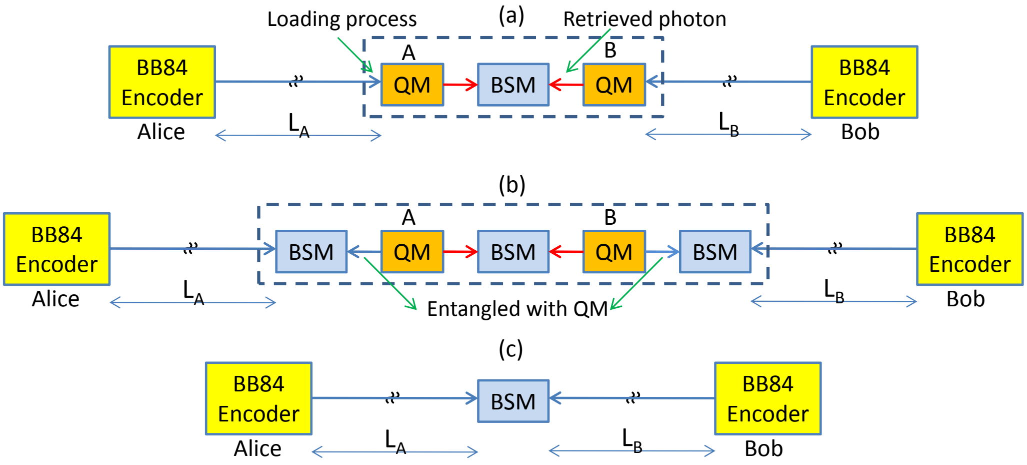


Figure 2.5: (a) MDI-QKD with directly heralding quantum memories. Alice and Bob use the efficient BB84 protocol to encode and send pulses to their respective QM in the middle of the link. At each round, each QM attempts to store the incoming pulse. Once they are both loaded, we retrieve the QMs' states and perform a BSM on the resulting photons. (b) MDI-QKD with indirectly heralding quantum memories. At each round, an entangling process is applied to each QM, which would generate a photon entangled, in polarization, with the QM. These photons interfere at the BSM modules next to the QMs with incoming pulses from the encoders. As soon as one of these BSMs succeeds, we stop the entangling process on the corresponding QM, and wait until both QMs are ready for the middle BSM operation. In this case, QMs are not required to be heralding; a trigger event is declared by the success of the BSM located between the QM and the respective encoder. (c) The original MDI-QKD protocol [4].

obtain a secret key. In this thesis, we neglect the finite-size-key effects in our analysis [62].

In the no-memory MDI-QKD case, the condition set for a successful BSM, is that both pulses must survive the path loss. Therefore, the key generation rate scales with the loss in the entire channel. In our scheme, each pulse, still requires that it will survive the path loss over half of the link, but this can happen in different rounds for the signal sent by Alice as compared to that of Bob. We essentially achieve the quantum repeater benefit in that the key generation rate, in the symmetric case, scales with the loss over half of the total distance. Moreover, in the case of directly heralding memories, our scheme is roughly immune against dark counts [47]. This is because the measurement efficiency in the BSM module is typically a few orders of magnitude higher than that of dark count rates. Dark counts will then only sightly add to the error rate. In our scheme, memory decoherence errors play a major role as we will explain in detail in Chapter 4.

Moreover, we study what are the writing times of these two different type of QMs. The writing time is a crucial parameter that defines the performance of the key rate versus distance. More specifically, writing time, in the directly heralding QMs, denotes the time difference between the time that a pulse arrives at the QM and the time that a successful/unsuccessful loading is denoted. The writing time for the indirectly heralding QMs, denotes the difference between the entangling process and BSM operation.

Another important parameter we take into consideration is the QM's coherence or dephasing time (T_2). This parameter directly affects the key rate versus distance as well.

As we explain in detail in Chapter 4, for high values of coherence times and short writing times, we prove that a memory-assisted system with suitable QM candidates, can outperform, in terms of key rate conventional no-memory QKD systems.

2.8 The main contributions of this thesis

In Chapter 1, we introduced the key features of QKD and the challenges it deals for a realistic implementation. In this thesis, we work on the following challenges to find possible solutions that can improve the performance of the system. These problems and our proposed solutions are given below:

Problem: QKD offers unconditional security based on the laws of quantum physics, however the practical implementation of specific QKD systems is prone from possible attacks that can be performed on the measurement parts of the system, if controlled by the users. MDI-QKD offers an alternative solution to overcome this limitation. Therefore the modeling of such a system has to be studied in full to check:

1. how it performs in a practical scenario, when, for instance, sources are imperfect in the sense that there are errors in the state-preparation stage; and

2. how can quantum memories improve the performance of an MDI-QKD system regarding its distance and rate and what requirements they must fullfil in order to achieve the highest possible performance.

Our contribution: In Chapter 3, we analyse a typical MDI-QKD system that uses single-photon sources but with potential modulation errors. We give a detailed description of how the key rate is affected by these errors, which allows us to identify the regimes of operation. We will show that MDI-QKD can still perform efficienctly under certain assumptions on the fidelity of each single-photon state.

Our contribution: In Chapter 4, we fully analyse an MDI-QKD system with imperfect QMs, where we analytically compute the secret key rate. QMs are of great importance when it comes to reach longer distances as it proven by the results. We find regimes of operation where our proposed system performs better than conventional QKD systems. The results are promising for near-future practical implementations.

Problem: The memory-assisted MDI-QKD needs to relax the constraints on the QMs to enable the use of a larger number of the avalaible QMs.

Our contribution: In Chapter 5 an alternative approach to the memory-assissted MDI-QKD is to use QMs that are indirectly heralding. We combine the memory-assisted MDI-QKD setup with entangled photon-pair sources. As we consider a realistic scenario we combine the idea of EPR sources being imperfect by including modulation errors. A full analysis to retrieve the key is provided and a comparison to the previous case is made. We show that this system allows us to still have a fully functional and efficienct system under certain assumptions.

Chapter 3

MDI-QKD with imperfect encoders

3.1 Introduction

In this chapter we focus on the state-preparation (modulation) flaws in the single-photon sources in an MDI-QKD setup. In the key rate analysis presented in Chapter 2, it was assumed that each source will generate the exact BB84 states as required. In a practical setup, this may not be a realistic assumption for the source. The key objective is to establish an employable MDI-QKD protocol that remains secure under the assumption of both imperfect single-photon sources and imperfect measurement devices. The main goal in this chapter is to calculate the key generation rate versus distance for single-photon sources with state-preparation imperfections. During the preparation of this thesis, a similar work has been reported by Lo *et al.* [63]. The work presented here has been obtained independently, and goes beyond the results presented in [63].

An ideal BB84 encoder has two properties. The first is that the source emits ideal single photons and the second is that the information is encoded without errors. However, these two assumptions can hardly be fulfilled with the current technology. Even single-photon sources that generate exactly one photon may produce a different polarisation from the initially intended state during the encoding process. This type of error is referred to as modulation errors. To address this issue, in this chapter, we consider imperfect encoders, as shown in Figure 3.1. The main objective is to analyse how the performance of this practical scenario would be affected when modulation errors are accounted for. We point out that this analysis is a preliminary step for Chapter 5, where imperfect EPR sources are used in a memory-assisted MDI-QKD.

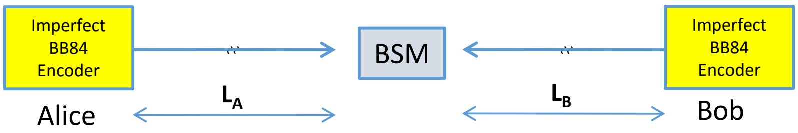


Figure 3.1: Asymmetric setup with imperfect BB84 encoders in an MDI-QKD scheme.

3.2 This chapter's contribution

- We analyse the MDI QKD system when the sources of each user are prone to modulation errors at the state-preparation stage. We fully analyse how to obtain the key rate and QBER formulas in this scenario.
- We consider different initial states of the single-photon source for each user. Firstly we assume that both users have imperfect single-photon sources that have a mixture of two single-photon states in a symmetric setup, where both users are at equal distance from the middle measurement module. We compare the key rate and QBER against the ideal case.
- In the second case, we consider that only one user has an imperfect single-photon source, whereas the other one has an ideal one. The reason is that we will be using an analogous case in Chapter 5.
- Lastly, we compare the case where the single-photon states can tolerate more imperfections by including cross-terms in our initial density matrix.

This chapter is organised as follows. Section 3.3 analyses the MDI-QKD with imperfect single-photon sources. In Section 3.4, an analysis of the key rate is provided. In Section 3.5 the results are summarised for different setups and fidelities and we conclude in Section 3.6.

3.3 System description

In this chapter, we assume that Alice and Bob are equipped with single-photon sources that generate qubit states but not necessarily in the desired polarised BB84 state. Alice and Bob follow the same procedure as described in Section 2.6 for a typical MDI-QKD with the difference that the single-photon sources are assumed imperfect (see Figure 3.1). The outcome of such an imperfect encoder, for user $x = A, B$, is modeled by the following density matrix:

$$\rho_{x;K}^{(m)} = \alpha_{x;K}^{(m)}|H\rangle\langle H| + \beta_{x;K}^{(m)}|H\rangle\langle V| + \beta_{x;K}^{(m)*}|V\rangle\langle H| + \gamma_{x;K}^{(m)}|V\rangle\langle V|, \tag{3.1}$$

where $m = \{0,1\}$ represents the transmitted bit in basis $K = \{X, Z\}$. $|H\rangle$ and $|V\rangle$ are two of the four BB84 polarised states in horizontal and vertical polarizations. $\alpha_{x;K}^{(m)}$, $\beta_{x;K}^{(m)}$, $\beta_{x;K}^{(m)*}$ and $\gamma_{x;K}^{(m)}$ are the probabilities respectively for the BB84 polarised states respectively $|H\rangle\langle H|$, $|H\rangle\langle V|$, $|V\rangle\langle H|$ and $|V\rangle\langle V|$. According to the normalization fo the density matrix the diagonal elements must obey the following condition $\alpha_{x;K}^{(m)} + \gamma_{x;K}^{(m)} = 1$. We use the same notation as in Chapter 2 for other system parameters. In particular, the distance between Alice (Bob) and the measurement module is denoted by L_A (L_B). The total distance between Alice and Bob is denoted by $L = L_A + L_B$. The transmission coefficient for a channel with length l is given by

$$\eta_{\text{ch}}(l) \equiv \exp(-l/L_{\text{att}}), \tag{3.2}$$

where L_{att} is the attenuation length of the channel (roughly, 22 km for 0.2 dB/km of loss).

Next we obtain the secret key generation rate for the scheme of Figure 3.1, when input states are given by Equation (3.1). Suppose Alice is sending bit m and Bob is sending bit n, in basis K. Their joint input state is then given by

$$\rho_{AB;K}^{(mn)} = \rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}. \tag{3.3}$$

In the following we model what happens to the initial state $\rho_{A;K}^{(m)}$ and $\rho_{B;K}^{(n)}$ once the corresponding photons travel through the setup of Figure 3.2. We model the path loss and detector efficiencies by beams splitters (BSs), as showing in Figure 3.2, the transmission coefficients $\eta_{ch}(L_A)$, $\eta_{ch}(L_B)$, and η_d. Their combined effect can then be represented by two beam splitters with transmission coefficients $\eta_\alpha = \eta_{ch}(L_A)\eta_d$, for Alice's side, and $\eta_\beta = \eta_{ch}(L_B)\eta_d$, for Bob's leg. If we represent the quantum operator by a beam splitter with transmissivity η by B_η, the joing state right before the $50-50$ BS is given by

$$\rho_{AB;K}^{(mn)'} = tr_V(B_{\eta_\alpha}B_{\eta_\beta}(\rho_{AB;K}^{(mn)})B_{\eta_\beta}^{\dagger}B_{\eta_\alpha}^{\dagger}), \tag{3.4}$$

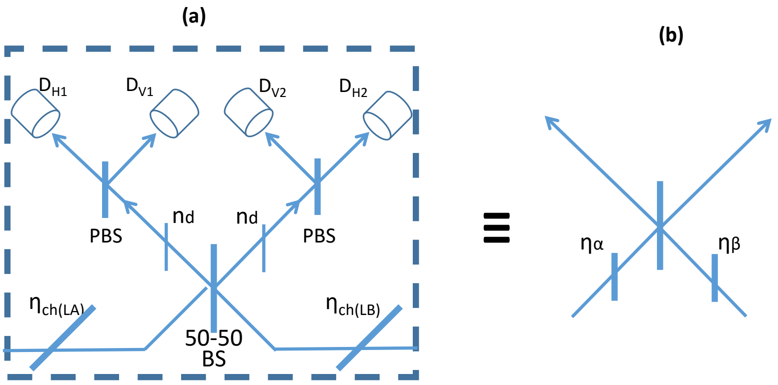


Figure 3.2: Modeling of the channel loss and detection efficiency in the BSM module.

where

$$B_\eta|P\rangle|0\rangle = \sqrt{n}|P\rangle\langle 0| + \sqrt{1-n}|0\rangle\langle P|, \tag{3.5}$$

and $P = \{H, V\}$ denotes a photon in one of the polarised BB84 states and tracing is done over all vacuum modes entering the BSs in Figure 3.2(b).

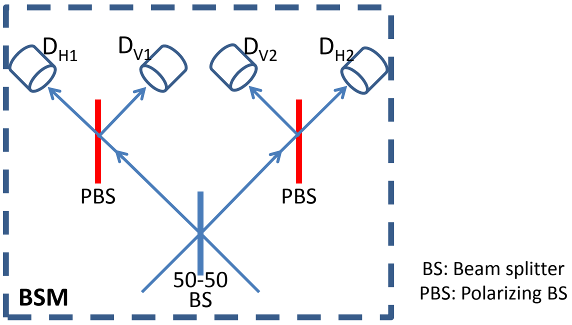


Figure 3.3: Bell-state measurement module for polarization states.

Next in order to model the BSM operation (see Figure 3.3), we apply the butterfly operator B_{BF} that includes the operation of both the BS and Polarising BS (PBS) (see Appendix C). With the help of MATLAB, we apply the butterfly operator B_{BF} on $\rho^{(mn)'}_{AB;K}$. The density matrix right before photodetection, $\rho^{(out)}_{AB}$, in Figure 3.3, is then given by

$$\rho^{(out)}_{AB} = B_{BF}(\rho^{(mn)'}_{AB;K})B^{\dagger}_{BF}. \tag{3.6}$$

Having calculated the output state, an analysis of the key rate will follow in the next section.

3.4 Key rate analysis

In this section we obtain the parameters needed to calculate the key rate in the case of imperfect single-photon sources. We start with the output state in Equation (3.6). One needs to apply the measurement operators $M_{D_iD_j}$ to find all possibilities of a successful BSM. More specifically, the probability that detectors i and j, where $i, j = H_1, V_1, H_2, V_2$ in Figure 3.3 click is given by

$$P_{D_iD_j}(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}) = tr(\rho_{AB}^{(out)} M_{D_iD_j}), \tag{3.7}$$

where measurement operators are defined by

$$\begin{aligned} M_{D_iD_j} &= (1-p_{\text{dc}})^2[I_i - (1-p_{\text{dc}})|0\rangle_{ii}\langle 0|] \\ &\otimes[I_j - (1-p_{\text{dc}})|0\rangle_{jj}\langle 0|] \\ &\otimes|0\rangle_{kk}\langle 0| \\ &\otimes|0\rangle_{ll}\langle 0|, \end{aligned} \tag{3.8}$$

where i, j are the corresponding detectors that click, whereas k, l are the single-photon detectors in Figure 3.3, that do not click, I is the identity operator and p_{dc} is the dark count probability. The probability that an acceptable click pattern occurs in the K basis, similar to Section 2.6.1 is defined as

$$Q_{AB}^K = Q_C^K + Q_E^K, \quad K = X, Z, \tag{3.9}$$

where

$$Q_{AB}^K = \frac{1}{4} \sum_{m=0,1} Q_{AB}(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}), \tag{3.10}$$

and more analytically is given by

$$\begin{aligned} Q_{AB}^K(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}) &= P_{D_{H_1V_1}}(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}) + P_{D_{H_1V_2}}(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}) \\ &+ P_{D_{V_1H_2}}(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}) + P_{D_{H_2V_2}}(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(n)}). \end{aligned} \tag{3.11}$$

The error terms in Z basis, Q_E^Z, corresponds to when Alice and Bob send the same bit, and it is given by

$$Q_E^Z = \frac{1}{2} \sum_{m=0,1} Q_{AB}^Z(\rho_{A;K}^{(m)} \otimes \rho_{B;K}^{(m)}), \tag{3.12}$$

where Q_{AB}^Z defined by Equation (3.11) and represents the probability of a successful BSM if Alice and Bob send a state given in the argument. The QBER in the Z basis is then given by

$$e_{11;Z} = \frac{Q_E^Z}{Q_{AB}^Z}. \tag{3.13}$$

The error probability in the X basis can be calculated by considering two cases. If the two send identical its, we have errors if we get two clicks on two orthogonally polarised detectors from two opposite sides, i.e., $D_{H_1V_2}$ or $D_{V_1H_2}$ (see Figure 3.2):

$$Q_{E1}^X = \frac{1}{2} \sum_{m=0,1} [P_{D_{H_1V_2}}(\rho_{A;X}^{(m)} \otimes \rho_{B;X}^{(m)}) + P_{D_{V_1H_2}}(\rho_{A;X}^{(m)} \otimes \rho_{B;X}^{(m)})] \tag{3.14}$$

If the bits sent from the users are complimentary then an error is occured in the case that two detectors click on the same side, i.e., $D_{H_1V_1}$ or $D_{H_2V_2}$ (see Figure 3.2). Then the error probability in the X basis becomes

$$Q_{E2}^X = \frac{1}{2} \sum_{m=0,1} [P_{D_{H_1V_1}}(\rho_{A;X}^{(m)} \otimes \rho_{B;X}^{(1-m)}) + P_{D_{H_2V_2}}(\rho_{A;X}^{(m)} \otimes \rho_{B;X}^{(1-m)})] \tag{3.15}$$

The QBER in the X basis is then given by

$$e_{11;X} = \frac{Q_E^X}{Q_{AB}^X}, \tag{3.16}$$

where $Q_E^X = Q_{E1}^X + Q_{E2}^X$.

Finally to find the key rate we have to take into account the probability of a successful click pattern in the Z basis as given from Equation (3.11) when the input state is given by Equation (3.1), given that the users have sent a single-photon each. Then the key rate is given by [64]

$$R \geq Q_{AB}^Z[1 - h(e_{11;X}) - fh(e_{11;Z})]. \tag{3.17}$$

Having fully analysed the key rate formula and the QBER we move on to the next section to apply numerical results in specific cases, such as the symmetric setup when the source fidelities change in a given input density matrix.

3.5 Numerical results

In this section, we study the impact of different parameters on the secret key generation rate of our scheme in different cases. We compare in a symmetric setup the QBER in X and Z bases and additionally the secret key generation rate per transmitted pulse for different fidelities of the single-photon BB84 states. We continue with the case of an imperfect single-photon source on one side and an ideal single-photon source on the other side to obtain again the QBER in X and Z bases and the key rate for both the asymmetric and symmetric setups. In the asymmetric setup we make the assumption that Alice is at distance $L_A = L$ from the measurement module, whereas Bob is at zero distance from the measurement module, i.e., $L_B = 0$. We have used Matlab to analytically obtain expressions for Equations (3.12), (3.16) and (3.17). In the symmetric setup the distance for Alice and Bob is considered equal, i.e., $L_A = L_B = L/2$. Finally, we compare the results of the two setups. Next we compare the symmetric and asymmetric setups again in terms of the secret key rate and QBER versus distance. All results have been obtained assuming an error correction inefficiency $f = 1.16$, 0.2 dB per km of loss in the channel, detection efficiency of $\eta_d = 0.15$, dark count rate per pulse $p_{\mathrm{dc}} = 3 \times 10^{-6}$, and no misalignments, i.e., $e_{dA} = e_{dB} = 0$. We used the density matrix from Equation (3.1) where Alice and Bob use the BB84 encoded single photon states in either X or Z basis and we analyse how these parameters change under different assumptions on the fidelity of the input density state. The fidelity is a parameter that estimates the quality of a state. In this case we are studying the quality of the single-photon states and their imperfections in two scenarios, when the users both use an imperfect single-photon source and when one user uses an imperfect single-photon source and the other uses a perfect single-photon source.

- Case A

  In the case that both users use imperfect single-photon sources, then the input density matrix stands as Equation (3.1). We want to compare the QBER terms in X and Z basis, for different fidelities of the diagonal terms. Hence we take the non-diagonal terms equal to zero ($\beta, \beta^* = 0$) from Eq. (3.1). The input state for Alice and

  $$\rho_{A;K}^{(m)} = \alpha_{A;K}^{(m)} |H\rangle\langle H| + \gamma_{A;K}^{(m)} |V\rangle\langle V| \tag{3.18}$$

  and similarly for Bob

  $$\rho_{B;K}^{(n)} = \alpha_{B;K}^{(n)} |H\rangle\langle H| + \gamma_{B;K)}^{(n)} |V\rangle\langle V| \tag{3.19}$$

  where $\alpha + \gamma = 1$ and $m, n = \{0, 1\}$ represents the transmitted bit in basis $K = \{X, Z\}$. Alice's input state for bit zero is given by

$$\rho^{(0)}_{(A;Z)} = F|H\rangle\langle H| + (1-F)|V\rangle\langle V|, \tag{3.20}$$

and for bit one,

$$\rho^{(1)}_{(A;Z)} = F|V\rangle\langle V| + (1-F)|H\rangle\langle H|, \tag{3.21}$$

where F is the fidelity of the single-photon state with given input in the Z basis. Bob's input states are similar to Equations (3.20) and (3.21). Neglecting all other sources of error but the modulation errors, the QBER in Z becomes

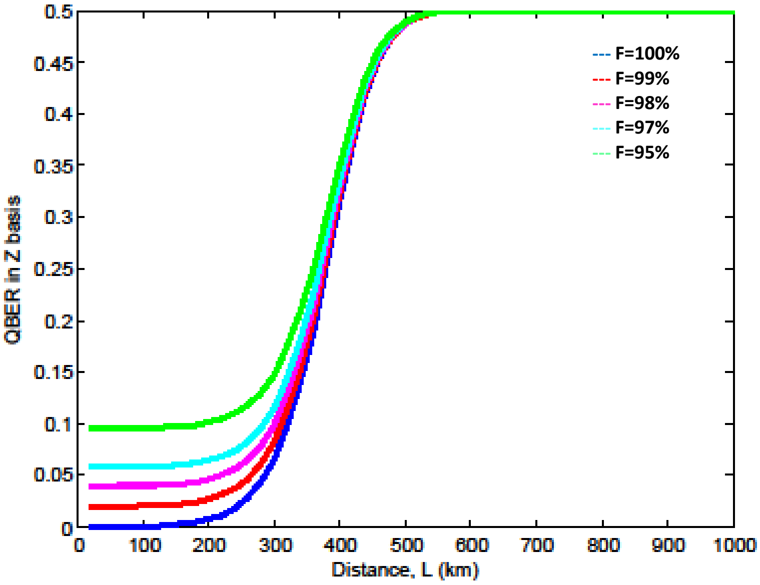


Figure 3.4: This is a comparison of the QBER-versus-distance in the Z and X basis of a symmetric setup for different fidelity values.

$$\begin{aligned} e_{11;Z} &= \frac{2F(1-F)}{2F(1-F)+F^2+(1-F)^2} \\ &= 2F(1-F). \end{aligned} \tag{3.22}$$

To derive the QBER in Z basis, we have considered the cases that we have both users send identical bits but due to the imperfections of single photons described by Equations (3.20) and (3.21) there is a probability to have a click on two detectors as expected in the correct case. For instance, if Alice and Bob send bit zero, then there is a probability $Q_E^Z = 2F(1-F)$ to get a correct pattern of clicks. We use a similar single-photon state with fidelity F to the intended state for Alice or Bob in the X basis. For instance for bit zero, we have

$$\begin{aligned} \rho^{(0)}_{(A;X)} &= F|+\rangle\langle+| + (1-F)|-\rangle\langle-| \\ &= \frac{1}{2}(|H\rangle\langle H| + |V\rangle\langle V|) + \\ &\quad \frac{(2F-1)}{2}(|H\rangle\langle V| + |V\rangle\langle H|) \end{aligned} \tag{3.23}$$

Under these assumptions, the QBER in X is equal to the Z basis. Figure 3.4 shows the QBER versus distance for different values of fidelity in the scenario of a symmetric setup. It can be seen that as the fidelity is lower the QBER is increased due to the inefficiencies from the source's part. If the fidelity remains higher than $F = 95\%$ then the protocol is still secure and practically employable. For values roughly lower than $F = 95\%$ the protocol is insecure. At low distances, the major source of error is the modulation error so the QBER follows the relation in Equation (3.21). The QBER becomes very high for distances of roughly 300 km because the dark count effects becomes the major source of errors in long distances. The QBER in X basis is similar to the QBER in Z.

- Case B

In the case that Alice uses an imperfect single-photon source and Bob uses instead an ideal single-photon source, then the input density matrix for Bob according to Equation (3.1) will become the same as Equation (3.19) with the difference that either α or γ becomes 0 and the other one becomes 1. For Alice the input state is given by Equations (3.20) and (3.21). The QBER in Z, in the low distance regime is then given by

$$e_{11;Z} = \frac{2(1-F)}{2F+2(1-F)} = 1-F. \tag{3.24}$$

The QBER in X is equal to the one from Z basis for the above input setting. The results for the QBER in Z are given in Figure 3.5. From Figure 3.5, we can see that as the fidelity decreases the state-preparation flaws contribute to higher values of QBER when compared to the corresponding values of QBER in Z basis for the same distance. This is similar to the QBER in Figure 3.4 with the difference that in the former, the values of QBER is almost half the value than the latter. This is due to the fact that the QBER in the case where both users have imperfect single-photon sources there is a higher chance for a modulation error at the sources' side, whereas if only one user uses an imperfect source and the other has a perfect single-photon source, the chance is lower.

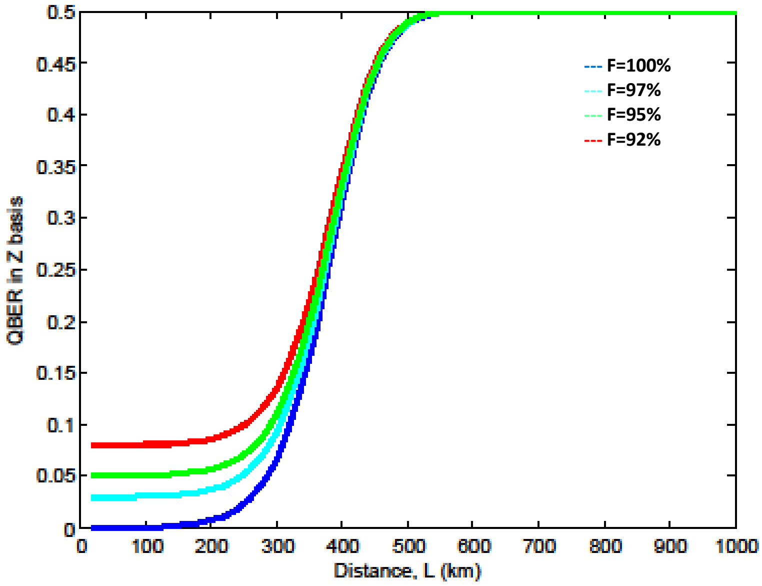


Figure 3.5: Comparison of the QBER in Z basis for a symmetric setup for different fidelity values using an imperfect single-photon source and an ideal single-photon source.

- Case C

Here, we study the effect of the non-diagonal terms, in the input density matrix Equation (3.1) ($\beta, \beta^* > 0$). We have made the assumption, for simplicity, that only the X basis accepts non-ideal single photons, whereas the Z basis accepts only perfect single photon states. The motivation behind this assumption is to study how it would affect the performance of the key generation rate if one of the single-photon encoders tolerates modulation errors and the other one is considered an ideal single-photon encoder. We use this assumption in Chapter 5.

The input density matrix for each user is given similarly to Equation (3.23) with the difference that the fidelity includes also the non-diagonal terms. Figure 3.6 shows how the QBER in X basis changes versus distance for different values of the non-diagonal terms in a symmetric setup. In this scenario we kept the values for Z the same and equal to the ideal single photon scenario. As we can see from this figure the lower the fidelity, the higher the QBER is at the sources' side. Similarly for longer distances than roughly 300 km the dark count effect becomes dominant over the correct clicks leading to non secure keys being generated. The fidelity is proportionally related to the non-diagonal terms therefore for higher values of fidelity the higher the values of the non-diagonal terms will be. Given the QBER in Z basis is very small, the QBER in X can be more than 11%.

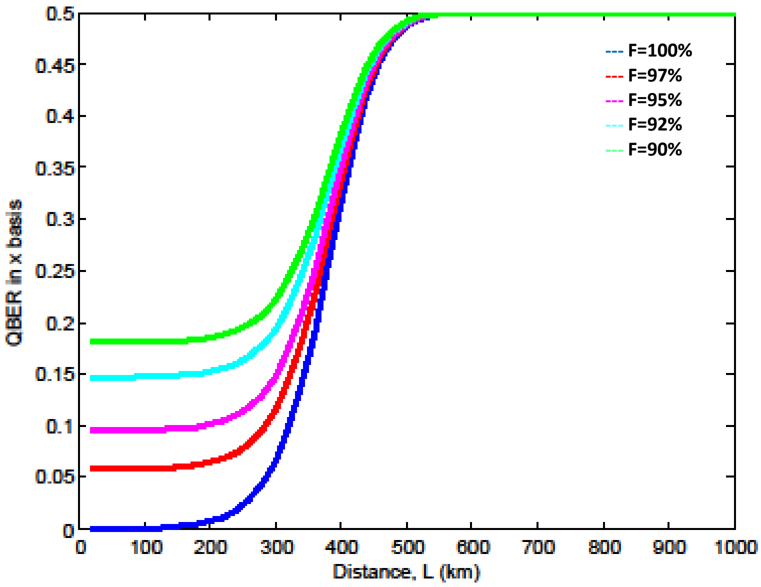


Figure 3.6: This is a comparison of the QBER-versus-distance in the X basis of a symmetric setup for different fidelity values of the non-diagonal terms.

In the next section we will compare in the above three cases how the key rate versus distance performance is affected in each scenario.

3.5.1 Rate-versus-distance

In this sections, we discuss the effects of fidelity and symmetry of the setup on the secret key generation rate. We make a comparison for the symmetric ($L_A = L_B = L/2$) and asymmetric ($L_A = L$ and $L_B = 0$) setup cases respectively to the cases taken in the previous section.

- Case A

In this scenario both Alice and Bob use imperfect single photon states (Equation (3.18) and (3.19) where the non-diagonal terms are taken as zero). In Figure 3.7, we can see that, for a symmetric setup, as the fidelity of the single photon states decreases the secure distance becomes lower. Secure distance is defined as the distance where the QBER is lower than 11%. The fidelity of a single photon source affects directly the QBER in both bases and therefore the key rate in terms of distance. For values of fidelity equal and lower than 95% there is a significant drop on the distance, reaching roughly 150 km. If the fidelities are kept higher than 97%, the distance ranges from around 280 km to the highest given by 320 km (for F=100%). The cut-off distance in each case is due to the path loss and dark count being dominant over the correct clicks, therefore there is a lower chance to retrieve a secret key.

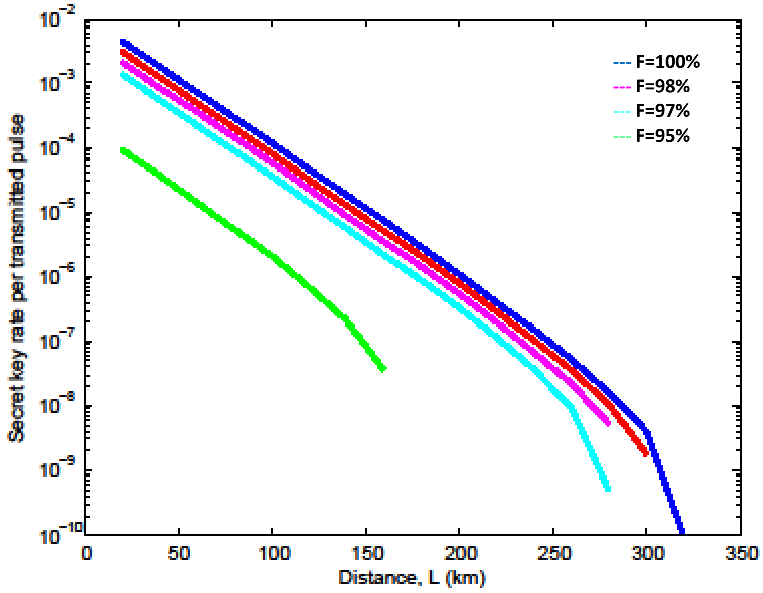


Figure 3.7: Comparison of the Rate-versus-distance for a symmetric setup for different fidelity values.

- Case B

In this case Alice and Bob follow the input states given from Case B in the previous section where Alice sends perfect single photon states whereas Bob sends imperfect single photon states. The Figure 3.8 is for the symmetric setup for different values of fidelity. As in the previous case in Figure 3.7 as the fidelity of the single photon states decreases, the secure distance decreases accordingly. A difference between these two Figures is that the errors contributed in the former case are from both sources being imperfect whereas in the latter case there is only one imperfect source. This means that for the same fidelities (e.g. 95%) the distance reaches longer lengths in the latter case (over 250 km) whereas in the former case it reaches up to roughly 160 km.

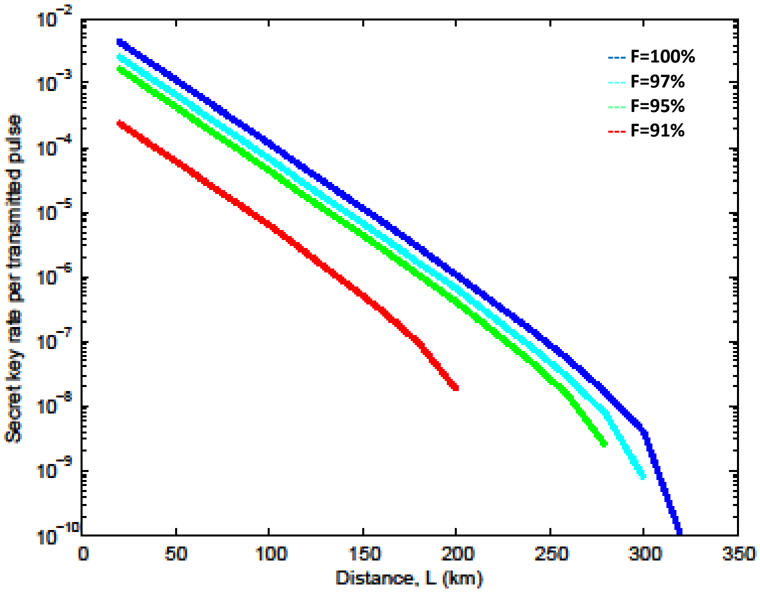


Figure 3.8: Comparison of the key rate versus distance for a symmetric setup for different fidelity values using an imperfect single-photon source and an ideal single-photon source.

In the same scenario where the input states are given as above, we have also made a comparison between an asymmetric and a symmetric setup. Figure 3.9 shows the difference between a symmetric and an asymmetric setup for the same fidelity values. The difference between the symmetric and asymmetric for fidelities 97% and 98% is that the asymmetric has lower key rate for the same distances and also reaches shorter distances (150 km and 170 km respectively) compared to the symmetric counterparts (close to 300 km and 350km respectively).

The difference between the asymmetric and symmetric case is the proximity of the BSM module to the source. The overall scaling of the path loss remains the same for both setups. However in the asymmetric, one of the sources is next to the BSM module, thus the error is given only by one side. This has a negative effect on the asymmetric case giving a higher

QBER and at the same time, lower key rate for the same distances and fidelities as we can see from Figure 3.9.

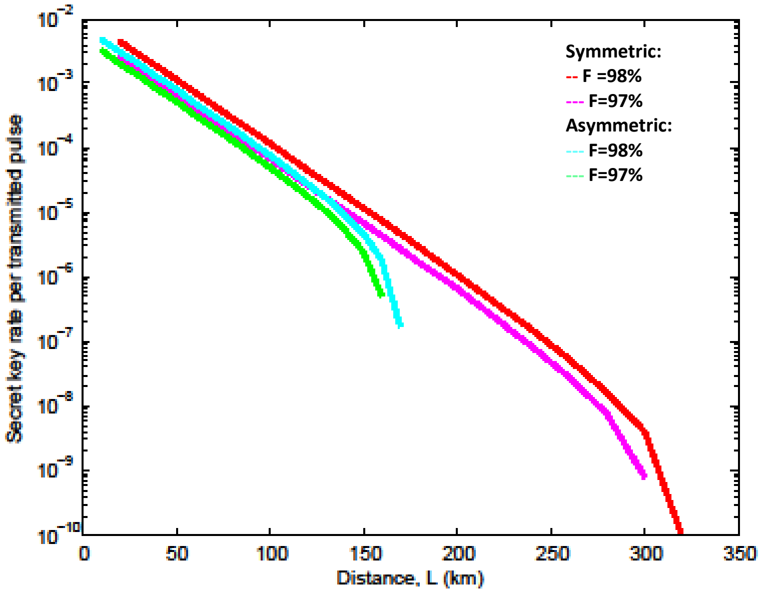


Figure 3.9: Comparison of the key rate versus distance for a symmetric and an asymmetric setup for different fidelity values using an imperfect single-photon source and an ideal single-photon source.

- Case C

  In this case the input states are given as in Section 3.5 where for both Alice and Bob in the Z basis use ideal BB84 encoded single photons, whereas in the X basis their single photons have imperfections during the state-preparation stage. From Figure 3.10 As the fidelity in the X basis decreases, the key rate decreases. The higher the fidelity, the higher the key rate and the longer the secure distance is. For example at $F = 97\%$ the distance reaches up to 300 km whereas for fidelities of 85% the cut-off distance is limited to 240 km. Because in this case, we have mainly X errors we can tolerate rather low fidelities.

3.6 Conclusion

In this Chapter, we studied and analysed the scenario of imperfect single-photon sources in an MDI-QKD protocol in terms of secret key generation rate and QBER with two different types of

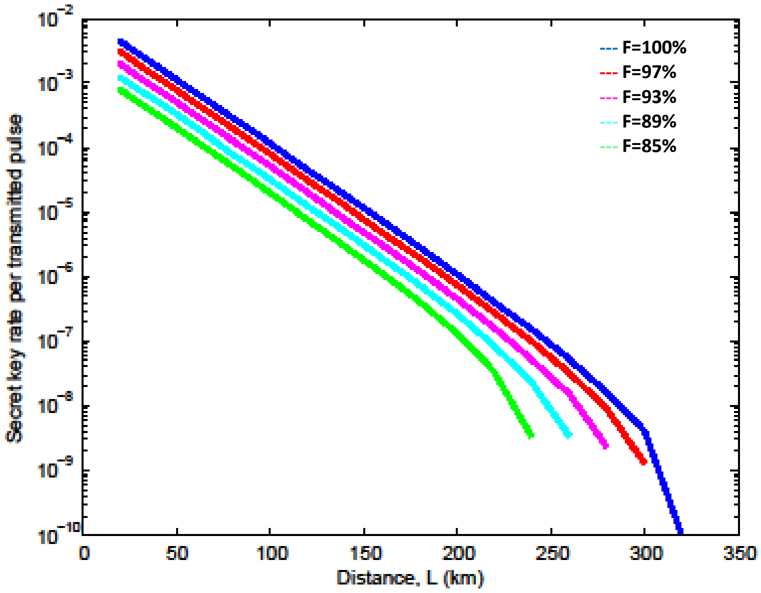


Figure 3.10: Key rate versus distance for different fidelities of the non-diagonal terms in a symmetric setup.

sources and symmetries of the setup.We considered different sources of imperfections such as channel loss, quantum efficiency and dark counts and obtained the optimal regime of operation as a function of system parameters. We first modeled the density matrix for an imperfect single-photon source in order to obtain the secret key rate and the QBER in X and Z bases.

Firstly we compared an imperfect single photon source, which emits a mixture of single photons of different polarisations at the state-preparation stage with different probabilities. We made a comparison for the diagonal terms and found that the higher fidelity they have the lower the QBER is and the higher key rate and longer distances can be achieved. If the fidelity is kept well above 95% we can still retrieve secret key in distances longer than 150 km.

Additionally we compared how the key rate performance changes in the case when one of the users has an ideal single-photon source and the other user has an imperfect single-photon source with the case that both users have imperfect sources. For the same fidelities, we have found that the key rate is higher for longer distances in the former when compared to the latter case.

Finally for an ideal source and an imperfect source, we compared two different symmetry setups for the same input density matrix as above. In the symmetric setup we assume that both users are at an equal distance from the measurement module. In the an asymmetric setup the distance for one user is taken as zero and the other user is at a double the distance from the first case. As their total loss remains equal for both cases, we compare how the symmetry changes when the BSM module is either next to one of the sources or located in the middle of both sources. We have concluded that in the asymmetric case, the QBER is higher as the loss is modeled on one side instead of both as in the symmetric case. This works as a negative effect for the asymmetric setup as the key rate is lower when compared to its counterpart in the symmetric setup for the same distances.

In this chapter we showed that an MDI-QKD protocol is still employable when considering that the source has imperfections at the state-preparation stage. To achieve a more efficient and still feasible implementation we introduce QMs in an MDI-QKD scenario in Chapters 4 and 5 which under certain assumptions we can improve the performance of the MDI-QKD protocol.

Chapter 4

Memory-assisted MDI-QKD

4.1 Introduction

Despite all commercial and experimental achievements in QKD [38, 39, 40, 41, 42], reaching arbitrarily long distances is still a remote objective. The fundamental solution to this problem, i.e., quantum repeaters, is known for over a decade. From early proposals by Briegel *et al.* [43] to the latest no-memory version by Munro *et al.* [44], quantum repeaters, typically, rely on highly efficient quantum gates comparable to what we may need for future quantum computers. While the progress on that ground may take some time before such systems become functional, another approach based on *probabilistic* gate operations was proposed by Duan and coworkers [45], which could offer a simpler way of implementing quantum repeaters for moderate distances of up to around 1000 km. The latter systems require quantum memory modules with high coupling efficiencies to light *and* with coherence times exceeding the transmission delays, which are yet to be achieved together. In this chapter, we propose a protocol that, although is not as scalable as quantum repeaters, for certain classes of memories, relaxes, to some extent, the harsh requirements on memories' coherence times, thereby paving the way for the existing technologies to beat the highest distance records achieved for no-memory QKD links [38]. The idea behind our protocol was presented in [46], and, recently, and, independently, has also been used in [47]. This work proposes additional practical schemes and rigorously analyzes them under realistic conditions.

Our protocol relies on concepts from quantum repeaters, on the one hand, and the recently proposed measurement-device-independent QKD (MDI-QKD), on the other. The original MDI-QKD [4] relies on sending encoded photons by the users to a middle site at which a Bell-state measurement (BSM) is performed. This BSM can be done by an untrusted party, e.g., the service provider, which makes MDI-QKD resilient to detector attacks, e.g., time-shift, remapping, and blinding attacks [25, 26, 27, 28, 29, 30]. The security is then guaranteed by the reverse EPR protocol [33]. In our scheme, by using two quantum memories at the middle site, we first store the state of the transmitted photons in the memories, and perform the required BSM, only when both memories are loaded. This way, similar to quantum repeaters, we achieve a rate-versus-distance improvement as compared to the MDI-QKD schemes proposed in [4, 48], or other conventional QKD systems that do not use quantum memories.

There is an important distinction between our protocol and a conventional quantum repeater system. In a typical quantum repeater link, which relies on initial entanglement distribution among neighboring nodes, the repeat period for the protocol is mainly dictated by the transmission delay for the shortest segment of the repeater system [49, 50]. In our scheme, however, the repeat period is constrained by the writing time, including the time needed for the herald/verification process, into memories. This implies that using sufficiently fast memories, one can run our scheme at a faster rate than that of a quantum repeater, thereby achieving higher key generation rates, as compared to conventional QKD links, and at lower coherence times, as compared to probabilistic repeater systems. This increase in clock rate is what our proposal shares with the recently proposed third generation of quantum repeaters, which use quantum error correction codes to compensate for loss and errors, thus also being able to speed up the clock rate to local processing times [44]. The need for long coherence times remains one of the key challenges in implementing the first generations of quantum repeaters before the latest no-memory quantum repeater proposals can be implemented.

The above two benefits would offer a midterm solution to the problem of long-distance QKD. While our scheme is not scalable the same way that quantum repeaters are, it possibly allows us to use the existing technology for quantum memories to improve the performance of QKD systems. In the absence of fully operational quantum repeater systems, our setup can fill the gap between theory and practice and will become one of the first applications of realistic quantum memories in quantum communications.

4.2 This chapter's contibution

- We analyze the memory-assisted MDI-QKD in a realistic scenario. We consider two different sources. Single-photon sources and the decoy states. In the first case, we use BB84 single photon states and in the second, we use phase-randomized coherent states. In each case we find the secret key generation rate versus distance.

- We analyse the storage time of imperfect QMs and how it affects system performance. We show that these QMs have lower coherence time requirements compared to the multi-memory probabilistic quantum repeaters. Additionally we prove that our proposed protocol can outperform the conventional QKD schemes in terms of rate-versus-distance and has the advantage of being practically constructed with the means of existing technology for QMs.

- We also consider the case of imperfect ensemble based QMs in the memory-assisted MDI-QKD. The ensemble based QMs suffer from multiple excitations thus leading to a lower performance than conventional no-memory systems in practical regimes of interest.

The rest of the Chapter is structured as follows. In Section 4.3, we describe our proposed schemes and the modeling used for each component therein. Section 4.4.1 presents our key rate analysis, followed by some numerical results in Section 4.5. Section 4.7 concludes the Chapter.

4.3 System description

Our scheme relies on "loading" quantum memories (QMs) with certain, unknown, states of light. This loading process needs to be heralding, that is, by the end of it, we should learn about its success. Within our scheme, two types of memories can be employed, which we refer to by *directly* versus *indirectly* heralding QMs. Some QMs can operate in both ways, while some others are more apt to one than the other. By directly heralding memories we refer to the class of memories to which we can directly transfer the state of a photon *and* we can verify—without revealing or demolishing the quantum state—whether this writing process has been successful. An example of such memories is a trapped atom in an optical cavity [65]. In the case of indirectly heralding memories, a direct writing-verification scheme may not exist. Instead, we assume that we can entangle a photonic state with the state of such QMs [45, 66, 67], and later, by doing a measurement on the photon, we can effectively achieve a heralded writing into the memory. These two approaches of writing cover most relevant practical examples to our scheme.

The scheme for directly heralding memories works as follows [46, 47]; see Figure 2.5(a). The two communicating parties, Alice and Bob, send BB84 encoded pulses [1], by either single-photon or weak laser sources, towards QM units located in the middle of the link. Each QM stores a photon in a possibly probabilistic, but *heralding*, way. Once both memories are loaded, we retrieve their states and perform a BSM on the corresponding photons. A successful BSM indicates some form of correlation between the transmitted bits by Alice and Bob.

We can easily extend the above idea to the case of indirectly heralding memories. An additional BSM, on each side, along with an entangling process between photons and QMs, can replace the verification process needed for directly heralding memories. In this case, see Figure 2.5(b), a successful BSM between the transmitted photon by the users and the one entangled with the QM, would effectively herald a successful loading process, that is, the state of the QM is correlated with the quantum state sent by the users.

Here, for simplicity, we work with polarization entanglement. Suppose once we entangle the memory A with a single photon P, the joint state of the two is given by

$$\frac{1}{\sqrt{2}}[|s_H\rangle_A|H\rangle_P + |s_V\rangle_A|V\rangle_P], \tag{4.1}$$

where $|H\rangle_P$ and $|V\rangle_P$, respectively, represent horizontally and vertically polarized single photons, and $|s_H\rangle_A$ and $|s_V\rangle_A$ are the corresponding memory states. By tracing out the memory system A in Equation (4.1), one can see that the photonic state out of the memory is similar to that of a BB84 encoder. Each leg of Figure 2.5(b), from the source to the respective QM, is then similar to an asymmetric setup of the original MDI-QKD scheme as depicted in Figure 2.5(c). The working of the system in Figure 2.5(b) will then follow that of the original MDI-QKD. We will use this similarity in our analysis of the system in Figure 2.5(b).

The main advantage of our scheme as compared to the original MDI-QKD, in Figure 2.5(c), is its higher resilience to channel loss and dark count. In the no-memory MDI-QKD, both pulses, sent by Alice and Bob, should survive the path loss before a BSM can be performed. The key generation rate then scales with the loss in the entire channel. In our scheme, each pulse still needs to survive the path loss over half of the link, but this can happen in different rounds for the signal sent by Alice as compared to that of Bob. We therefore achieve the quantum repeater benefit in that the key generation rate, in the symmetric case, scales with the loss over half of the total distance. Moreover, in the case of directly heralding memories, our scheme is almost immune against dark counts [47]. This is because the measurement efficiency in the BSM module is typically a few orders of magnitude higher than that of dark count rates. Dark counts will then only sightly add to the error rate. In our scheme, memory decoherence errors play a major role as we will explain in this and the following sections.

In the following, we describe the protocol and its components in more detail.

4.3.1 Protocol

In our protocol, Alice and Bob, at a rate R_S, send BB84 encoded pulses to the middle station (dashed box in Figure 2.5). At the QMs, for each incoming pulse, we either apply a loading process by which we can store the state of the photons into memories and verify it, or use the indirectly heralding scheme of Figure 2.5(b). Once successful for a particular QM, we stop the loading procedure on that QM, and wait until both memories are loaded, at which point, a BSM is performed on the QMs. The BSM results are sent back to Alice and Bob, and the above procedure is being repeated until a sufficient number of raw key bits is obtained. The rest of the protocol is the same as that of MDI-QKD. Sifting and postprocessing will be performed on the raw key to obtain a secret key. In this chapter, we neglect the finite-size-key effects in our analysis [62].

4.3.2 Component modeling

In this section, we model each component of Figure 2.5 including sources and encoders, the channel, QMs, and the BSM module.

4.3.2.1 Sources and encoders

We consider two types of sources: ideal single-photon sources and phase-randomized weak laser pulses. The latter will be used in the decoy-state [56] version of the protocol. Each source, at both Alice's and Bob's sides, generates pulses at a rate R_S. Each pulse is polarization encoded in either the rectilinear (Z) or diagonal (X) basis. Here, we use the efficient version of BB84 encoding, where the Z basis is used much more frequenctly than the other basis [57]. The pulse duration is denoted by τ_p and it is chosen in accordance with the requirements of the memory system in use.

4.3.2.2 Channels

The distance between Alice (Bob) and the respective QM is denoted by L_A (L_B). The total distance between Alice and Bob is denoted by $L = L_A + L_B$. The transmission coefficient for a channel with length l is given by

$$\eta_{\text{ch}}(l) \equiv \exp(-l/L_{\text{att}}), \tag{4.2}$$

where L_{att} is the attenuation length of the channel (roughly, 22 km for 0.2 dB/km of loss).

The channel is considered to have a background rate of γ_{BG} per polarization mode, which results in an average $p_{\text{BG}} = 2\gamma_{\text{BG}}\tau_p$ background photons per pulse. This can stem from stray light or crosstalk from other channels, especially if classical signals are multiplexed with quantum ones in a network setup [42, 41, 68, 69, 70].

We also consider setup misalignment in our analysis. We assume certain polarization maintenance schemes are in place for the Alice's and Bob's channels, so that the reference frames at the sources and memories are, on average, the same. We, nevertheless, consider a setup misalignment error probability e_{dK}, for $K = A, B$, to represent misalignment errors in each channel.

4.3.2.3 Quantum memories

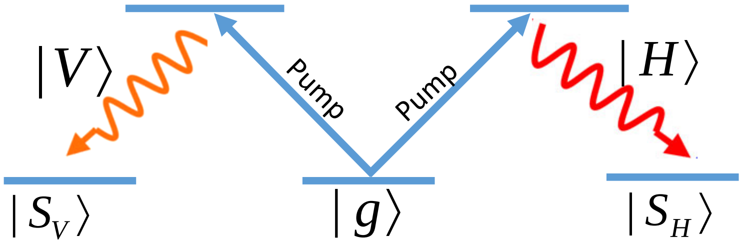


Figure 4.1: One possible energy-level configuration for a QM suitable for polarization encoding.

We use the following assumptions and terminologies for the employed QMs. This list covers most relevant parameters in an experimental setup, whether the QM is operated in the directly or indirectly heralding mode.

- In the case of a successful loading, each QM in Figure 4.1 ideally stores a polarization *qubit* corresponding to the polarization of the incoming pulse. We assume that this is the case even if at the input of the QM there is a non-qubit state, e.g., a coherent state. One suitable energy level structure for such a memory is the double-Λ configuration, with a common ground state and two other metastable states corresponding to two orthogonal polarizations. The excited states can then facilitate Raman transitions from the ground state to each of the metastable states, using known optical transition techniques [71, 72], in response to the input polarization state.

We assume that each QM only stores one spatio-temporal mode of light. Our protocol can be extended to incorporate multimode QMs [73] or multiple QMs [49], in which case a linear improvement in the rate is expected. In this work, we focus on the case of a single logical memory per user and leave extensions to future work.

- For directly heralding memories, we denote the QM's writing efficiency by η_w. The writing efficiency is the probability to store a qubit and herald success conditioned on having a single-photon at the QM's input. Note that η_w also includes the chance of failure for our verification process. For indirectly heralding memories, we introduce an entangling efficiency, η_{ent}, which is the probability of success for entangling a photon with our QM.
- We denote the QM's reading efficiency by η_r. That is the probability to retrieve a single photon out of the QM conditioned on a successful loading in the past. The reading efficiency is expected to decay over a time period t as $\eta_r(t) = \eta_{r0} \exp[-t/T_1]$, where T_1 is the memory amplitude decay time and η_{r0} is the reading efficiency right after loading. In our example of a double-Λ-level memory, such a decay corresponds to the transition form one of the metastable states to the ground state, in which case, no photon will be retrieved from the memory.
- We denote the QM's writing time by τ_w. For directly heralding memories, it is the time difference between the time that a pulse arrives (beginning of the pulse) at the QM and the time that a successful/unsuccessful loading is declared. This is practically the fastest repeat period one can run our protocol. In the case of indirectly heralding memories, τ_w includes the time for the entangling process as well as that of the side BSM operation. Accounting for such timing parameters is essential in enabling us to have a fair comparison between memory-assisted and no-memory QKD systems.
- We denote the QM's reading time by τ_r. It is the time difference between the time that the retrieval process is applied until a pulse (end of the pulse) is out.
- We denote the QM's coherence (dephazing) time by T_2. For an initial state $\rho(0)$ of the QM at time zero, its state at a later time t is given by [49]

$$\rho(t) = p(t)\rho(0) + [1 - p(t)]Z\rho(0)Z, \tag{4.3}$$

where $p(t) = [1 + \exp(-t/T_2)]/2$. Note that dephazing would only occur if we are in a superposition of Z eigenstates, e.g., the eigenstates of X. The above model better captures the decoherence effect in most practical cases of interest than the model used in [47], in which the memory state switches suddenly from an intact one to a fully randomized version after a certain time. We discuss the implications of each model in our numerical result section.

4.3.2.4 BSM module

Figure 3.3 shows the schematic of the BSM module used in our analysis. This module enables an incomplete BSM over photonic states. In order to use this module, in our scheme, we first need to read out the QMs and convert their qubit states into polarization-encoded photons. The BSM will then be successful if exactly two detectors click, one H-labeled and one V-labeled. Depending on which detectors have clicked and what basis is in use, Alice and Bob can identify what bits they ideally share [48].

We assume the BSM module is symmetric. We lump detector quantum efficiencies with other possible sources of loss in the BSM module and denote it by η_d for each detector. We also assume that each detector has a dark count rate of γ_{dc}, which results in a probability $p_{\text{dc}} = \gamma_{\text{dc}}\tau_p$ of having a dark count per pulse. The implicit assumption here is that the retrieved and the writing photons have the same pulse width. Finally, we assume that there is no additional misalignment error in the BSM module.

4.4 Key rate Analysis

In this section, we find the secret key generation rate for our proposed schemes in Figures 2.5(a) and 2.5(b). We later compare it with two conventional QKD schemes, namely, BB84, summarized in Appendix A, and the original MDI-QKD in Figure 2.5(c), summarized in Appendix B, that use no memories. In all cases, we consider both single-photon and decoy-state sources. In all forthcoming sections, f denotes the inefficiency of the error correction scheme, i.e., the ratio between the actual cost of error correction and its minimum value obtained by the Shannon's theorem, assumed to be constant, and we denote the binary entropy function as $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$, for $0 \leq p \leq 1$.

4.4.1 Key rate for single-photon sources

With ideal single-photon sources, the secret key generation rate in the setups of Figures 2.5(a) and 2.5(b) is lower bounded by [52]

$$R_{\mathrm{QM}} = R_S Y_{11}^{\mathrm{QM}}[1 - h(e_{11;X}^{\mathrm{QM}}) - fh(e_{11;Z}^{\mathrm{QM}})], \tag{4.4}$$

where efficient BB84 encoding is employed [57]. In the above equation, $e_{11;X}^{\mathrm{QM}}$ and $e_{11;Z}^{\mathrm{QM}}$, respectively, represent the quantum bit error rate (QBER) between Alice and Bob in the X and Z basis, when single photons are used, and Y_{11}^{QM} represents the rate at which both memories are loaded with single photons of the same basis *and* the middle BSM is successful.

To obtain the individual terms in Equation (4.4), we can decompose the protocol into two parts: the memory loading step and the measurement step, once both memories are loaded. The first step is a probabilistic problem with two geometric random variables, N_A and N_B, corresponding, respectively, to the number of attempts until we load Alice and Bob's memories with single photons. The number of rounds that it takes to load both memories is then $\max\{N_A, N_B\}$. Once both memories are loaded, the rest of the protocol is similar to that of original MDI-QKD in terms of rate analysis: the QMs replace the sources in Figure 2.5(c) and the total transmission-detection efficiency is replaced by the reading-measurement efficiency in the BSM module. We can therefore use many of the relationships obtained for the original MDI-QKD, summarized in Section 2.6.1, for the memory-assisted versions of Figure 2.5.

For finite values of T_1, the reading efficiency for Alice's QM could be different from that of Bob. In fact, we can assume that, once both memories are loaded, one of the memories (late) will be read immediately, while the other (early) $|N_A - N_B|$ rounds after its successful loading. The effective measurement efficiency for the leg K, $K = A, B$, corresponding to the path originating from memory K in the BSM module will then be given by

$$\eta_{mK} = \begin{cases} \eta_m \equiv \eta_{r0}\eta_d, & \text{if memory } K \text{ is late} \\ \eta_d\, \eta_r(t = |N_A - N_B|T), & \text{if memory } K \text{ is early} \end{cases} . \tag{4.5}$$

With the above setting, and considering the required time for reading from the QMs, we obtain

$$\begin{aligned} Y_{11}^{\mathrm{QM}} &= \frac{1}{N_L(\eta_{1A}, \eta_{1B}) + N_r} \mathrm{E}\{Y_{11}(\eta_{mA}, \eta_{mB})\} \\ &= \frac{1}{N_L(\eta_{1A}, \eta_{1B}) + N_r} Y_{11}(\eta_m, \eta_m'), \end{aligned} \tag{4.6}$$

where Y_{11} is the corresponding yield term, given by Equation (2.22), for the MDI-QKD protocol and $N_L = \mathrm{E}\{\max(N_A, N_B)\}$ is given by Equation (A.3). Here, $\mathrm{E}\{\cdot\}$ represents the expectation value operator with respect to N_A and N_B, and $\eta'_m = \eta_d \overline{\eta_r}$, where $\overline{\eta_r} = \eta_{r0}\mathrm{E}\{\exp(-|N_A - N_B|T/T_1)\}$ can be obtained from Equation (A.4). In Equation (4.6), N_r, represents the extra rounds lost due to the nonzero reading times of QMs, once they are both loaded, and is given by

$$N_r = \left\lceil \frac{\tau_r + \tau_w}{T} \right\rceil - 1, \quad \tau_r, \tau_w > 0, \quad \tau_w \le T, \tag{4.7}$$

where $T = 1/R_S$ is the repetition period. The condition $\tau_w \le T$ is a matter of practicality as sending photons faster than they can be stored is of no benefit. The fastest possible rate is then obtained at $T = \tau_w$.

In the case of directly heralding memories of Figure (2.5a), we have

$$\eta_{1K} = 1 - (1 - \eta_w \eta_{\mathrm{ch}}(L_K))e^{-\eta_w p_{\mathrm{BG}}}, \quad K = A, B, \tag{4.8}$$

as the probabilities of successful loading of Alice and Bob's QMs with single-photon sources (or background noise). In the case of indirectly heralding memories of Figure (2.5b), following our discussion in Section (4.3) about the equivalence of each leg of Figure (2.5b) to an asymmetric MDI-QKD system, we have

$$\eta_{1K} = Y_{11}(\eta_d \eta_{\mathrm{ch}}(L_K), \eta_d \eta_{\mathrm{ent}}), \quad K = A, B, \tag{4.9}$$

where the above terms must be calculated at an effective dark count rate of $\gamma_{\mathrm{dc}} + \gamma_{\mathrm{BG}}\eta_d/2$.

We remark that, although obtained from different methods, the analysis in [47] also finds similar expressions for the yield term. In [47], the analysis is only concerned with the symmetric setup, and some of the parameters considered in our work take their ideal values. It can be verified, however, that in the special case of $\tau_w = T$, $\tau_r = 0$, $\gamma_{\mathrm{BG}} = 0$, $L_A = L_B$, $\eta_w = 1$, and $T_1 \to \infty$, for directly heralding memories, Equation (4.6) reduces to the same result obtained in [47]. By accounting for additional relevant parameters, our analysis offers a better match to realistic experimental scenarios.

Similarly, the error terms are given by

$$\begin{aligned}
e_{11;Z}^{\mathrm{QM}} &= \mathrm{E}\{e_{11;Z}(\eta_{mA},\eta_{mB},e_{dZ}^{\mathrm{QM}}(\eta_{1A},\eta_{1B}))\} \\
&= e_{11;Z}(\eta_m,\eta_m',e_{dZ}^{\mathrm{QM}}(\eta_{1A},\eta_{1B})), \\
e_{11;X}^{\mathrm{QM}} &= \mathrm{E}\{e_{11;X}(\eta_{mA},\eta_{mB},e_{dX}^{\mathrm{QM}}(\eta_{1A},\eta_{1B}))\} \\
&\approx e_{11;X}(\eta_m,\eta_m',\mathrm{E}\{e_{dX}^{\mathrm{QM}}(\eta_{1A},\eta_{1B})\}), \qquad (4.10)
\end{aligned}$$

where, $e_{11;Z}$ and $e_{11;X}$, given by Equation (2.22), are the corresponding error terms for the original MDI-QKD. In addition to the typical sources of error, such as loss and dark count, the above expressions are functions of misalignment parameters. This misalignment could be a statistical error in the polarization stability of our setup, modeled by e_{dA} and e_{dB}, or an effective misalignment because of memory dephazing [74] and/or background photons. Putting all these effects together, as we have done in B, we obtain

$$\begin{aligned}
e_{dS}^{\mathrm{QM}}(\eta_A,\eta_B) &= e_{dS}^{(A)}(\eta_A,\eta_B)(1-e_{dS}^{(B)}(\eta_A,\eta_B)) \\
&+ e_{dS}^{(B)}(\eta_A,\eta_B)(1-e_{dS}^{(A)}(\eta_A,\eta_B)), \quad S=X,Z, \qquad (4.11)
\end{aligned}$$

where $e_{dS}^{(A)}$ and $e_{dS}^{(B)}$, respectively, represent the misalignment probabilities for Alice's and Bob's memories, for basis $S=\{X,Z\}$, at loading probabilities η_A and η_B and are given by Equations (B.2) and (B.5). The above Equation accounts for the fact that if the state of both memories are flipped, Alice and Bob will still share identical key bits. We assume that the BSM module is balanced and does not have any setup misalignment.

Note that in Equation (4.11), because of no dephazing errors for the Z eigenstates, e_{dZ}^{QM} is independent of N_A and N_B, whereas e_{dX}^{QM} is a function of them. The approximation in Equation (4.10) assumes $\mathrm{E}\{e_{dX}^{\mathrm{QM}}\eta_{mA}\eta_{mB}\} \approx \mathrm{E}\{e_{dX}^{\mathrm{QM}}\}\mathrm{E}\{\eta_{mA}\eta_{mB}\}$, which is valid when $T_1 \gg T_2$, to give a more readable final result.

Equation (4.11) can also be used in the case of indirectly heralding QMs as explained in Appendix B. The main idea is to use the analogy of each leg in Figure 2.5(b) with the original MDI-QKD in Figure 2.5(c).

4.4.2 Key rate for decoy states

Suppose Alice and Bob use a decoy-state scheme with average photon numbers μ and ν, respectively, for the two main signal intensities, and infinitely many auxiliary decoy states. The secret key generation rate, in the limit of infinitely long key, is then given by

$$R_{\text{QM}} = R_S[Q_{11}^{\text{QM}}(1 - h(e_{11;X}^{\text{QM}})) - fQ_{\mu\nu;Z}^{\text{QM}}h(E_{\mu\nu;Z}^{\text{QM}})], \tag{4.12}$$

where

$$Q_{\mu\nu;Z}^{\text{QM}} = \frac{1}{N_L(\eta_{\mu A}, \eta_{\nu B}) + N_r} Y_{11}(\eta_m, \eta_m') \tag{4.13}$$

is the rate at which both memories are loaded, by Alice (Bob) sending a coherent state in the Z basis with μ (ν) average number of photons, and a successful BSM is achieved. In the case of directly heralding memories,

$$\eta_{\mu A} = 1 - e^{-\eta_{\text{ch}}(L_A)\eta_w\mu - \eta_w p_{\text{BG}}} \text{ and } \eta_{\mu B} = 1 - e^{-\eta_{\text{ch}}(L_B)\eta_w\nu - \eta_w p_{\text{BG}}} \tag{4.14}$$

are the probabilities for successful loading of Alice and Bob's QMs with coherent-state sources. Similarly,

$$E_{\mu\nu;Z}^{\text{QM}} = e_{11;Z}(\eta_m, \eta_m', e_{dZ}^{\text{QM}}(\eta_{\mu A}, \eta_{\nu B})) \tag{4.15}$$

is the QBER in the Z basis, and

$$Q_{11}^{\text{QM}} = Q_{\mu\nu;Z}^{\text{QM}} \frac{\eta_{1A}\eta_{1B}}{\eta_{\mu A}\eta_{\nu B}} \mu\nu e^{-\mu-\nu} \tag{4.16}$$

is the contribution of single-photon states in the gain term of Equation (4.13).

Similar to the treatment in the previous subsection, one can find or approximate the above terms in the case of indirectly heralding memories as well as analysed in the next Chapter.

Apart from all additional parameters considered in our model as compared to [47], our treatment of the decoy-state QKD is different from that of [47] in the way that QMs are modeled. In our work, we assume QMs store qubits, which while is not necessarily an exact model, it often serves a good first-order approximation to the reality. In [47], however, QMs are assumed to be able to store number states. This assumption seems more restrictive as many QMs, such as single trapped atoms or ions, can only store one photon.

4.4.3 Storage time

To get some insight into the working of our system, in this section, we simulate the achievable rates assuming $L_A = L_B = L/2$. The average number of trials to load both memories from

Equation (A.3) is then given by [75]

$$N_L(\eta,\eta) = \frac{3-2\eta}{\eta(2-\eta)} \approx \frac{3}{2}\cdot\frac{1}{\eta}, \quad \text{for } \eta \ll 1, \tag{4.17}$$

where η is the probability of successfully loading a QM at distance $L/2$, approximately, given by $\eta_{\rm QM}\exp(-(L/2)/L_{\rm att})$, where $\eta_{\rm QM} = \eta_w$ for directly heralding memories, and $\eta_{\rm QM} = \eta_{\rm ent}\eta_d^2$ for indirectly heralding QMs. Similarly, the average required storage time, from Equation (A.5), is given by

$$T_{st} = {\rm E}\{|N_A - N_B|\}T = \frac{2(1-\eta)T}{\eta(2-\eta)} \approx \frac{T}{\eta}, \quad \text{for } \eta \ll 1, \tag{4.18}$$

which is similar to the result reported in [47].

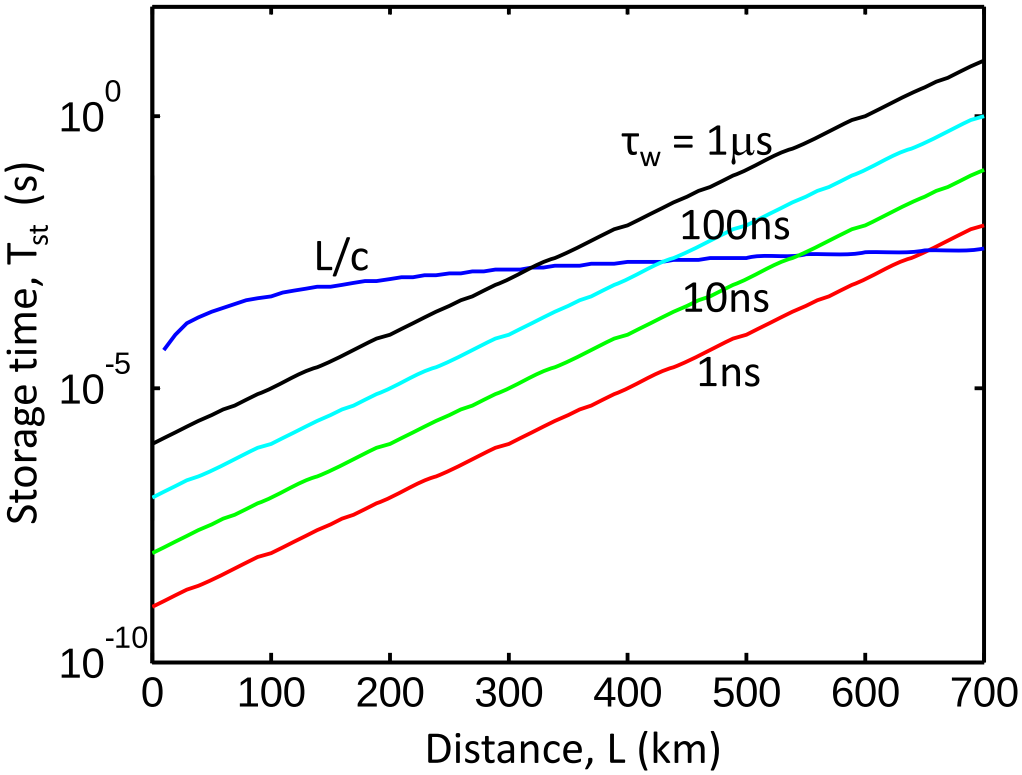


Figure 4.2: Average required storage time, T_{st}, versus distance, in our scheme, for different repetition rates $1/\tau_w$. As compared to that of a probabilistic quantum repeater, labeled by L/c, where $c = 2\times 10^8$ m/s is the speed of light in optical fiber, our scheme requires lower coherence times up to a certain distance. The crossover distance at $\tau_w = 1$ μs is over 300 km and at $\tau_w = 1$ ns is nearly 700 km. In all curves, $\eta_w = \eta_d = \eta_{\rm ent} = 1$ and $p_{\rm BG} = 0$.

The secret key generation rate in Equations (4.4) and (4.12) is proportional to the pulse generation rate $R_S = 1/T$ at the encoder. To maximize R_S, we choose $T = \tau_w$, throughout this section and next, resulting in $T_{st} \approx \tau_w/\eta$. Figure (4.2) compares T_{st} with the required storage time in multi-memory probabilistic quantum repeaters [49], L/c, where c is the speed of light in the channel. It can be seen that our scheme offers lower required coherence times until a certain distance. With fast memories of shorter than 10 ns of access time, this crossover distance could be longer than 500 km. With such memories, the required coherence time at 300 km is roughly 1 μs, or lower, as compared to over 1 ms for probabilistic quantum repeaters.

It is worth mentioning that the possible advantage of requiring low coherence times is only achievable for systems with nesting level one, i.e., with one stage of entanglement swapping. Unlike quantum repeaters, our protocol, in terms of its timing, is not scalable to higher nesting levels. Nevertheless, even with only one entanglement swapping stage, our protocol can outperform conventional QKD schemes in terms of rate-versus-distance behaviour, and, more importantly, this can possibly be achieved with existing technology for quantum memories. We explore this and other aspects of our scheme in the next section.

4.5 Numerical results

In this section, we study the impact of various parameters on the secret key generation rate of our scheme. All results have been obtained assuming the symmetric setup described in Section (4.4.3), $\tau_w = T$, $f = 1.16$, $c = 2 \times 10^8$ m/s, and 0.2 dB/km of loss in the channel. We also compare our scheme with the efficient BB84 and MDI-QKD protocols, whose secret key generation rates are, respectively, summarized in Appendices A and B.

4.5.1 Coherence time

In this section, we discuss the effects of memory dephazing on the secret key generation rate. As mentioned before, while our scheme in Figure 2.5(a) is particularly resilient to dark count errors, it still suffers from memory errors. Figure 4.3 demonstrates the secret key generation rate per pulse at different coherence times for the scheme of Figure 2.5(a). A finite coherence time is the only source of nonideality considered in this Figure. Since, in our model, the dephazing process only affects the diagonal basis, $e_{11;Z}^{\text{QM}} = 0$ at all distances; hence $R_{\text{QM}} \propto 1 - h(e_{11;X}^{\text{QM}})$ remains always positive. The rate is initially proportional to $\exp(-(L/2)/L_{\text{att}})$, and with low values of $e_{11;X}^{\text{QM}}$ for short distances, our scheme beats the BB84 case depicted by the dashed line. Note that, because of the partial BSM in Figure 3.3, the initial key rate at $L = 0$ for our scheme is lower than that of BB84. At large distances, however, the dephazing process becomes significant and results in

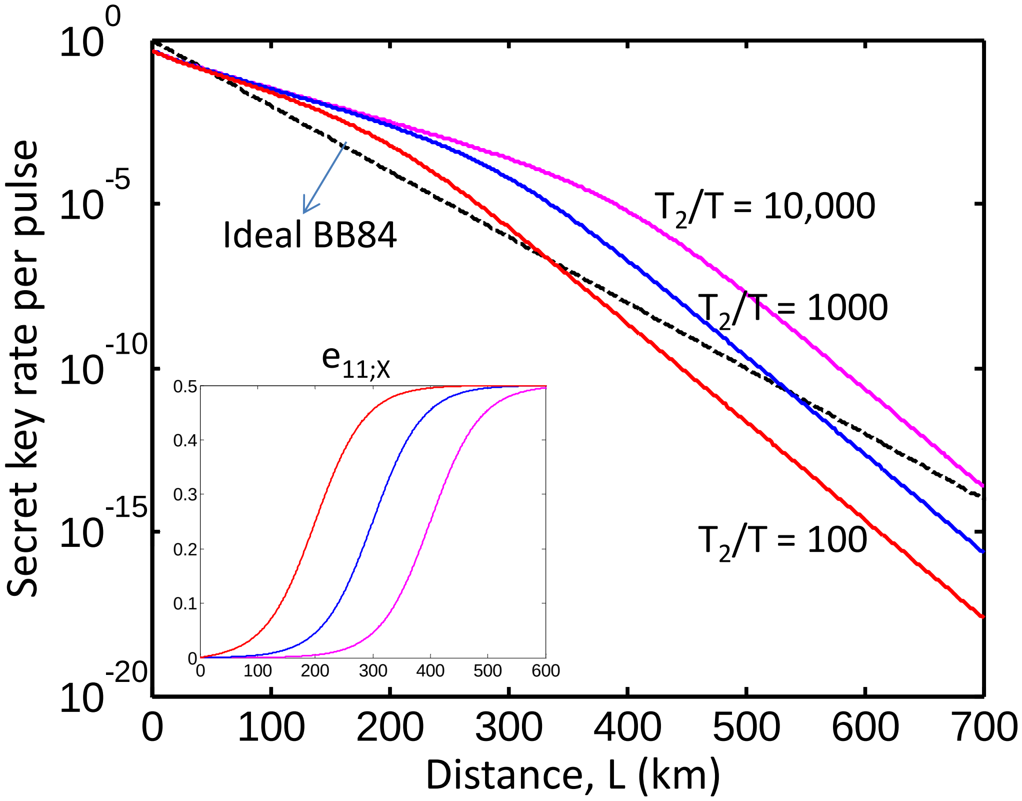


Figure 4.3: Secret key generation rate per pulse for the heralded scheme of Figure 2.5(a) for different values of T_2/T using single-photon sources. The dashed line represents the ideal efficient BB84 case. Unless explicitly mentioned, all other parameters assume their ideal values: $T_1 \to \infty$, $\eta_w = \eta_{r0} = \eta_d = 1$, $\gamma_{\text{BG}} = \gamma_{\text{dc}} = 0$, $e_{dA} = e_{dB} = 0$, and $\tau_r = 0$.

$e_{11;X}^{\text{QM}}$ approaching 1/2; see the inset. Subsequently, R_{QM} decays with a faster slope and at some point becomes lower than what one can achieve with an ideal BB84 system. The window between the two crossing points on each curve is the range where our scheme, can, in principle, beat a noise-free BB84 system. This window is larger for QMs with longer coherence times.

In [47], authors look at the minimum required coherence time to achieve nonzero key rates, assuming $e_{11;X}^{\text{QM}} = e_{11;Z}^{\text{QM}}$ within their model of decoherence. Although the models used for decoherence in our work and [47] are different, $e_{11;X}^{\text{QM}}$ has a similar behaviour in both cases. In our case, however, the transition from 0 to 1/2 is smoother than that of [47]. This is expected as the model in [47] is an abrupt good-bad model for the memory. A consequence of this difference is that the minimum required coherence time is then higher in our case, which highlights the importance of the more accurate model we have used for decoherence.

The comparison in Figure 4.3 assumes that the source rate R_S is the same for both the BB84

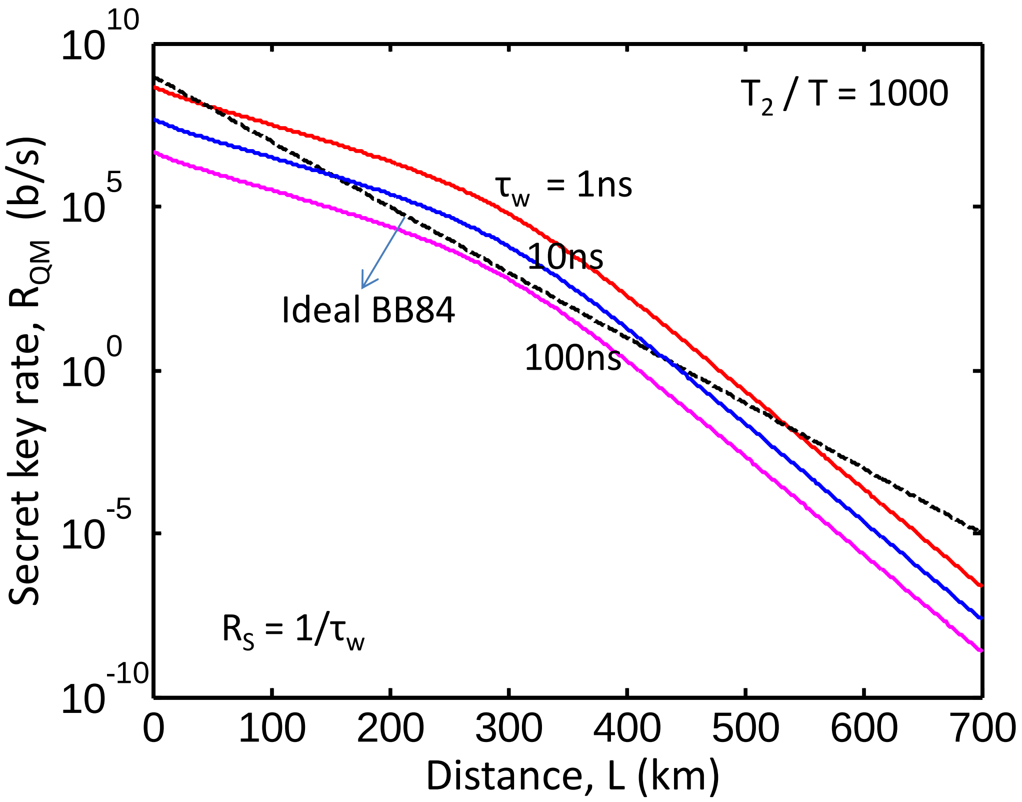


Figure 4.4: Secret key generation rate for different values of τ_w at $T_2/T = 1000$ using single-photon sources. The dashed line represents the ideal efficient BB84 case at $R_S = 1$ Gpulse/s. Unless explicitly mentioned, all other parameters assume their ideal values: $T_1 \to \infty$, $\eta_w = \eta_{r0} = \eta_d = 1$, $\gamma_{\text{BG}} = \gamma_{\text{dc}} = 0$, $e_{dA} = e_{dB} = 0$, and $\tau_r = 0$.

protocol and our scheme. In our scheme, however, R_S depends on the writing time of the memories. Figure 4.4 shows the secret key generation rate for the scheme of Figure 2.5(a) at a fixed value of $T_2/T = 1000$, but for several values of $T = \tau_w = 1/R_S$. The BB84 system is run at a fixed rate of 1 GHz. Again, we assume that the only source of nonideality is memory dephazing. It can be seen that slow memories with writing times of 100 ns, or higher, can hardly compete with an ideal BB84 system. The two orders of magnitude lost because of the lower repetition rate cannot be compensated within the first 300 km. It is still possible to beat the BB84 case, at long distances, if memories have higher coherence times.

4.5.2 Realistic examples

It is interesting to see if any of the existing technologies for quantum devices can be employed in our scheme to beat conventional QKD systems. Figure 4.5 makes such a comparison between

BB84, MDI-QKD, and memory-assisted MDI-QKD for a particular experimental setup. We have chosen our QM based on the two lessons learned from Figures 4.2 and 4.4: the QM needs to have a high bandwidth-storage product (T_2/τ_w) on the order of 1000 or higher, and, it also needs to be fast, with writing times on the order of nanoseconds. Both these criteria are met for the QM used in [5], which particularly offers fast reading and writing with 300-ps-long pulses at a storage time of around 4 μs. The employed memory in this experiment is an atomic ensemble, which fits our indirectly heralding scheme of Figure 2.5(b). We assume that, by driving this ensemble with short pulses, one can ideally generate the jointly entangled state in Equation (4.1) between the ensemble and a photon [76], where, in this case, $|s_H\rangle$ and $|s_V\rangle$ are, respectively, the corresponding symmetric collective excited states to horizontal and vertical polarizations [45, 77]. By keeping the entangling efficiency low at $\eta_{\text{ent}} = 0.05$, here, we neglect the effect of multiple excitations in such memories [66, 78, 74]. We also assume that $T_2 = T_1$ and use the state-of-the-art single-photon detectors with $\eta_d = 0.93$ at $\gamma_{\text{dc}} = 1$ count per second and 150 ps of time resolution [79] for all systems.

We consider two sets of parameter values for our employed QM in Figure 4.5. In the first set, corresponding to the curve labeled A on the Figure, we use the same numerical values as reported in [5], that is, $\eta_{r0} = 0.3$, $T_1 = 4$ μs, and $\tau_w = \tau_r = \tau_p = 300$ ps. We, however, assume that $R_S = 1/\tau_w$, which is much faster than the repetition rate used in [5]. In the curve labeled B, we improve the performance by assuming $\eta_{r0} = 0.73$, which is what another group has obtained for a similar type of memory [76], and $T_1 = T_2 = 100$ μs, which is attainable by improving magnetic shielding [80]. It can be seen that, whereas the current QM employed in [5] is short of beating either of no-memory systems, our slightly boosted system, in curve B, outperforms both systems at over roughly 200 km. The cut-off distance in curve B is about 400 km, which is mainly because of memory decoherence, and it can be improved by using memories with longer coherence times. This implies that with slightly improving some experimental parameters, we would be able to employ realistic QMs to improve the performance of practical quantum communication setups. We remark that the example QM chosen in Figure 4.5 is not necessarily the only option, and improved versions of other types of memories can potentially offer the same performance [67, 81, 82, 83].

4.6 MDI-QKD with ensemble-based memories

In the memory-assisted MDI-QKD we achieve an improvement on rate-versus-distance over the no-memory MDI-QKD systems. However in order to beat the no-memory QKD systems,

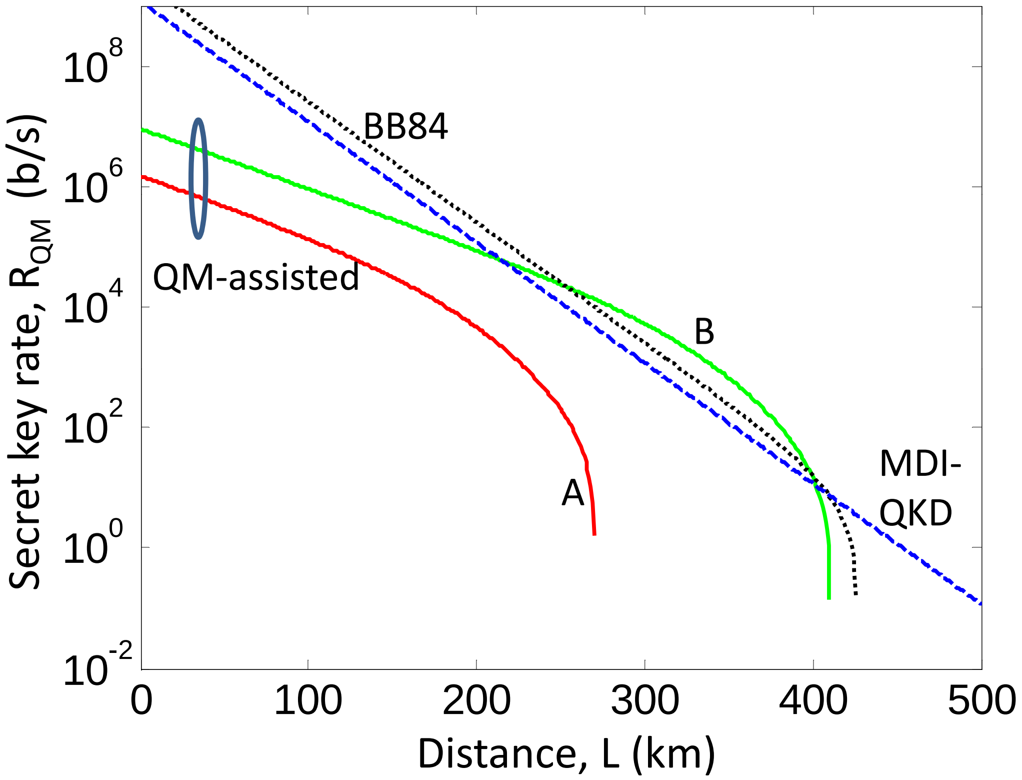


Figure 4.5: Secret key generation rate for single-photon BB84 (dotted), MDI-QKD (dashed), and our indirectly heralding scheme of Figure 2.5(b) (solid) at practical parameter values. In all curves, $\eta_d = 0.93$, $\gamma_{\text{dc}} = 1$/s, $\gamma_{\text{BG}} = 0$, and $e_{dA} = e_{dB} = 0.005$. For BB84 and MDI-QKD, $R_S = 3.3$ G pulse/s, similar to $R_S = 1/\tau_w$, in our scheme. For our scheme, we have used the experimental parameters reported in [5]. For the curve labeled A, $\eta_{\text{ent}} = 0.05$, $\eta_{r0} = 0.3$, $T_1 = T_2 = 4$ μs, and $\tau_w = \tau_r = \tau_p = 300$ ps. For the curve labeled B, everything is the same except that $\eta_{r0} = 0.73$ and $T_1 = T_2 = 100$ μs.

according to our setup described in Figure 2.5(b) must be equipped with QMs that have large storage-bandwidth products as well as short access and entangling times. The state-of-the-art for single-qubit QMs, for instance single atoms [67], or ions [84], is still not at the required level to fullfil the current conditions of practical memory-assisted protocols. More specifically, faster QMs are needed for the practical ranges of interest.

A suitable candidate that meets the requirements of having very large bandwidths, and therefore very short acces times, for a memory-assisted protocol, are the ensemble-based memories. The main drawback of these QMs is that they suffer from multiple-excitation effects, that in turn affect the results of a successful side BSM that may have been resulted from two photons originating from the QM in Figure 2.5(b). This fact leads to the final measurement results to have no

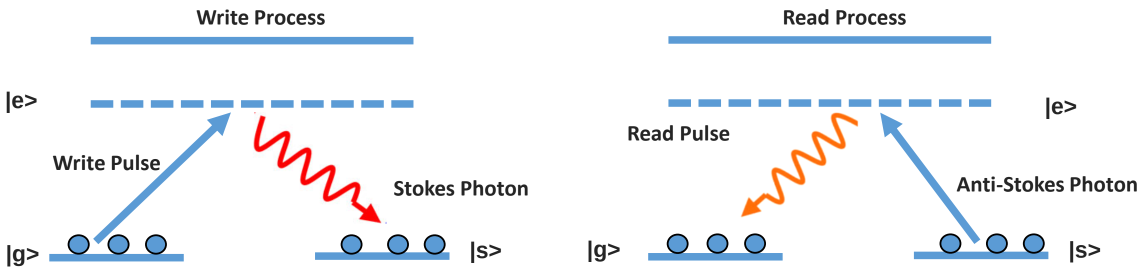


Figure 4.6: Level scheme for the creation of collective excitations in atomi ensembles via spontaneous Raman emission (write process) and for their readout (read process).

correlation with the transmitted signal by the user. The results from this scheme show that such effects can be counterproductive in a way that we cannot beat the no-memory QKD systems within practical ranges of interest. Below there is a brief description of the ensemble-based memory MDI-QKD scheme [6].

Firstly in this setup the ensemble-based memory can be considered as a non-interacting ensemble of quantum systems. The QMs are assumed to be an ensemble of neutral atoms with the Λ configuration as shown in Figure 4.6. One of the possible ways to entangle a photon with a QM is to excite the ensemble by using a short pulse, conditioned that the ensemble was initially in the ground state ($|g\rangle$). This short pulse should have a probability p of driving an off-resonant Raman transition in the ensemble kept much lower than one. The joint state of the released Raman optical field and the ensemble is similar to the two-mode squeezed state given by [85]

$$|\Psi\rangle_{AP} = \sum_{n=0}^{\#ofatoms} \sqrt{(1-p)p^n |n\rangle_A |n\rangle_P}, \tag{4.19}$$

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

$$\rho_P(p) = (1-p)|1\rangle_P\langle 1| + p|2\rangle_P\langle 2|, \tag{4.20}$$

which denotes an imperfect single-photon source with a nonzero probability p of emitting two photons. According to Figure 2.5(b) this is the expected type of state that one would get for the

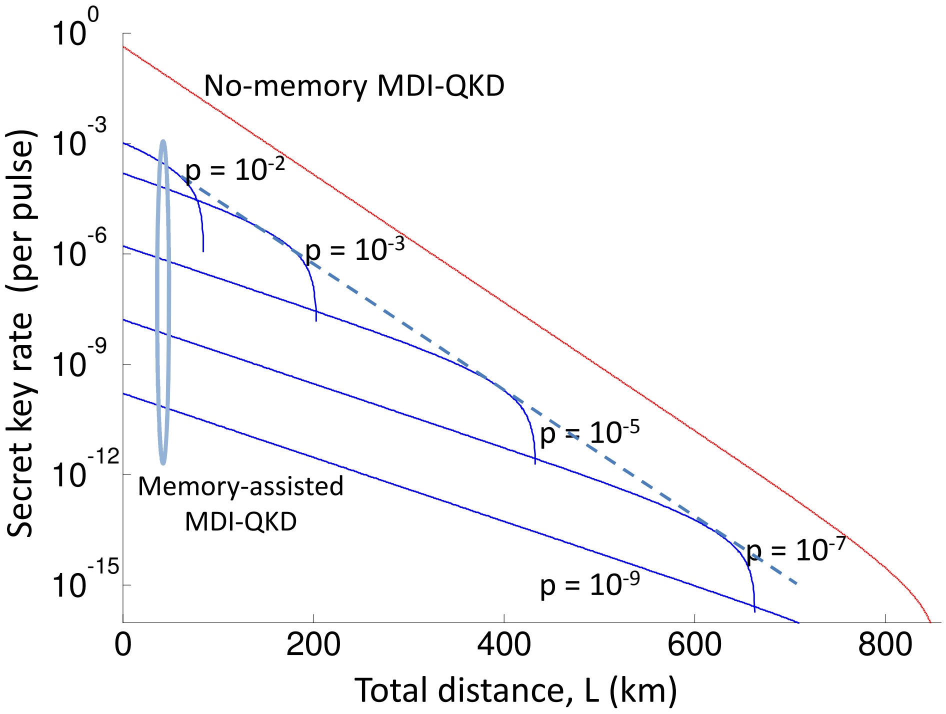


Figure 4.7: Secret key generation rate per transmitted pulse versus distance for the MDI-QKD and without memories for different values of the excitation probability p [6].

photons entangled with the QMs. To be specific the states here represented are not maximally entangled.

This setup is based on the description from Figure 2.5(b) with the difference that the single-qubit QMs are now replaced by ensemble based QMs. Alice and Bob are using perfect single-photon sources. The analysis for the key rate is similar to the one given by Equation (4.4) where the terms Y_{11}^{QM}, $e_{11;X}^{\mathrm{QM}}$ and $e_{11;Z}^{\mathrm{QM}}$ change according to the ensemble based QMs parameters. The difference with the single-qubit QMs is that in the ensemble based QMs, due to the multiple excitation effect, we may have stored more than one excitation overall, even if only one perfect single photon was sent from each user.

The effects of the multiple excitations are shown in Figure 4.7 where there is a comparison of the secret key generation rate versus distance for different probabilities p against the no-memory setup [6]. There was no decay or misalignment in the setup and the dark count has very low probability. In Figure 4.7, the memory-assisted setup cannot outperform the no-memory system for a reasonable range of rates and/or distances. As the values of p decreases, so does the probability for entangling a photon with the memories. This is the reason that the initial key generation rate drops. However, for lower values of p the generation of multiple-excitation are much lower, therefore the cut-off security distance becomes longer. It, however, never reaches the security distance of a no-QM system. In the following chapter, we propose a solution to this problem, which can go around the multiple-excitation effect in ensemble-based memories.

4.7 Conclusions

In this Chapter, we analysed our proposed protocol, memory-assisted MDI-QKD, using perfect single-photon sources and decoy states in order to find the secret key generation rate. Additionally we have analysed the QMs in terms of coherence times and compared the secret key rate of the memory-assisted MDI-QKD with conventional QKD systems for different coherence times. We found that for QMs with long coherence times could beat a noise-free BB84 system. Additionally we considered QMs with different writing times and thus different access times, which essentially affects the secret key rate. When we compared the memory-assisted MDI-QKD with the no-memory QKD systems, we found that for writing times lower than 100 ns would be required if the memories also have high coherence times ($T_2/T > 1000$).

By combining ideas from quantum repeaters and MDI-QKD, we proposed a QKD scheme that relied on quantum memories. While offering the same rate-versus-distance improvement that quantum repeaters promise, the coherence-time requirements for the quantum memories employed in our scheme could be less stringent than that of a general probabilistic quantum repeater system. That would provide a window of opportunity for building realistic QKD systems that beat conventional no-memory QKD schemes by only relying on existing technologies for quantum memories. In our work, we showed that how close some experimental setups would be in achieving this objective. Our protocol acts as a middle step on the roadmap to long-distance quantum communication systems.

Moreover, since the state-of-the-art for the QMs is very challenging, we looked at specific scenario of ensemble-based QMs. In this case, the effects of multiple excitations, have shown to deteriorate the performance of the memory-assisted MDI-QKD in such way that it can no longer beat their no-memory counterparts. Therefore another solution is needed to extend the distance. As a solution, we introduce the memory-assisted MDI-QKD with imperfect EPR sources in the next chapter.

Chapter 5

Memory-assisted MDI-QKD with EPR sources

5.1 Introduction

The memory-assisted MDI-QKD was analysed in Chapter 4 in the case of directly and indirectly heralding QMs. The requirements set for directly heralding QMs in this protocol are very demanding for the current technology to make it practical. Alternatively we proposed the possibility of using indirectly heralding QMs. In order to extend the performance of the protocol to improve the secret key rate versus distance, we proposed to use ensemble-based memories, as described in Section 4.6. However in this scenario the phenomenon of multiple-excitation effect deteriorates the performance of the MDI-QKD in such a way that it cancels the benefits we gain from the memory-assisted MDI-QKD protocol over other no-memory counterparts. The solution we are proposing in this Chapter is to instead use nearly ideal entangled-photon sources. This Chapter is focused on the memory-assisted MDI-QKD scenario using imperfect entangled photon pairs produced by an imperfect EPR source.

There are two conventional ways to produce entangled photon pairs. The spontaneous parametric down-conversion (SPDC) has been widely used as a source both for entangled photon pairs and for single photons. Its principle of operation is based on the properties of a nonlinear crystal. When a laser is directed to this crystal, the photons can split into pairs of photons that according to the conservation laws of energy and momentum, they have combined energies and momenta, equal to the energy and momentum of the original photon. The polarizations of this pair of photons are then correlated. There are two type of correlations depending on the polarization that the photons share. Type I is for the photons that share the same polarization and type II is for the anticorrelated photons, i.e., their polarizations are perpendicular to each other. However due to its probabilistic nature, SPDC makes it difficult to be used as an on-demand source of entanglement. More importantly, SPDC suffers from the same multi-photon components that made ensemble-based QMs useless in the setup of Figure 2.5(b).

An alternative method of generating entangled photon pairs is from the radiative decay of a single quatum dot. Entangled photon pairs are based on the Heisenberg uncertainty due to the correlations they present when being spatially separated. These EPR photon pairs confirm the quantum entanglement and by violating the Bell inequalities confirm their quantum nature. Quantum dots are eligible candidates of“artificial atoms” due to their three-dimensional electronic confinement and discrete energy levels. One of the most useful applications of the quantum dots is their generation of entangled photon pairs in terms of polarization.

A quantum dot structure has been proven almost immune to the multi-photon components and can be run at high GHz rates. Therefore it can be used as an imperfect EPR source in our memory-assisted MDI-QKD with indirectly QMs protocol. I will explain furthermore in the next section the system and analyse it in terms of its secret key rate performance.

5.2 This chapter’s contribution

- We analyse the memory-assisted MDI-QKD system when indirectly heralding QMs are loaded with the help of EPR sources. We particularly look at the case when quantum dot sources are used. In a realistic scenario the entangled photons at the state-preparation stage may undergo modulation errors similar to Chapter 3. We fully analyse the EPR state being generated in such a case and we obtain the key rate for our modified protocol.

- We consider different initial states for the EPR source. In the first scenario we consider that the main state produced by the EPR source is taken with imperfections included as described in [7]. We study how in this scenario the fidelity of such state alters the QBER and the key rate versus distance performance.

- In the final case we assume that the initial entangled photon state is a Werner state with a given fidelity. We use this EPR source in our protocol and make a comparison against its no-memory counterparts.

The rest of this chapter is structured as follows. In Section 5.3 we describe our proposed schemes and the modeling used for each component therein. Section 5.4 presents our key rate analysis, followed by the numerical results in Section 5.5. We conclude in Section 5.6.

5.3 System description

In this Chapter, we propose a new scheme that can potentially resolve the multiple-excitation problem we faced with ensemble-based QMs in the setup of Figure 2.5(b). There, the key problem was in driving the QMs, which, in turn could result in multiple excitations. If, however, we generate an entangled pair of photons, and store one in the QM, and use the other one to teleport the user's state to the QM, we will only excite as many photons as our EPR source generates. If we make sure that our EPR source generates only one single photon in each leg, we can be optimistic that our system can outperform the no-QM setups.

In Figure 5.1 there are two single-photon sources transmitting photons in the BB84 basis, towards a side-BSM. Simultaneously an EPR source emits two entangled photons, one towards the side-BSM and one towards its QM. At the side-BSM module, the two photons interfere and ideally two single-photon detectors click. Similar to Chapter 4, depending on which two single-photon detectors click and by knowing the initial state of the EPR photon pair we can estimate the state of the other entangled photon that has been stored in the QM. As soon as both QMs have been indicated the storage of a single photon from the side-BSM clicks, they follow the protocol similarly to the memory-assisted MDI-QKD protocol described in Chapter 4, where the middle-BSM follows. Below I will describe the quantum-dot EPR sources.

5.3.1 EPR source

The generation of entangled photon pairs from a quantum dot source is described below. The quantum dot consists of four energy levels and initially it is excited to a biexciton state. A biexciton state consists of two electrons and two heavy holes [7]. In the next step the quantum dot decays to the ground state by emitting in sequence two photons, that are constrained to have zero angular momentum (see Figure 5.2). The polarisations of the two generated photons are considered maximally entangled if the intermediate level states (excitons) of the dot are degenerate. The generated photon pair from this process is

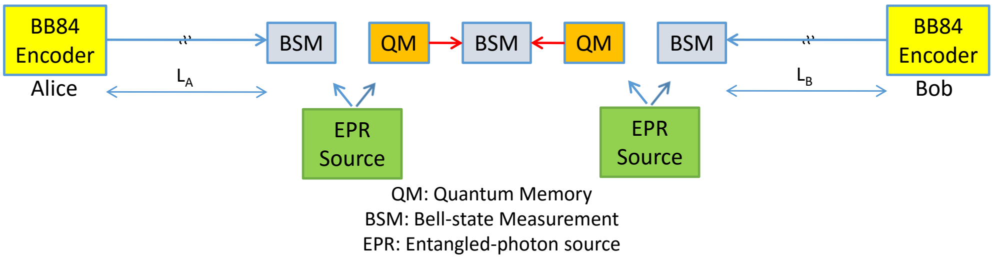


Figure 5.1: Memory-assisted MDI-QKD with EPR sources.

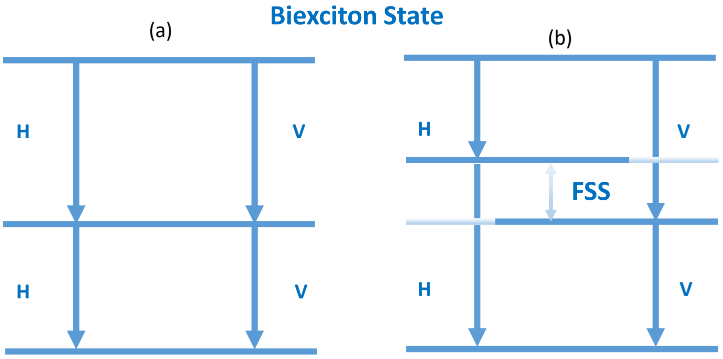


Figure 5.2: Decay paths in (a) a degenerate quantum dot and (b) non-degenerate dot as explained in [7].

$$\frac{|H_{xx}H_x\rangle + |V_{xx}V_x\rangle}{\sqrt{2}}, \tag{5.1}$$

where H and V denote the polarisation and subscripts xx and x are the first and second emmited photons, respectively. However, there is a fine-structure splitting (FSS) between two orthogonal states respective to H and V such that the decay is imposed to choose between the two distinguishable paths shown in Figure 5.2(b). In [7] they study how to control the FSS of a single quantum dot in order to find the degree of entanglement of the emission. They prove that the entanglement is tolerant of small fluctucations of the FSS and that the precise output state can be controlled by exploiting the FSS. The cross-dephasing time is defined as the characteristic time of dephasing between the superimposed H and V intermediate exciton photon states.

The biexciton and ground states do not evolve in time, however, the intermediate state of the first emitted photon is considered a superposition of two exciton-photon states with S being their energy separation difference equal to the FSS (see Figure 5.2(b)). The difference in phase created by the two states is equal to $St/\hbar$, where t is the random time spent in the middle states, and the final state is given by the following state

$$|\phi\rangle = \frac{|H_{xx}H_x\rangle + \exp(iSt/\hbar)|V_{xx}V_x\rangle}{\sqrt{2}}. \tag{5.2}$$

If one averages over t, then the generated EPR state will be in the subspace spanned by

$$|\Phi^{\pm}\rangle = \frac{|H_{xx}H_x\rangle \pm |V_{xx}V_x\rangle}{\sqrt{2}}. \tag{5.3}$$

In [7], there is an analysis that proves that entanglement of the photon pair is robust to the dephasing of the exciton state for the first-order coherence time of either single photon. In [7] the authors include the effects from background light, spin-scattered light and dephased light. The background light relates to uncorrelated polarised states of light that comes from other than the dot areas. The spin-scattering relates to the spin being scattered, after the emission of the first photon thus leading to uncorrelated polarisation, and dephasing is related to the randomized phase between the two superimposed eigenstates. By accounting for characteristic times of spin scattering, cross-dephasing and radiative recombination, the source output state in the rectilinear basis $|H_{xx}H_x\rangle, |V_{xx}V_x\rangle$ is given by

$$\rho_{Qdot} = \begin{bmatrix} A' & 0 & 0 & H' \\ 0 & B' & 0 & 0 \\ 0 & 0 & C' & 0 \\ H' & 0 & 0 & D' \end{bmatrix} \tag{5.4}$$

where A', B', C', D' represent the probabilities for, respectively, the states $|HH\rangle\langle HH|$, $|HV\rangle\langle HV|$, $|VH\rangle\langle VH|$ and $|VV\rangle\langle VV|$, whereas H' is the probability for the states $|HH\rangle\langle VV|$ and $|VV\rangle\langle HH|$. In order to analyse the system in the most general form, in our analysis, we assume the following general density matrix for our EPR source.

$$\rho_{EPR} = \begin{bmatrix} A & E & G & H \\ E & B & K & L \\ G & K & C & F \\ H & L & F & D \end{bmatrix} \tag{5.5}$$

where A, B, C, D, respectively, represent the probabilities for the Bell states $|\Phi^+\rangle\langle\Phi^+|$, $|\Phi^-\rangle\langle\Phi^-|$, $|\Psi^+\rangle\langle\Psi^+|$, $|\Psi^-\rangle\langle\Psi^-|$.This matrix is in the Bell basis, i.e., from left to right are the columns correspond to $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$, where

$$|\Phi^{\pm}\rangle = \frac{|HH\rangle \pm |VV\rangle}{\sqrt{2}} \tag{5.6}$$

and

$$|\Psi^{\pm}\rangle = \frac{|HV\rangle \pm |VH\rangle}{\sqrt{2}}. \tag{5.7}$$

Moving on to the next subsection we want to describe the protocol in which we have indirectly heralding QMs in the memory-assisted MDI-QKD by using EPR sources as taken from the special cases of the matrix in (5.5). We consider that the main entangled state generated by the quantum dot in [7] is given by Equation (5.2). The main components are generated by the HH photons and VV terms with a time difference in the subspace due to the cross-dephasing effect, thus there could be a mixture of the Bell states, $|\Phi^+\rangle$ and $|\Phi^-\rangle$.

5.4 Key rate analysis of MDI vs setup inefficiencies

In Figure 5.1 Alice and Bob send single photon states encoded as in BB84 polarisations. Simultaneously, each EPR source generates entangled photon pairs and sends one photon towards the side-BSM and the other photon towards the QM. The side-BSM heralds the teleportation of the users state to the QM. Here, we implicitly assume that storing a photon, generated by the local EPR source, into the QM can be done efficiency. The state of the EPR source is considered as the one given by Equation 5.5. However since each single photon sent by Alice and Bob are in the Z or X basis we need to apply the rotation matrix from Bell basis to the H/V basis, given by

$$R = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \end{bmatrix} \tag{5.8}$$

to obtain

$$\rho_{EPR;HV} = R^{\dagger}(\rho_{EPR})R, \tag{5.9}$$

which is the initial state of the EPR source in the HV basis.

In our rate analysis, we use the modelling introduced in Chapter 3 to break the setup in Figure

5.1 to smaller systems. In fact, the setup in Figure 5.1 can be thought as three sub-systems of the type we discussed in Chapter 3. The first and second subsystems are the MDI-QKD setups between the users and the corresponding photon P generated by the EPR source; see Figure 5.3. The third sub-system is the middle BSM on retrieved photons, from QMs. All these three sub-systems have the same structure as the MDI-QKD with imperfect sources discussed in Chapter 3. We can then use our results there in our key rate analysis here.

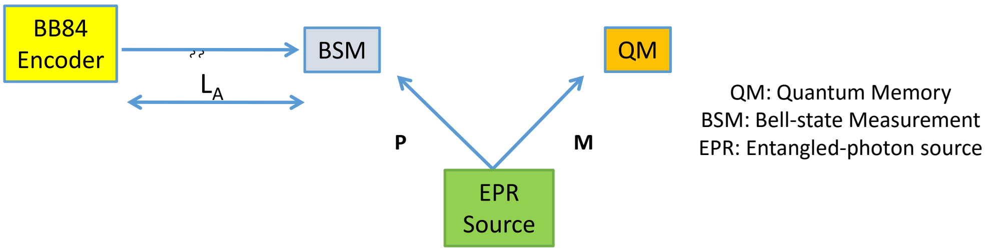


Figure 5.3: Side BSM operation for Alices' side. We can consider a similar structure for the Bob's side. The EPR source is located next to the QM and the measurement module.

In Figure 5.3, the initial density matrix including Alice single photon is given by

$$\rho_{AE;K}^{(m)} = \rho_{A;K}^{(m)} \otimes \rho_{EPR;HV}, \tag{5.10}$$

where $m = 0,1$ is the transmitted bit by Alice and K denotes the chosen basis by Alice. The EPR state consists of the memory photon and the photon that interferes at the BSM with Alices' (Bob's) as seen in Figure 5.3 and is given by

$$\rho_{EPR;HV} = \sum_{n,l,r,s=H,V} p_{n,l,r,s} |nl\rangle_{PM} \langle rs|, \tag{5.11}$$

where $p_{n,l,r,s}$ is the corresponding terms to the matrix given by Equation (5.9). From the above Equation we have that the full initial density matrix becomes

$$\rho^{(m)}_{AE;K} \quad = \sum_{n,l,r,s=H,V} p_{n,l,r,s}(\rho^{(m)}_{A;K} \otimes |n\rangle_P\langle r|) \otimes |l\rangle_M\langle s|, \tag{5.12}$$

where P denotes the photon that interferes at the side-BSM, whereas M denotes the single photon stored in the QM as seen in Figure 5.3. In the above Equation, the term in brackets represent an input state to a general MDI-QKD system as we discussed in Chapter 3. In order to find the output state, from each side-BSM, we first represent the term in brackets by $\rho^{(m)}_{AP;K}$ and then apply the procedure we developed in Chapter 3. Thus the output state for the two photons interfering at the side-BSM becomes

$$\rho^{(m)'}_{AP;K} = B_{ent}B_{\eta_\alpha}(\rho^{(m)}_{AP;K})B^{\dagger}_{\eta_\alpha}B^{\dagger}_{ent}, \tag{5.13}$$

where B_{η_α} is the same as in Equation (3.5). In Equation (5.13), Alice is at distance L_A from the side BSM. Thus, $\eta_a = \eta_{\mathrm{ch}}(L_A)\eta_d$, while for the EPR photon, P, we consider that it has an imperfection equal to $\eta_{ent} = \eta_g\eta_d$, where η_g is the chance of generating an EPR pair. By applying the butterfly operation as in Equation (C.1) to $\rho^{(m)'}_{AP;K}$, we can find the premeasurement state $\rho^{(m)}_{out;K}$. To obtain Bobs' initial and output density matrices, the same analysis is followed as for the Alices' case.

Next, an analysis of how to obtain the key rate with the given initial density matrix from both sides, follows.The key rate is given as in Equation (4.4) with the difference that the term Y^{QM}_{11} is now replaced by the Y^{QM}_{EPR} as given below

$$R_{\mathrm{QM}} = R_S Y^{\mathrm{QM}}_{EPR}[1 - h(e^{\mathrm{QM}}_{11;X}) - fh(e^{\mathrm{QM}}_{11;Z})]. \tag{5.14}$$

In Equation (5.14) $e^{\mathrm{QM}}_{11;X}$ and $e^{\mathrm{QM}}_{11;Z}$, respectively, represent the QBER between Alice and Bob in the X and Z basis, when single photons are used, and Y^{QM}_{EPR} represents the rate at which both memories are loaded with single photons of the same basis and the middle BSM is successful. The yield Y^{QM}_{EPR} changes according to Eqs. (4.6) and (A.3) as they depend on the values of η_{1A} and η_{1B}.

Such parameters must be calculated for each of the output density matrices $\rho^{(m)}_{out;K}$ corresponding to the terms in bracket in Equation (5.12).

Both the yield and the QBER in X and Z depend on the final state of each QM and essentially on the initial state of the EPR source and single photons sent by the source. The post-measurement state of each side-BSM will provide us with the teleported state to each QM. Once the state of each QM is known, we use the procedure outlined in Chapter 3 to calculate the success rate for the middle BSM.

To find the final post-measurement state, first we need to apply in the same order all the above to Bob's side and obtain his QM state right before the middle BSM measurement operation. The final state of Bob's QM can be obtained similarly.

5.5 Numerical results

In this section, we study the impact of different parameters on the secret key generation rate of our scheme in different cases. We compare in a symmetric setup the QBER in X and Z bases and additionally the secret key generation rate per transmitted pulse for different fidelities of the Bell states generated from an EPR source assuming the users' single-photon sources are ideal. We continue by comparing different Werner states being produced by an imperfect EPR source in terms of the QBER in X and Z bases and the key rate for both the asymmetric and symmetric setups and finally compare the results between the two setups. Next we compare the symmetric and asymmetric setups again in terms of the secret key rate and QBER versus distance. All results have been obtained assuming an error correction inefficiency $f = 1.16$, 0.2 dB per km of loss in the channel, detection efficiency of $\eta_d = 0.15$, dark count rate per pulse $p_{\mathrm{dc}} = 1 \times 10^{-6}$, and no misalignments, i.e., $e_{dA} = e_{dB} = 0$ and efficiency for an EPR source $\eta_g = 1$. For the memories it is assumed that the reading efficiency $\eta_r = 1$, reading time $\tau_r = 0$, writing time $\tau_w = 1 \times 10^{-6}$ sec. The single photon repetition rate $R_S = 1 \times 10^{-6}$sec and there is no memory decay..

- Case 1: A mixture of $|\Phi^+\rangle$ and $|\Phi^-\rangle$

  In a realistic scenario it is assumed that at the state-preparation stage of the EPR source there are imperfections. In this scenario we study the case where there is a mixture of Bell states as part of imperfections. More specifically we take a mixture of Φ^+ and Φ^- thus the initial density matrix of the EPR source in the Bell basis is equal to

$$\rho_{EPR;\Phi} = \begin{bmatrix} A & 0 & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{5.15}$$

  where A is the probability for the Bell state $|\Phi^+\rangle = \frac{|HH\rangle + |VV\rangle}{\sqrt{2}}$ and B is the probability for Bell state $|\Phi^-\rangle = \frac{|HH\rangle - |VV\rangle}{\sqrt{2}}$. Equivalently, we have

$$\rho_{EPR;\Phi} = F|\Phi^+\rangle\langle\Phi^+| + (1-F)|\Phi^-\rangle\langle\Phi^-|, \tag{5.16}$$

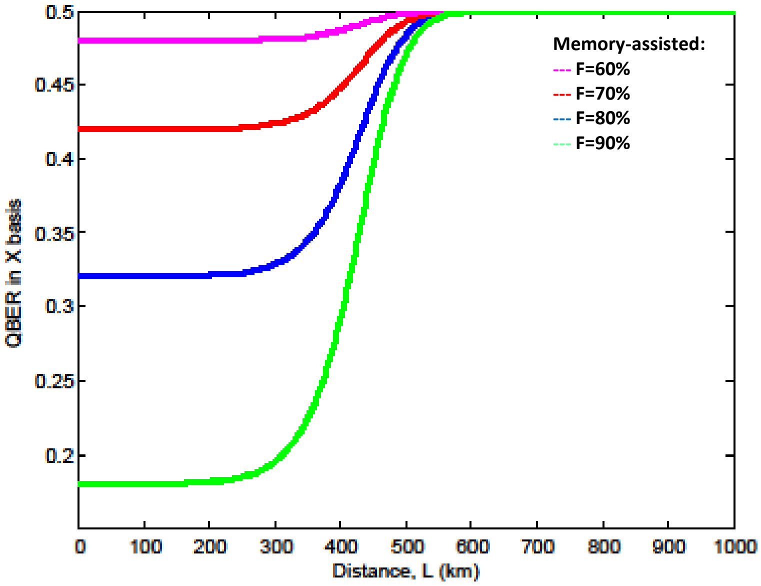


Figure 5.4: QBER in X basis versus distance for different fidelities of a Bell state.

where F = A. As we can see from Figure 5.4 for different values of fidelity, F, for the input state, the QBER in X basis increases as the fidelity of the main EPR state (in this case $|\Phi^+\rangle$) decreases. The reason is that the mixture of the two Bell states, creates false errors on the detectors both in the side-BSMs and the middle BSM operations. Thus the probability of having an error is high. For fidelities of F=60% of $|\Phi^+\rangle$ the QBER is very high at the sources side, making the protocol insecure. For fidelities higher than 60%, the QBER is constant up to a distance of 300 km and then increases abruptly due to the dark count effects being dominant over the correct clicks.

In Figure 5.5, for similar fidelities of the input state, we compare the system with its no-memory counterpart. We can see that for fidelities lower than 70% the memory-assisted MDI-QKD has a low performance due to the QBER being high from the imperfection in the EPR source. For a fidelity equal to 80% the memory-assisted MDI-QKD can outperform its no-memory counterpart between rougly 90 km to 250 km in terms of key rate per transmitted pulse, however it reaches shorter distances in comparison to the latter one. For fidelities higher than 80% our memory-assisted scheme can outperform the no-memory

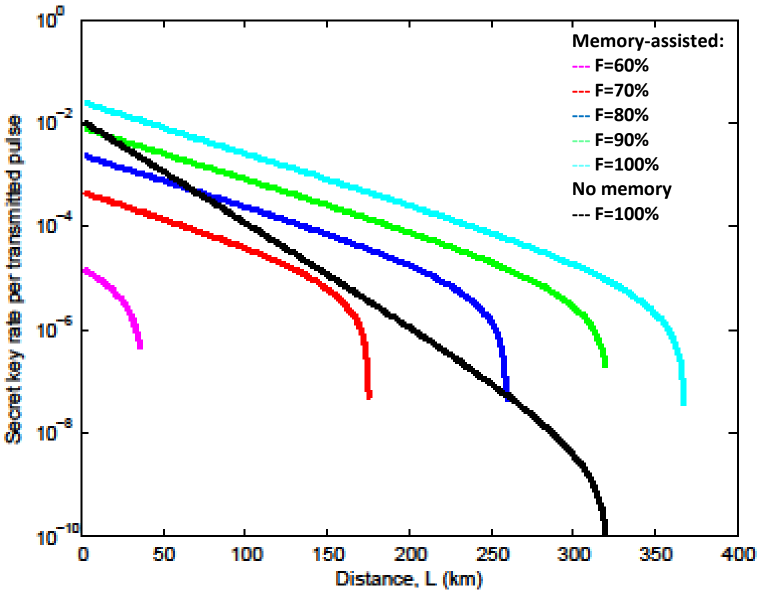


Figure 5.5: Key rate versus distance for different fidelities of a Bell state.

system both in terms of distance and key rate per pulse, (for F=100% reaches up to 360 km in Figure 5.5).

- Case 2: Werner states

In a different scenario to the above, we are studying the case where there is a mixture of the four maximally entangled states as given by the Werner state below

$$\rho_{EPR} = F|\Phi^+\rangle\langle\Phi^+| + \frac{(1-F)}{3}(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|). \qquad (5.17)$$

In this scenario, we are studying the case of having a mixture of Bell states as we consider imperfections at the state-preparation stage of the EPR source. In the matrix format, the initial density matrix of the EPR source is equal to

$$\rho_{EPR;W} = \begin{bmatrix} F & 0 & 0 & 0 \\ 0 & (1-F)/3 & 0 & 0 \\ 0 & 0 & (1-F)/3 & 0 \\ 0 & 0 & 0 & (1-F)/3 \end{bmatrix}. \qquad (5.18)$$

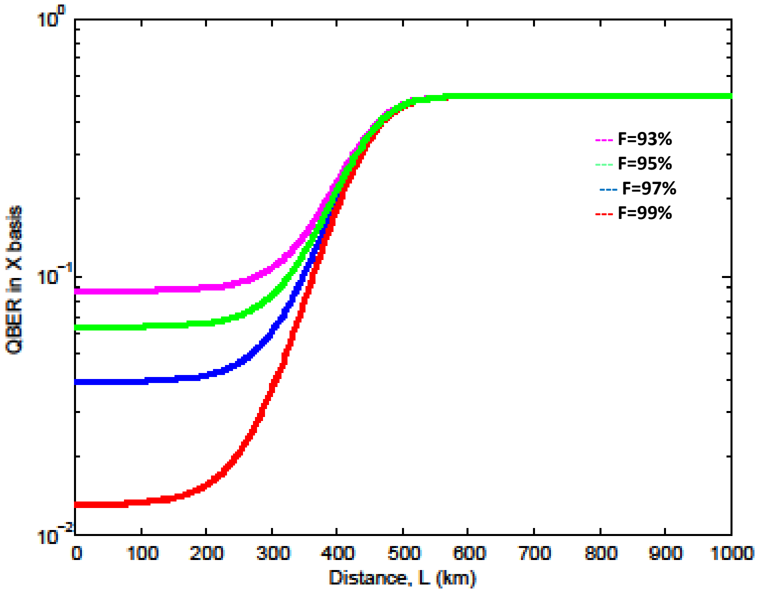


Figure 5.6: QBER in X basis versus distance for different fidelities of a Werner state.

We have taken fidelities ranging from 93% to 99%, meaning that the mixture of other maximally entangled states is kept as low as possible and having the main state generated by an EPR source at the highest possible fidelity. From Figure 5.6 we can see that the lower the fidelity is, the higher the QBER becomes. At values less than 93% our procol is insecure because the error rate at the source's side becomes significantly higher than 11%. For fidelities kept well above 93%, our protocol is functional, with the dark count effect becoming the main source of QBER at distances roughly above 300 km. Additionally as a comparison to the previous case, where only a mixture of two states was included in modulation errors, the QBER in this case is much higher. This is due to the fact that the errors at the modulation stage is now higher as there are three possible states contributing to error clicks at the side-BSM and BSM stages.

In Figure 5.7 we make a comparison with similar values of fidelities and compare them to the no-memory case. For fidelities equal to 93% our protocol behaves better within the region of roughly 100 km to 260 km in terms of key rate per pulse, however the no-memory system reaches longer distances in this case (320 km). For values of equal and higher fidelity than 95% all our memory-assisted cases, outperform the no-memory case, in both key rate per pulse and security distance. At 95% fidelity, it reaches up to roughly 325 km

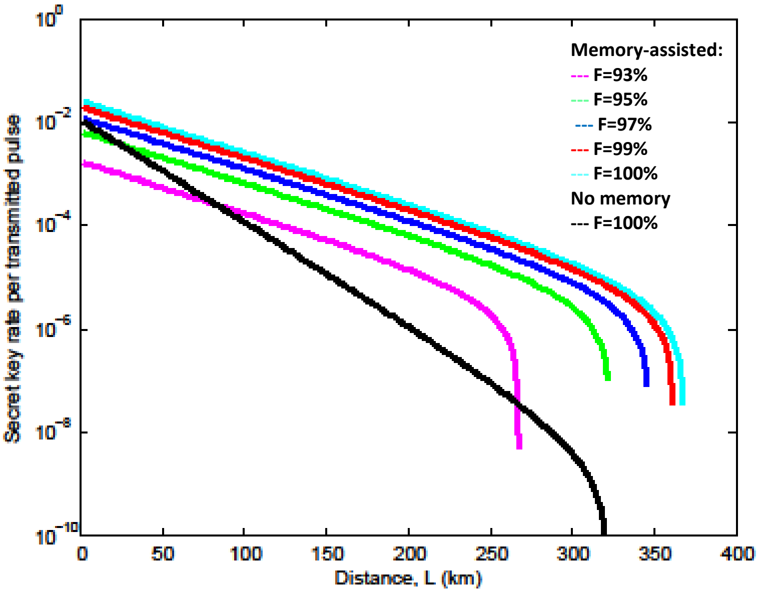


Figure 5.7: Key rate versus distance for different fidelities of a Werner state.

and for 99% it reaches up to 360km.

5.6 Conclusion

In this chapter we analysed a memory-assisted MDI-QKD with EPR sources for indirectly heralding QMs mentioned in Chapter 4. To avoid the multiple excitation effect that ensemble based memories are prone to, which eventually deteriorate the key rate performance in a memory-assisted MDI-QKD scenario, we proposed instead the usage of EPR sources. The generation of entangled photon pairs can be achieved in two ways, the SPDC and quantum dots. The SPDC method has the disadvantage of generating multiple photons itself, therefore not improving the performance. The quantum dots can however both avoid the multi-photon components and also perform adequately at high rates on the order of GHz. They have been fully studied in terms of timing imperfections, i.e., cross-dephasing, background light and spin-scattering and still function sufficiently well under certain assumptions as an imperfect EPR source. In our protocol we considered that the EPR source could tolerate, at the state-preparation stage, some modulation errors and our protocol would still be able to outperform the no-memory QKD schemes.

We provided a detailed analysis on how to retrieve the state of the two memories under the assumption that the EPR source generates a generalised state with a mixture of all Bell states. We have considered different cases for the initial state and studied how the performance of the key rate versus distance and QBER is affected. In the first case we considered only Bell states that expected to be generated by a quantum dot source. We assumed that one state has a lower chance to be generated. As the fidelity of the dominant state is increased, the key rate performance is significantly increased compared to the no-memory case. Additionally the QBER is decreased accordingly as the chance of having an error from the side-BSMs and middle BSM and also at the modulation stage are low.

In the another case, we studied how the fidelity of Werner states affects key rate and QBER versus distance performance. The lower the fidelity of the leading generated state, the higher the QBER at the source's side and the shorter the security distance becomes. For a fidelity of 93% our scheme offers higher rates over distances of roughly 100 km to 260 km however, the no-memory system reaches longer distances in this case (320 km). For fidelities $> 95\%$ all our memory-assisted cases outperform the no-memory case, in both key rate per pulse and security distance. At 95% , the security distance reaches up to roughly 325 km and at 99% it reaches up to 360 km. Therefore we conclude that an entangled photon source with high fidelity in our memory-assisted MDI-QKD can successfully outperform, in terms of key rate per pulse and the security distance, conventional no-memory MDI-QKD schemes.

Chapter 6

Summary and future work

In this thesis we addressed the impact of quantum memories employed in an MDI-QKD scenario to improve its performance over no-memory conventional QKD systems, through the analysis of the secret key rate. We considered a detailed analysis of non-idealities at the source's side as well as on the memory side.

We firstly analysed the effects of a single-photon source being imperfect at the state-preparation stage and how it would affect the key rate and QBER versus distance. We made a comparison between an ideal MDI-QKD and a conventional BB84 system and an source MDI-QKD system with imperfect sources to study the performance in each case when modulation errors are accounted for.

Then we continued by introducing a new MDI-QKD system that used QMs in its setup. In Chapter 4, we meticulously considered imperfections in the QMs in terms of decoherence and storage time and how their addition to the MDI-QKD affects the key rate versus distance. Yet considering the strict requirements in terms of coherence times and writing times of the QMs, we proposed an alternative system using ensemble-based QMs. The ensemble-based memories, fullfil the criteria we set for having large storage-bandwidth product and short access and entangling times. However, we found that due to the multiple excitation effect of the ensemble based QMs, we could no longer outperform the no-memory systems. Therefore we proposed an alternative system, using EPR sources.

This system consisted of EPR sources used in our memory-assisted MDI-QKD protocol. For a realistic scenario, we included imperfections at the EPR source's state-preparation stage as we did similarly for single-photon sources in Chapter 3. The quantum dot is the best candidate as an entangled photon source as it has minimum multiple photon components and can be used on demand. By including modulation errors on the EPR source's side, we estimated the maximum achievable distance for the memory-assisted MDI-QKD system. We found that when the fidelity of these entangled photon pairs has kept at a sufficiently high value, the system behaved quite promising against its no-memory conventional counterparts.

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

- In Chapter 5 we have analysed how the protocol performs under the assumption of single photon states used. In the future, as an extension to the same protocol we apply the decoy-state method to study how it behaves under certain assumptions, making it still possible to retrieve high key rates and longer secure distances when compared to no-memory protocols.
- Our work has analysed the schemes for Chapter 4 and 5 under the assumption of using infinitely many keys. As a more practical assumption, we will study the finite key analysis on all protocols described in Chapters 4 and 5 and compare these to tight security bounds for practical decoy state QKD protocols.
- We analyse how our memory-assisted MDI-QKD performs using specific quantum memories that are currently advanced in technological terms to be suitable candidates for the requirements we have set in Chapters 4 and 5.
- In Chapter 5 we have not accounted for the required coherence times for the QMs. In the next step we will study the coherence time requirements in the memory-assisted MDI-QKD with EPR sources for a more practical implementation of the protocol.

Our results pave the way for a promising future work to be further pursued. This trust-free protocol could be used as part of a quantum repeater system that could lead to a future quantum network. Such a network could potentially be implemented by a number of imperfect quantum memories, however the key rate would remain at high rates.

Appendix A

Loading process

The loading process in the setups of Figures 2.5(a) and 2.5(b) are probabilistic ones, with two geometric random variables N_A and N_B playing the major role. Suppose the success probability for each loading attempt corresponding to these random variables is, respectively, given by η_A and η_B. Then, we obtain the following probability distribution for $|N_A - N_B|$:

$$\Pr(|N_A - N_B| = k) = [(1-\eta_A)^k + (1-\eta_B)^k]P_0, \quad k > 0, \tag{A.1}$$

where

$$P_0 = \Pr(N_A = N_B) = \frac{\eta_A \eta_B}{\eta_A + \eta_B - \eta_A \eta_B}. \tag{A.2}$$

Using the above expressions, we then obtain

$$\begin{aligned} N_L(\eta_A, \eta_B) &= \mathrm{E}\{\max(N_A, N_B)\} \\ &= \frac{1}{2}\mathrm{E}\{|N_A - N_B| + N_A + N_B\} \\ &= \frac{1}{2}\left[\frac{\eta_A(1-\eta_B)}{\eta_B(\eta_A + \eta_B - \eta_A\eta_B)} + \frac{\eta_B(1-\eta_A)}{\eta_A(\eta_A + \eta_B - \eta_A\eta_B)} + \frac{1}{\eta_A} + \frac{1}{\eta_B}\right]. \end{aligned} \tag{A.3}$$

Moreover,

$$\mathrm{E}\{\exp(-|N_A - N_B|\delta)\} = P_0 \left[\frac{1}{1-e^{-\delta}(1-\eta_A)} + \frac{1}{1-e^{-\delta}(1-\eta_B)} - 1\right] \tag{A.4}$$

and the average storage time, T_{st}, is given by

$$T_{st} = \mathrm{E}\{|N_A - N_B|\}T = \frac{\eta_A(1-\eta_B)T}{\eta_B(\eta_A+\eta_B-\eta_A\eta_B)} + \frac{\eta_B(1-\eta_A)T}{\eta_A(\eta_A+\eta_B-\eta_A\eta_B)}. \tag{A.5}$$

Finally, we can show that

$$\Pr\{N_A \geq N_B\} = \frac{\eta_B}{1-(1-\eta_A)(1-\eta_B)} = 1 - \Pr\{N_A < N_B\} \tag{A.6}$$

and

$$\begin{aligned} S_{A<B}(\delta) &\equiv \sum_{1=n_a<n_b}^{\infty} \Pr\{N_A = n_a, N_B = n_b\} \exp[(n_a - n_b)\delta] \\ &= \frac{\eta_A\eta_B(1-\eta_B)e^{-\delta}}{[1-(1-\eta_B)e^{-\delta}][1-(1-\eta_A)(1-\eta_B)]}. \end{aligned} \tag{A.7}$$

Appendix B

Misalignment Parameters

In this Appendix, we obtain the misalignment probability for each of the setups in Figures 2.5(a) and 2.5(b). Let us first consider the directly heralding memory case in the Z basis and assume loading probabilities η_A and η_B for Alice's and Bob's memories. Suppose the legitimate state is $|s_H\rangle\langle s_H|$. Assuming setup misalignment probabilities e_{dK}, $K = A,B$, for leg K of Figure 2.5(a), in the absence of background counts, the stored state in memory K will become $\rho_{d0} = (1-e_{dK})|s_H\rangle\langle s_H| + e_{dK}|s_V\rangle\langle s_V|$. Now, including the background counts, the memory state will become

$$\rho_{dZ} = [1-e_{\mathrm{BG}}^{(K)}]\rho_{d0} + e_{\mathrm{BG}}^{(K)}\frac{|s_H\rangle\langle s_H| + |s_V\rangle\langle s_V|}{2}, \tag{B.1}$$

where $e_{\mathrm{BG}}^{(K)} = \frac{1-e^{-\eta_w p_{\mathrm{BG}}}}{\eta_K}$, $K = A,B$, is the probability that our memory has been loaded by a background (unpolarized) photon conditioned on a successful loading. The total misalignment probability in the Z basis for the Alice's and Bob's memory is then given by

$$e_{dZ}^{(K)} = e_{dK}(1-e_{\mathrm{BG}}^{(K)}) + e_{\mathrm{BG}}^{(K)}/2, \quad K = A,B, \text{ for directly heralding QMs.} \tag{B.2}$$

Now, let's assume the legitimate state, in the X basis, is $|s_+\rangle\langle s_+|$, where $|s_\pm\rangle = (|s_H\rangle \pm |s_V\rangle)/\sqrt{2}$. Right after a successful loading, the state of the memory is then given by

$$\rho_{dX}(0) = [1-e_{\mathrm{BG}}^{(K)}]\rho'_{d0} + e_{\mathrm{BG}}^{(K)}\frac{|s_H\rangle\langle s_H| + |s_V\rangle\langle s_V|}{2} \tag{B.3}$$

where $\rho'_{d0} = (1 - e_{dK})|s_+\rangle\langle s_+| + e_{dK}|s_-\rangle\langle s_-|$. If memory A is the late memory, i.e., if $N_A \geq N_B$, then there will be no dephazing errors, in which case, $e_{dX}^{(A)} = e_{dZ}^{(A)}$. If it is the early memory, however, the dephazing operation in Equation (4.3) will act on $\rho_{dX}(0)$ to give us

$$\rho_{dX}(t) = [1 - e_{\text{BG}}^{(K)}]\rho'_{d0}(t) + e_{\text{BG}}^{(K)} \frac{|s_H\rangle\langle s_H| + |s_V\rangle\langle s_V|}{2}, \tag{B.4}$$

where $\rho'_{d0}(t) = [(1-e_{dK})p(t) + e_{dK}(1-p(t))]|s_+\rangle\langle s_+| + [e_{dK}p(t) + (1-e_{dK})(1-p(t))]|s_-\rangle\langle s_-|$. The misalignment probability is then given by

$$e_{dX}^{(K)} = e_{dZ}^{(K)} + \beta_A e_{\text{deph}}^{(K)}, \tag{B.5}$$

where $\beta_K = (1 - 2e_{dK})(1 - e_{\text{BG}}^{(K)})$, $K = A, B$, and

$$e_{\text{deph}}^{(A)} = \begin{cases} 0 & N_A \geq N_B \\ (1/2)[1 - \exp(-|N_A - N_B|T/T_2)] & N_A < N_B \end{cases}, \tag{B.6}$$

where N_A and N_B are geometric random variables with success probabilities η_A and η_B. By averaging over these variables, we obtain

$$\text{E}\{e_{dX}^{(A)}\} = e_{dZ}^{(A)} + \beta_A \text{E}\{e_{\text{deph}}^{(A)}\}, \tag{B.7}$$

where

$$\text{E}\{e_{\text{deph}}^{(A)}\} = [\Pr\{N_A < N_B\} - S_{A<B}(T/T_2)]/2, \tag{B.8}$$

which can be obtained from equations (A.6) and (A.7). One can obtain similar expressions for $e_{dX}^{(B)}$ by swapping A and B in equations (B.6)–(B.8).

To calculate $\text{E}\{e_{dX}^{\text{QM}}\}$ from Equation (4.11), the final remaining term is given by

$$\text{E}\{e_{dX}^{(A)} e_{dX}^{(B)}\} = e_{dZ}^{(A)} e_{dZ}^{(B)} + \beta_A \text{E}\{e_{\text{deph}}^{(A)}\} e_{dZ}^{(B)} + \beta_B \text{E}\{e_{\text{deph}}^{(B)}\} e_{dZ}^{(A)}, \tag{B.9}$$

where we used the fact that $e_{\text{deph}}^{(A)} e_{\text{deph}}^{(B)} = 0$, as one of the two terms is always zero regardless of the values of N_A and N_B.

In the case of indirectly heralding QMs, we assume that each erroneous click on the side BSMs will effectively result in a flip to the corresponding QM state, and can also be modeled as misalignment. This assumption is valid at low distances where majority of errors are caused by the setup misalignment. We then obtain

$$e_{dZ}^{(K)} = e_{11;Z}(\eta_d \eta_{\mathrm{ch}}(L_K), \eta_d \eta_{\mathrm{ent}}, e_{dK}), \quad K = A, B, \tag{B.10}$$

for indirectly heralding QMs, where $e_{11;Z}$ can be calculated from Equation (2.22) at an equivalent dark count rate of $\gamma_{\mathrm{dc}} + \eta_d \gamma_{\mathrm{BG}}/2$. At long distances, most errors originate from dark counts or background photons, whose effective misalignment effect will approach half of $e_{11;Z}$ in the above equation. As a conservative assumption, we use the expression in Equation (B.10) for all distances.

All other terms in Equations (4.10) and (4.11) can be obtained following the same expressions in Equations (B.5)–(B.9) at $\beta_K = 1 - 2e_{dZ}^{(K)}$, for $K = A, B$, and using Equation (B.10) for $e_{dZ}^{(K)}$.

Appendix C

Butterfly operator

In this Appendix, we obtain the butterfly operator B_{BF} that acts on the input state for the setup given in Figure 3.1. Let us first consider the input state is taken from Equation (5.10) accordingly for Alice and Bob including their EPR state for each side. This input state after modeling the path loss as in Figure 3.2 has three possible outcomes in polarisation, i.e., in the Z basis we have the H,V photon polarisations and the vacuum state $|0\rangle$. Hence our input state is a bipartite system of a combination of 3 possible outcomes in each case leading to a 9×9 system. The analytical expression of Alice and Bob's input state is after modeling the path loss is given by

$$\begin{aligned}
\rho_{A;Z}^{(m)'} &= \eta(\alpha|H\rangle_A\langle H| + \gamma|V\rangle_A\langle V|) \\
&+ \beta|H\rangle_A\langle V| + \beta^*|V\rangle_A\langle H|) \\
&= \eta_A\rho_{A;Z}^{(m)} + (1-\eta_A)|0\rangle_A\langle 0| \qquad \text{(C.1)}
\end{aligned}$$

and similarly for Bob

$$\begin{aligned}
\rho_{B;Z}^{(n)'} &= \eta(\alpha|H\rangle_B\langle H| + \gamma|V\rangle_B\langle V|) \\
&+ \beta|H\rangle_B\langle V| + \beta^*|V\rangle_B\langle H|) \\
&= \eta_B\rho_{B;Z}^{(n)} + (1-\eta_B)|0\rangle_B\langle 0|. \qquad \text{(C.2)}
\end{aligned}$$

Ψ_A	Ψ_B	$B_{BF}(\Psi_A\Psi_B)$
$\vert H\rangle$	$\vert H\rangle$	$[\vert 2\rangle_{D_{H_1}}\vert 0\rangle_{D_{H_2,V_1,V_2}}-\vert 0\rangle_{D_{H_1,V_1,V_2}}\vert 2\rangle_{D_{H_2}}]/\sqrt{2}$
	$\vert V\rangle$	$[\vert 1\rangle_{D_{V_1}}\vert 1\rangle_{D_{H_2}}\vert 0\rangle_{D_{H_1,V_2}}-\vert 1\rangle_{D_{V_2}}\vert 1\rangle_{D_{H_2}}\vert 0\rangle_{D_{H_1,V_1}}+\vert 1\rangle_{D_{V_1}}\vert 1\rangle_{D_{H_1}}\vert 0\rangle_{D_{H_2,V_2}}-\vert 1\rangle_{D_{H_1}}\vert 1\rangle_{D_{V_2}}\vert 0\rangle_{D_{H_2,V_1}}]/2$
	$\vert 0\rangle$	$[\vert 1\rangle_{D_{H_2}}\vert 0\rangle_{D_{H_1,V_1,V_2}}+\vert 0\rangle_{D_{H_2,V_1,V_2}}\vert 1\rangle_{D_{H_1}}]/\sqrt{2}$
$\vert V\rangle$	$\vert H\rangle$	$[\vert 1\rangle_{D_{V_2}}\vert 1\rangle_{D_{H_2}}\vert 0\rangle_{D_{H_1,V_1}}-\vert 1\rangle_{D_{V_1}}\vert 1\rangle_{D_{H_2}}\vert 0\rangle_{D_{H_1,V_2}}-\vert 1\rangle_{D_{V_1}}\vert 1\rangle_{D_{H_1}}\vert 0\rangle_{D_{H_2,V_2}}+\vert 1\rangle_{D_{H_1}}\vert 1\rangle_{D_{V_2}}\vert 0\rangle_{D_{H_2,V_1}}]/2$
	$\vert V\rangle$	$[\vert 2\rangle_{D_{V_1}}\vert 0\rangle_{D_{H_2,H_1,V_2}}-\vert 0\rangle_{D_{H_1,H_2,V_1}}\vert 2\rangle_{D_{V_2}}]/\sqrt{2}$
	$\vert 0\rangle$	$[\vert 1\rangle_{D_{V_1}}\vert 0\rangle_{D_{H_1,H_2,V_2}}+\vert 0\rangle_{D_{H_1,H_2,V_1}}\vert 1\rangle_{D_{V_2}}]/\sqrt{2}$
$\vert 0\rangle$	$\vert H\rangle$	$[\vert 1\rangle_{D_{H_1}}\vert 0\rangle_{D_{H_2,V_1,V_2}}-\vert 0\rangle_{D_{H_1,V_1,V_2}}\vert 1\rangle_{D_{H_2}}]/\sqrt{2}$
	$\vert V\rangle$	$[\vert 1\rangle_{D_{V_1}}\vert 0\rangle_{D_{H_1,H_2,V_2}}-\vert 0\rangle_{D_{H_1,H_2,V_1}}\vert 1\rangle_{D_{V_2}}]/\sqrt{2}$
	$\vert 0\rangle$	$\vert 0\rangle_{D_{H_1}}\vert 0\rangle_{D_{H_2}}\vert 0\rangle_{D_{V_1}}\vert 0\rangle_{D_{V_2}}$

Table C.1: Butterfly operation on input state

The butterfly operator B_{BF} will be given analytically for the above joint state according to Equation (5.10) as shown in the Table C.1.

Bibliography

[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE.

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

[3] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* , 67:661, 1991.

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

[5] 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.*, 107:053603, Jul 2011.

[6] N.L. Piparo, M. Razavi, and C. Panayi. Measurement-device-independent quantum key distribution with ensemble-based memories. *Selected Topics in Quantum Electronics, IEEE Journal of*, 21(3):138–147, May 2015.

[7] A. J. Hudson, R. M. Stevenson, A. J. Bennett, R. J. Young, C. A. Nicoll, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields. Coherence of an entangled exciton-photon state. *Phys. Rev. Lett.*, 99:266802, Dec 2007.

[8] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telgraphic communications. *J. AIEE*, 45:109–115, 1926.

[9] Cipher A. Deavours and Louis Kruh. *Machine Cryptography and Modern Cryptanalysis*. Artech House, Inc., Norwood, MA, USA, 1985.

[10] Whitfield Diffie and Martin E. Hellman. New directions in cryptography, 1976.

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

[12] M. Gardner. Mathematical games, a new kind of cipher that would take millions of years to break. *Sci. Am*, 237:120, 1977.

[13] A. Shamir. Cryptographic hardware and embedded systems: first international worskhop. *Proceedings of CHES'99, WOrcester, MA, USA, Lecture*, 1717, 1999.

[14] et al. T. Kleinjung, P. Zimmermann. Factorization of a 768-bit rsa modulus. *Factorization of a 768-bit RSA modulus*, 6223:333–350, February 2010.

[15] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Computing*, pages 1484–1509, 1997.

[16] M. Hendrych M. Dusek, Norbert Lütkenhaus. Quantum cryptography. *Progress in Optics*, pages 381–454, 2006.

[17] Claude E. Shannon. Communication Theory of Secrecy Systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[18] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.

[19] D. Gottesman, Hoi-Kwong L., N. Lütkenhaus , and J. Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, pages 136–, June 2004.

[20] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[21] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* , 91:057901, August 2003.

[22] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[23] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[24] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[25] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comput.*, 7:073, 2007.

[26] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Experimental demonstration of time-shift attack against practical quantum key distribution systems. *Phys. Rev. A*, 78:042333, 2008.

[27] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, 4(10):686–689, 2010.

[28] C Wiechers, L Lydersen, C Wittmann, D Elser, J Skaar, Ch Marquardt, V Makarov, and G Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1):013043, 2011.

[29] Henning Weier, Harald Krauss, Markus Rau, Martin Fürst, Sebastian Nauerth, and Harald Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics*, 13(7):073024, 2011.

[30] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.*, 107:110501, Sep 2011.

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

[32] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, Mar 2012.

[33] E. Biham, B. Huttner, and T. Mor. Quantum cryptographic network based on quantum memories. *Phys. Rev. A*, 54(4):2651, 1996.

[34] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, Jul 2007.

[35] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008.

[36] F. Xu, B. Qi, and H. Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, 2010.

[37] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, (4):686–689, 2010.

[38] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.*, 37(6):1008–1010, March 2012.

[39] M. Sasaki, M. Fujiwara, and et. al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Exp.*, 19(11):10387–10409, 2011.

[40] M. Peev *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.*, 11:075001, 2009.

[41] I. Choi, R. J. Young, and P. D. Townsend. Quantum information to the home. *New J. Phys.*, 13:063039, June 2011.

[42] 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*, 2:041010, Nov. 2012.

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

[44] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and Kae Nemoto. Quantum communication without the necessity of quantum memories. *Nat. Photon.*, 6:771–781, Oct. 2012.

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

[46] C. Panayi and M. Razavi. Measurement device independent quantum key distribution with imperfect quantum memories. In *Tech. Digest, The Sixth International Conference on Quantum, Nano and Micro Technologies*, Rome, Italy, 2012.

[47] Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß. Measurement-device-independent quantum key distribution with quantum memories. *arXiv:1306.3095*, 2013.

[48] Xiongfeng Ma and Mohsen Razavi. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A*, 86:062319, Dec. 2012.

[49] Mohsen Razavi, Marco Piani, and Norbert Lütkenhaus. Quantum repeaters with imperfect memories: Cost and scalability. *Phys. Rev. A*, 80:032301, Sept. 2009.

[50] M. Razavi, K. Thompson, H. Farmanbar, Ma. Piani, and N. Lütkenhaus. Physical and architectural considerations in quantum repeaters. In *Proc. SPIE*, volume 7236, page 723603, San Jose, CA, 2009.

[51] Mohsen Razavi, Nicolo Lo Piparo, Christiana Panayi, and David E. Bruschi. Architectural considerations in hybrid quantum-classical networks (invited paper). In *Iran Workshop on Communication and Information Theory (IWCIT)*, pages 1–7, Tehran, Iran, 2013.

[52] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* , 85(2):441, July 2000.

[53] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457, 2003.

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

[55] Xiongfeng Ma. Quantum cryptography. *Thesis*, 2008.

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

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

[58] Nikolina Ilic. The ekert protocol. *Journal of Physics*, 2007.

[59] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[60] Thomas Jennewein, Christoph Simon, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729, 2000.

[61] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[62] Xiongfeng Ma, Chi-Hang Fred Fung, and Mohsen Razavi. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A*, 86:052305, Nov 2012.

[63] Zhiyuan Tang, Kejin Wei, Olinka Bedroya, Li Qian, and Hoi-Kwong Lo. Experimental measurement-device-independent quantum key distribution with imperfect sources. *arXiv*, 2015.

[64] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A*, 90:052314, Nov 2014.

[65] S. Lloyd, M. S. Shahriar, J. H. Shapiro, and P. R. Hemmer. Long distance, unconditional teleportation of atomic states via complete bell state measurements. *Phys. Rev. Lett.*, 87:167903, Sep 2001.

[66] Mohsen Razavi and Jeffrey H. Shapiro. Long-distance quantum communication with neutral atoms. *Phys. Rev. A*, 73:042303, April 2006.

[67] Stephan Ritter, Christian Nölleke, Carolin Hahn, Andreas Reiserer, Andreas Neuzner, Manuel Uphoff, Martin Mücke, Eden Figueroa, Joerg Bochmann, and Gerhard Rempe. An elementary quantum network of single atoms in optical cavities. *Nature*, 484:195–200, April 2012.

[68] N. A. Peters, P. Toliver, T. E. Chapuran, and et. al. Dense wavelength multiplexing of 1550nm QKD with strong classical channels in reconfigurable networking environments. *New J. Phys.*, 11:045012, April 2009.

[69] T. E. Chapuran, P. Toliver, N. A. Peters, and et. al. Optical networking for quantum key distribution and quantum communications. *New J. Phys.*, 11:105001, Oct. 2009.

[70] M. Razavi. Multiple-access quantum key distribution networks. *IEEE Trans. Commun.*, 60(10):3071–3079, 2012.

[71] J. R. Kuklinski, U. Gaubatz, F. T. Hioe, and K. Bergmann. Adiabatic population transfer in a three-level system driven by delayed laser pulses. *Phys. Rev. A*, 40:6741–6744, Dec 1989.

[72] Mohsen Razavi and Jeffrey H. Shapiro. Nonadiabatic approach to entanglement distribution over long distances. *Phys. Rev. A*, 75:032318, 2007.

[73] Christoph Simon, Hugues de Riedmatten, Mikael Afzelius, Nicolas Sangouard, Hugo Zbinden, and Nicolas Gisin. Quantum repeaters with photon pair sources and multimode memories. *Phys. Rev. Lett.*, 98:190503, May 2007.

[74] Nicoló Lo Piparo and Mohsen Razavi. Long-distance quantum key distribution with imperfect devices. *Phys. Rev. A*, 88:012332, Jul 2013.

[75] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy. Multiplexed memory-insensitive quantum repeaters. *Phys. Rev. Lett.*, 98:060502, Feb 2007.

[76] Xiao-Hui Bao, Andreas Reingruber, Peter Dietrich, Jun Rui, Alexander Dück, Thorsten Strassel, Li Li, Nai-Le Liu, Bo Zhao, and Jian-Wei Pan. Efficient and long-lived quantum memory with cold atoms inside a ring cavity. *Nat. Phys.*, 8:517–521, May 2012.

[77] T. Chanelière, D. N. Matsukevich, S. D. Jenkins, S.-Y. Lan, T. A. B. Kennedy, and A. Kuzmich. Storage and retrieval of single photons transmitted between remote quantum memories. *Nature*, 438:833–836, 2005.

[78] Jeyran Amirloo, Mohsen Razavi, and A. Hamed Majedi. Quantum key distribution over probabilistic quantum repeaters. *Phys. Rev. A*, 82:032304, Sept. 2010.

[79] F. Marsili, 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. Detecting single infrared photons with 93% system efficiency. *Nat. Photon.*, 7:210–214, Feb. 2013.

[80] Ryan M. Camacho, Praveen K. Vudyasetu, and John C. Howell. Four-wave-mixing stopped light in hot atomic rubidium vapour. *Nat. Photon.*, 3:103–106, Jan. 2009.

[81] A. Stute, B. Casabone, P. Schindler, T. Monz, P. O. Schmidt, B. Brandstätter, T. E. Northup, and R. Blatt. Tunable ion photon entanglement in an optical cavity. *Nature*, 485:482, May 2012.

[82] A. Amari, A. Walther, M. Sabooni, M. Huang, S. Krll, M. Afzelius, I. Usmani, B. Lauritzen, N. Sangouard, H. de Riedmatten, and N. Gisin. Towards an efficient atomic frequency comb quantum memory. *Journal of Luminescence*, 130(9):1579 – 1585, 2010.

[83] 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*, 469:512–515, Jan. 2011.

[84] A. Stute and et. al. Tunable ionphoton entanglement in an optical cavity. *Nature*, 485:4, May 2012.

[85] Mohsen Razavi and Jeffrey H. Shapiro. Long-Distance Quantum Communication with Neutral Atoms, December 2005.