DEVELOPMENT OF A POST-PROCESSING TECHNIQUE FOR A QUANTUM KEY DISTRIBUTION SYSTEM

Masters Thesis

Author:
ML Umuhire

Supervisors:
Prof. F. Petruccione
Dr. Y. Ismail

University of KwaZulu-Natal
College of Agriculture, Engineering and Science
School of Chemistry and Physics

December, 2017

A thesis submitted in fulfilment of all the academic requirements for the degree of Masters of science in the School of Chemistry and Physics, University of KwaZulu-Natal, Westville Campus.

As the candidate's supervisor I have/have not approved this thesis/dissertation for submission.

Signed

_____

Name

_____

Date

_____

Signed

_____

Name

_____

Date

_____

Preface

"In the sciences, the authority of thousands of opinions is not worthy as much as one tiny spark of reason in an individual man"

_ Galileo Galilei

"But in science the credit goes to the man who convinces the world not to the man to whom the idea first occurs."

_ Francis Darwin

Declaration

I hereby declare that this thesis, which I hand in for evaluation in the consideration of the outstanding merit of a high degree of Masters of Science, is my own genuine work and has not been presented before to any institution for evaluation purposes. Furthermore, all precautions were taken to guarantee the originality of this thesis to the best of my understanding. This thesis does comply with copyright law, and has not been taken from other authors except where such work has been referenced and recognized within the text.

Signed

_____

Name

_____

Date

_____

Publications and Presentations

Publications

- M. L. Umuhire, Y. Ismail and F. Petruccione, 2017, *Development of a post-processing technique for a quantum key distribution system*, SAIP 2017 Conference Proceedings. Submitted for Publication.
- M. L. Umuhire, Y. Ismail and F. Petruccione, 2017, *The efficient post-processing scheme for a quantum crypto system*, South African Journal of Science. In preparation.

Presentations

- Deep Learning Indaba 2017, Witwatersrand University (Johannesburg), from 10^{th} - 15^{th} September, Poster presentation "*Development of a post-processing technique for a quantum key distribution system*".

- SAIP 2017 Conference Proceedings, Stellenbosch University (Western Cape), from 3^{rd} - 7^{th} July, Oral Presentation "*Development of a post-processing technique for a quantum key distribution system*".
- Research Day 2016, University of KwaZulu-Natal, Howard Campus (Durban), 29^{th} November, Poster Presentation "*Development of a quantum key distribution system*".
- SAIP 2016 Conference Proceedings, University of Cape Town (Western Cape), from 4^{th} - 8^{th}July, Poster Presentation "*Development of a quantum key distribution system*".

Award

- Best poster presenter at The Deep learning Indaba 2017, Witwatersrand University (Johannesburg). Prize: Nividia Titan Xp.

Summer School

- *The* 25^{th} *Chris Engelbrecht Summer School in Quantum Machine Learning*, from 23^{rd} January - 01^{st} Frebuary 2017 at Alpine Health Resort, Drakensberg, KwaZulu-Natal.

Acknowledgements

My immense and sincere appreciation goes to the person who significantly contributed to the progress of this research, Professor Francesco Petruccione, for his endless support, enthusiasm, motivation, patience and mostly for his immense knowledge. His finite wisdom and guidance helped me along the way of my masters program. I could not have thought working under supervision of a such better advisor and mentor for my research.

My gratitude and respect goes to Dr. Yaseera Ismail for her consistent guidance, her passionate participation, and most of all for her hard working personage of putting me in the right direction every time the occasion presented itself.

My sincere thanks also goes to Ms. Sharmini Pillay, Ms. Betony Adams, Ms. Samkelisiwe Phekhukwayo, and Mr. Reginald Abdul for their involvement in this work. I am gratefully indebted to their precious comments. I thank my fellow colleagues for the encouraging discussions, for providing a rich, enjoyable working environment around me, and for all the fun we have had in the last two years.

Last but not least, my respect goes to my parents Innocent and Phoebe Rwahama, for putting me on this world, for their unfailing support and continuous encouragement during the period of my research and writing this thesis. This achievement would not have been possible without them.

Thank you.

Abstract

Quantum Information, Processing and Communication (QIPC) is a field concerned with technological implementations established on quantum mechanical phenomena. It is established on the concept that the action of manipulating information is controlled by the quantum physical effects. Therefore, quantum information can be characterised, quantified and processed as a physical body applying laws of quantum mechanics. QIPC consists of two major disciplines, quantum computing and quantum communication.

Communication is bound by the transfer of information. Quantum communication applies some of the fundamental features of quantum mechanics, such as, the superposition principle and the Heisenberg uncertainty principle to protect the transfer of information. One of the most advanced quantum information related technology at present is Quantum Key Distribution (QKD). It is defined as a process of encoding information into a quantum carrier in the form of single photons and distribute that information amongst legitimate entities.

Therefore, the security of the transfer of information is no longer provided by the computational complexity of a mathematical function rather by laws of quantum mechanics. The implementation of QKD requires an appropriate protocol utilising two channels namely a quantum channel and an authenticated classical channel. The quantum channel is utilised for the distribution of single photons from which a raw key can be obtained. The classical channel is used to obtain a final secret key through a process named post-processing. An experimental set up is constructed using a single photon source and free space as a quantum channel. A shared key is obtained from the quantum transmission. The main focus of this work is the post-processing procedure where the error correction protocol named Cascade is applied to locate and fix the errors detected in the shared raw key.

List of Abbreviations

ARP	Address Resolution Protocol
AES	Advanced Encryption Standard
BBO	Barium Borate Crystal (a nonlinear optical material)
DES	Data Encryption Standard
DNS	Domain Name System
IP	Internet Protocol
IR	Information Rate
LDPC	Low-Density Parity Check
MITM	Man-In-The-Middle
PNS	Photon Number Splitting

OTP	One-Time Pad
QIPC	Quantum Information Processing and Communication
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QND	Quantum Non-Demolition
RB	Redundancy Bits
RSA	Ronald Rivest, Adi Shamir, and Leonard Adleman
SSL	Secure Socket Layer
TB	Total of all Bits
UV	Ultra-Violet
XOR	Exclusive Or

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Quantum Information, Processing and Communication (QIPC) is a field of study based on how information can be computed and exchanged by applying laws of Quantum Mechanics to provide the security to the information exchange. Ideas which late gave light to QIPC, were first introduced by Claude E. Shannon as Information Theory in his two papers entitled "A Mathematical Theory of Communication "and "Communication Theory of Secrecy Systems"published in 1948 and 1949 [1, 2]. In these two papers, Shannon defined Information Theory as a science of encoding information in all sorts of symbols and transmitting it through noisy channels [1, 2]. In other words, this means information can be measured as a physical entity and can be manipulated and transmitted between two distant points.

This study is an interdisciplinary field which has seen the intersection of Mathematics, Statistics, Physics, Computer Science and Neuroscience . It can be divided into two major classes:

- Quantum Computing: the field of study which applies the laws of quantum mechanics for quantum information processing. It deals with how one can build a quantum computer and algorithms which can exploit its power [3].
- Quantum Communication: the field of study which is based on transferring quantum information (e.g. quantum states) from one place to the other [3].

Cryptography is a technique of securing communication in the presence of an adversary [4]. This technique consists of transforming a message (plain text) into an incomprehensible form called a cipher text such that if it was intercepted by an adversary, it reveals little, if not, no information about the actual message.

The first time the use of cryptography was introduced, it was only related to ensure the message was not disclosed to the unintended person by transforming messages from a coherent shape into an incoherent one and vice versa [4]. Typical example of these classical ciphers would be:

- transposition ciphers: are encoding methods which change the arrangement of letters in a message into a cipher text depending on an appropriate regular system (e.g.; 'hello world' becomes 'ehlol owrdl') [4].
- substitution ciphers: another type of encoding method which consists of shifting the position of letters upside down with other letters in a message according the order of the alphabet. Caesar cipher is a typical illustration of a substitution cipher [4].

During the modern era with the birth of computers, the objectives of cryptography go beyond privacy techniques with respect to a message to include other techniques. For example:

- checking if the message reached the receiver untouched,
- ensuring the identity of the sender and receiver,
- verifying the message content by encoding it with the sender signature,
- checking if the communication done between the sender and the receiver is authentic, and many more [5].

Modern classical cryptography is organised into two major parts: Symmetric key algorithms and Asymmetric key algorithms .

A Symmetric key algorithm involves a technique where both users (usually referred to as Alice and Bob) utilize an identical private key for encryption and decryption. This algorithm is used as either a block cipher or a stream cipher. A block cipher takes a block of a message and transforms it into a cipher text instead of transforming bit by bit at a time. A typical example of a block cipher is Data Encryption Standard (DES) or Advanced Encryption Standard (AES), first introduced by the US government [5].

On the contrary, a stream cipher constructs a random long sequence key, which is added to the plain text, one by one or letter by letter, such that the output stream is built according to the secret internal condition that evolves as the cipher performs. The secret internal condition is initially set up using a private key. An example of a stream cipher is the One-Time Pad (OTP) scheme introduced by Gilbert Vernam [5].

An Asymmetric key algorithm is another type of cryptographic algorithm where users have two different keys: a key for encrypting the message and available to the sender and the receiver and a private key used for decryption kept secret by both users [5]. Asymmetric ciphers are designed by robust computations. RSA was the first public-key cipher established by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 [5].

All these cryptographic techniques rely on either the computational security or the information theoretic security (unconditional security) [6].

The computational security describes a system which is easily deconstructed in theory by using any possible key but it requires more effort and time for an attacker to implement it [6].

The information theoretic security indicates a system where the adversary has massive technological resources but the system is still unbreakable. This is much more suitable than computational security but it is complicated to reach practically [6].

According to Claude E. Shannon [2], one can implement a system with unconditional security if the secret key is the same size as the plain text. Information Theory can be used in different ways in cryptography: to check if the system used is unconditionally secure, to establish the range of existence of the unconditional security of system, or to minimize the task decomposition of a system which is the same as a decomposition of one of its primitives (e.g. a one-way function)[2].

There exists a particular case of symmetric key ciphers that Shannon used to prove that unconditional security is possible: the One-Time Pad (OTP) encryption [7]. The use of OTP requires some basic conditions to be fulfilled:

- the secret key must be arbitrary, non repetitive,
- the secret key and the plain text(message) have the same length,
- and the secret key is used only one time and then discarded never to be used again.

When the above conditions are fulfilled, then an easy operation of encoding (like a logical XOR) will produce an unbreakable cipher text. Although an

adversary might have massive technological resources, they will not obtain any information from the seized message [7].

Both Symmetric key algorithms and the Asymmetric key algorithms are presently used worldwide for example in Internet banking and some are installed directly in physical devices such as smart cards. However, the security of these techniques can be compromised because it is only based on the computational complexity of mathematical functions [3]. With the quick growth of information technology, one will be able to build a quantum computer which can factorize large numbers then these techniques will no longer be reliable [8]. In addition, classical cryptographic techniques don't offer the possibility of Alice and Bob detecting if the communication is being tampered with, by the eavesdropper usually referred to as Eve.

In order to overcome these problems, Quantum Cryptography also known as Quantum Key Distribution (QKD) was introduced as a process of exchanging a symmetric key instead of the encoded message itself [9]. QKD is a process of encoding information in a quantum carrier, such as single photon and distribute that information between Alice and Bob , despite of the adversary's presence (Eve) [10]. The implementation of QKD is protected by laws of quantum mechanics such as:

- Heisenberg uncertainty principle: ensures that if Eve intercepts information coming from Alice, and tries to measure it, that action of measuring will introduce changes in the quantum states "disintegration of the wave function"[11] prior to reaching the intended receiver [12].

  The errors in the quantum transmission are observed in the changes of the quantum state introduced by Eve, and enable Alice and Bob to notice Eve's interference.

- No-cloning property: removes any possibility for Eve to make copy of quantum states [13, 14].

Quantum transmissions require an appropriate protocol using two channels (link), namely a quantum link and an authenticated classical link. The quantum link is applied for the quantum transmission by exchanging encoded single photons. A quantum link is any material connecting two users, (Alice and Bob) enabling light to pass through it with few losses by isolating the quantum state from any interaction with the environment. A quantum link used for the implementation of QKD can be an optical fibre or free-space. The authenticated classical link is used to compare measurements between Alice and Bob by identifying and correcting errors obtained during the quantum information. This process is called post-processing which results in a final key. An example of an authenticated public channel is a computer network, a telephone line or a radio.

1.1. Research Description

Implementations of a QKD system requires users to ensure the security and the efficiency of system against the intervention of an adversary. One aspect of a QKD system that demands additional and critical observation is the error correction process. The quantum link suffers from losses resulting from the optical fibre or even from free-space medium of the atmosphere, as well as from eavesdropping attacks. These losses introduce noise in the quantum transmission which turn out to be errors in the transmitted key. Therefore an error correction protocol is crucial to a QKD system.

In this research, we describe the steps followed to produce a final key. Our main focus is on the post-processing process where an error reconciliation protocol named "Cascade"is applied to correct errors obtained in the experiment [15].

1.2. Research Objectives

The implementation of a QKD system experiences errors due to noisy devices and potential interference of an eavesdropper. Both effects prevent the achievement of the proper quantum transmission required by an ideal QKD protocol, and lead to errors in the transmitted key.

Efficiently reconciling these errors is the primary focus of this research by applying the Cascade error correction protocol [15]. This thesis will also discuss other error correction protocols such as Low-Density Parity Check (LDPC) [16, 17], and Winnow [18] in comparison to the Cascade error correction protocol [15] in terms of effectiveness and the privacy amplification methods.

In order to achieve the aim of this work, the Cascade error correction protocol is applied to a sifted key obtained from a QKD protocol constructed through the experimental set-up. The Cascade correction protocol implemented in this work aims to identify and reconcile errors in that sifted key.

1.3. Research Questions

This thesis attempts to find answers to the following questions regarding the effectiveness of the Cascade error correction protocol:

- What is the efficiency rate of the cascade correction protocol in terms of correcting errors introduced in the shared key?
- What is the meaning of an error estimation, a quantum bit error rate and the information leakage? What impact do all these elements have in terms of the performance of the Cascade correction protocol?
- Is there any difference if an initial permutation was to be applied to the sifted key during the error correction process which involves the use of the Cascade protocol?
- Why was the Cascade correction protocol chosen for this work and not any other error correction protocol?

This thesis is structured into six chapters:

- **Chapter 1**: provides an introduction of cryptography and the difference between classical cryptography and quantum cryptography.
- **Chapter 2** : discusses quantum mechanical laws applied in the implementation of a QKD system to protect the exchange of information between users.
- **Chapter 3**: is a literature review of the key distribution process, and different protocols which can be implemented to produce a secure key. This chapter also discusses different types of schemes an attacker can use to interfere in the communication transfer.
- **Chapter 4**: describes the post-processing procedure which is performed over the classical channel and it consists of three parts. The first part involves estimating the errors in the sifted key. The second part involves the error correction process and the third part involves

the privacy amplification process. In this chapter, different error correction protocols are defined and their application for a QKD system is discussed.

- **Chapter 5**: provides a methodology used in this research to correct errors obtained in the experiment. This chapter presents the results obtained, the analysis of the cascade error correction protocol in terms of its effectiveness, its advantages, and its limitations.

- **Chapter 6**: presents the conclusion of this research and recommendations for future research outcomes.

Chapter 2

Basic Properties of Quantum Mechanics

Classical mechanics is the field of study of physical laws defining the motion of bodies resulting from the effect of a system of forces [19]. It was developed during the time of Isaac Newton, and has been applied ever since in multiple disciplines of science such as Astronomy, Chemistry, Geology, and Engineering.

Classical mechanics describes the motion of bodies at the macroscopic scale and provides accurate results. But when one needs to describe bodies at the microscopic scale, or speeds approaching the speed of light, classical mechanics fails [19]. The description of the behaviour of light is one of the downfalls of classical mechanics. For example:

- Interference and diffraction of light describe light as a wave.
- The photo-electric emission and scattering of light describe light as composed of small particles which are called photons, and each pho-

ton has a specific energy and momentum quantized depending on the light frequency. Photons appear to have a real existence similar to an electron or any other particle known in Physics [19].

Another failure of classical mechanics arises when one tries to define a model of an atom with electrons moving around the nucleus in classical orbits. Throughout such motion as any accelerated motion, electrons will lose their energy which will cause them to spiral into the nucleus. According to classical electrodynamics, the atom would not be stable but all this doesn't comply with the reality [20]. Therefore it was suitable to set up a new scheme which could describe physical phenomena on the atomic level more than classical mechanics; which is quantum mechanics [20].

Quantum mechanics provides a mathematical and conceptual structure for the development of laws of a physical system at a microscopic scale. It provides the foundation to quantum computation and quantum information. Quantum mechanics takes place in the Hilbert space $\mathscr{H}$ also defined as the state space. The Hilbert space itself is determined as a real or a complex vector space which satisfies to the inner product rule of the system. Any quantum mechanical system is defined by its state vector, which is a unit vector in the system's state space [20].

2.1. The Qubit

A simple illustration of a quantum mechanical system is a qubit which has a 2-dimensional state space. A state itself refers to a perfect representation of a physical system. The bit represents the unit of a classical information, which takes one of the two possible values, either 0 or 1. However, the unit of quantum information is represented by a quantum bit or a qubit [20].

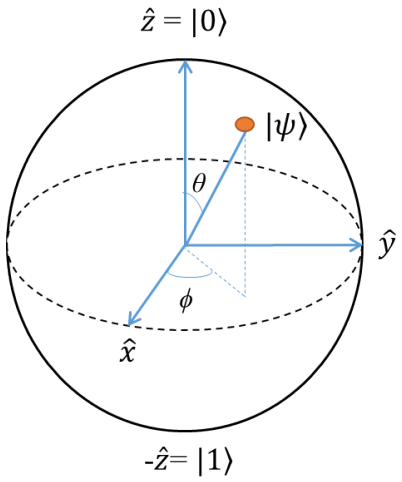

Figure 2.1. Geometric representation of a qubit.The vector $|\psi\rangle$ makes an angle with the z-axis.To determine if the state of $|\psi\rangle$, a measurement is made by using its projection on z-axis.

The Bloch sphere describes the pure state space of a qubit in a simplest form (see Figure 2.1). The wavefunction describing a qubit in a generic superposition state might collapse in one of the two eigenstates, in analogy to a classical bit that can have either one of the two possible values. However, a qubit differs from a classical bit in its ability to exist in a superposition of states. This implies that one can encode more information than a classical bit.

According to Figure 2.1, the z-axis is used as a measuring basis. The vector $|\psi\rangle$ makes an angle θ with the z-axis, and the Bloch sphere indicates that $|\psi\rangle$ is not fully in $|0\rangle$ or $|1\rangle$ state. But its projection on the z-axis will determine in which state $|\psi\rangle$ is. This means that when the measurement is performed, $|\psi\rangle$ will collapse in one of the two states.

2.2. The Superposition Principle

Consider having a state $|0\rangle$ and a state $|1\rangle$, and these two states form an orthogonal basis of a given state space. Therefore we can say that a state vector of a qubit can be defined as a combination of state $|0\rangle$ and $|1\rangle$:

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

where α and β are complex numbers. The normalization condition for state vectors requires the states vectors to be orthonormal, demonstrated by the relation $\langle\psi|\psi\rangle = 1$, therefore α and β are tied by this relation:

$$\left|\alpha^2\right| + \left|\beta^2\right| = 1\,. \tag{2.2}$$

According to the superposition principle, if a qubit has a basis of 2 states then a full system of $\boldsymbol{K}$ qubits will have a basis of $2^{\boldsymbol{K}}$ states. It is the same way for a music note having different harmonic frequencies or for light composed by multiple colours [21].

2.3. Quantum Entanglement

Quantum entanglement is defined as the level of correlation between quantum systems. Entanglement can occur between two quantum systems or more. The interesting part is that these correlations occur between quantum systems located in different places, which means any changes made on one system are simultaneously correlated with changes to the other distant system [22, 23].

Quantum entanglement is a remarkable aspect of quantum theory and has many applications, such as: quantum cryptography to produce an uncondi-

tional secure key, and quantum teleportation to transfer quantum information from point to point [22, 23, 24]. Two entangled qubits can be described by the following expression:

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(\left|H\right\rangle_s \left|H\right\rangle_i + \left|V\right\rangle_s \left|V\right\rangle_i), \tag{2.3}$$

where $|\phi\rangle$ is a Dirac notation called "a ket"and represents a column vector in Hilbert space [25]. $|H\rangle$ represents horizontal polarisation state, $|V\rangle$ represents vertical polarisation state, s and i represent signal and idler photons respectively. These qubits are in a state called equal superposition, there are equal probabilities to measure either $|H\rangle_s |H\rangle_i$ or $|V\rangle_s |V\rangle_i$ which is $\left|1/\sqrt{2}\right|^2 = 1/2$. Suppose these two entangled qubits are distant, and one each is given to Alice and Bob. If Alice measures her qubit, there are equal probabilities of obtaining either $|H\rangle$ or $|V\rangle$. Hence, Bob's measurement must be exactly the same as Alice's because of the qubit's entanglement.

2.4. The Heisenberg Uncertainty Principle

The Heisenberg Uncertainty Principle states that it is impossible to determine with definite precision the position of a particle (x) and its momentum (p) at the same time [26]. The more precisely one of these values is known, the less precisely the other value is known [26]. Let us use an example of an electron to explain this point. Consider an electron with a wavelength λ and a momentum p that satisfies the de Broglie relation $\lambda = h/p$. Then consider that electron oscillating as a sine wave and expand to infinity. Since the wavefunction of this electron Ψ has a known wavelength λ, the momentum of the electron is known [12]. But the wavefunction expands to infinity, which means the precise position of the electron is unknown even if the probability of finding the electron at a certain time and position is $|\Psi|^2$.

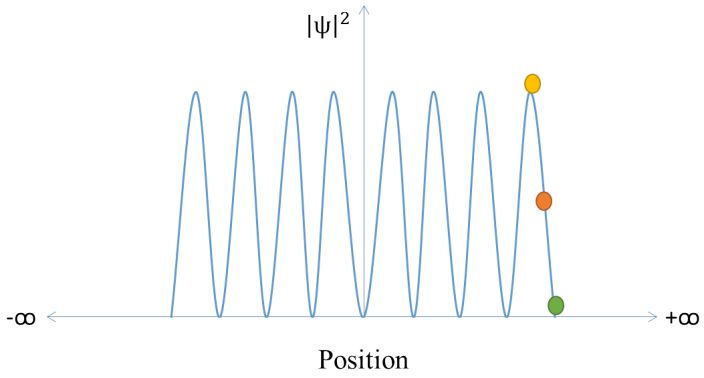

Figure 2.2. Graph of probabilities $|\Psi|^2$ in terms of position of an electron. This graph indicates that the electron has a high probability of being in the yellow coloured region, or it has medium probability of being in orange coloured region and a low probability of being in the green coloured region [27].

Heisenberg defined the product of the uncertainty in measurement of position $\triangle x$, and the uncertainty in measurement of momentum $\triangle p$ to be approximately greater than Planck constant h. Therefore we have the mathematical relation:

$$\triangle x \,.\, \triangle p \geqslant \frac{\hbar}{2}\,, \tag{2.4}$$

where $\triangle x$ and $\triangle p$ are not the range of the value of x and p, but rather the range within one standard deviation of those values and $\hbar = \frac{h}{2\pi}$. This principle is used in the implementation of a QKD system in such a way that for an adversary to obtain information from the key distribution process, they intercept photons coming from the sender, corrupt the state of those photons by performing the measurement, and resend the photons to the receiver. This action of measuring introduces changes in the state of photons which will leave a trace in quantum transmission. Therefore, the adversary's activity is noticed by Alice and Bob.

2.5. The No-Cloning Theorem

Another pillar of QKD is the no-cloning theorem which is used to prevent the adversary from making a copy of a quantum state while keeping the original state unchanged [28].

Consider an instrument which can transform the state $|H\rangle$ into $|HH\rangle$ and the state $|V\rangle$ into $|VV\rangle$ where these symbols stand for arbitrary states. Let us consider what will happen if we introduce into that instrument a linear combination :

$$|L\rangle = \alpha\,|H\rangle + \beta\,|V\rangle\ . \tag{2.5}$$

Since quantum mechanics respects linearity properties, the output for their superposition have to be the superposition of the output:

$$|M\rangle = \alpha\,|HH\rangle + \beta\,|VV\rangle\ . \tag{2.6}$$

We expected to get the original and the copy:

$$|L\rangle\,|L\rangle = (\alpha\,|H\rangle + \beta\,|V\rangle)(\alpha\,|H\rangle + \beta\,|V\rangle)\,. \tag{2.7}$$

But this is not the outcome we get with the state $|M\rangle$. In conclusion one cannot make a perfect copy of an unknown state without having any knowledge of it in advance [25, 28]. An important aspect of this theorem is that any adversary who tries to make a copy of a quantum state, performs a measurement which introduces an error in the quantum transmission.

Chapter 3

Quantum Key Distribution Process

Quantum key distribution (QKD) is a procedure of concealing information in a quantum carrier such as a single photon and distributing that information amongst legitimate users [29]. The goal of QKD is only to securely generate and exchange the key amongst legitimate users. Thereafter, this key is used with any encryption algorithm to conceal information distributed over the classical link. This process is secure because it does not compromise the message content and it also provides Alice and Bob the possibilities of detecting Eve's presence.

QKD is comprised of two parts. The first part is performed through the quantum link. It consists of the exchange of quantum information between Alice and Bob and also performing measurements implemented by Bob. The second part is performed through the classical link and it consists of three steps as shown in Figure 3.1. The first step is error estimation which allows users to calculate the percentage of errors introduced during the quantum transmission.

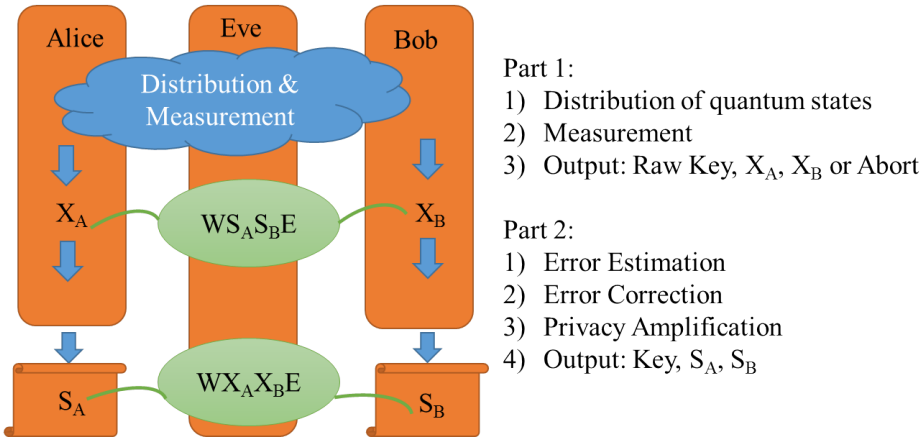

Figure 3.1. The Quantum Key Distribution Process is performed between Alice and Bob. Eve is an adversary who is trying to interfere in the communication between Alice and Bob. QKD consists of two parts where the first part starts with sharing quantum states between Alice and Bob thereafter they perform measurements which yields to a raw key. The second parts Alice and Bob analyse the raw key by performing the sifting process, error correction and privacy amplification which yield to a secret key [30].

The second step is error correction which enables Alice and Bob to reconcile errors in the transmitted key. The last step is privacy amplification and it is performed in order to minimise the information an adversary could have obtained during the quantum distribution process and error correction process [29].

The concepts of QKD were introduced in 1970's by Stephen Wiesner, in his seminal paper entitled "Conjugate coding"[31]. According to Wiesner, it is possible to store or to send two encoded messages using "conjugate variables"such as linear and circular polarised light in such a way that only one could reach the intended receiver and be transformed into the original message [10, 31]. In other words, if the linear polarisation is observed or measured, all chances of measuring the circular polarisation is lost. It was later that Charles H. Bennett and Gilles Brassard introduced the first QKD protocol named BB84, (respective to their surnames Bennett, Brassard and

the year of publication 1984) which uses Wiesner's idea of superposition of states [10].

QKD can be implemented with any particle such as ions, electrons, atoms, and spin. However, photons travelling at the speed of light have proven to be suitable for the task. Therefore, the quantum states of light can be sent over long distances [22].

3.1. Quantum Key Distribution Channels

The meaning of communication may be regarded as a transfer of information between two distant points. Therefore, whenever information is exchanged over any distance, a communication conveyor is always needed [32]. For the operation of a QKD system, a quantum link such as an optical fibre or free-space is required as well as a classical link such as a radio or a computer network.

The use of a quantum link for the operation of a QKD system serves in the transmission of quantum information (e.g. states) while the use of a classical link serves for the distribution of classical information. That is where users find the percentage of error introduced in the quantum transmission, and how to correct those errors and to minimise the information Eve could have obtained.

3.1.1. Optical Fibre Links

An optical fibre is a narrow, long glass cylinder with specific properties to carry light from one end of the fibre to another [32]. An optical fibre is made of the core, the cladding and the buffer.

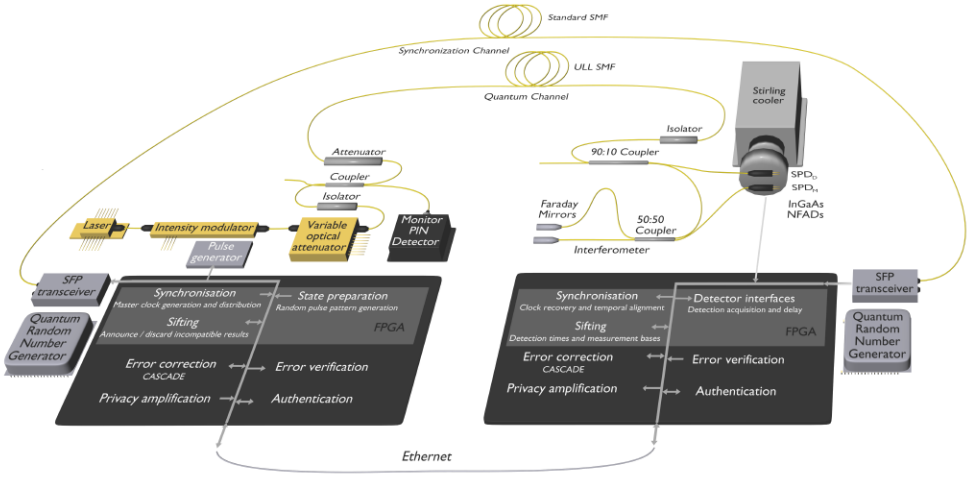

Figure 3.2. Implementation of COW protocol using an optical fibre of 307 km long as a quantum link [33].

The core is made of glass and has a higher index of refraction than the cladding. The cladding on the other hand is made of plastic material and has a lower index of refraction than the core. The boundary between the core and the cladding acts as a mirror to keep the light contained even when the fibre bends around corners. The buffer is used for the protection of the fibre [32].

The implementation of a QKD system might require the use of optical fibres as quantum links to transfer single photons from Alice to Bob. A typical example is shown by Figure 3.2 where a secret key was obtained by implementing the Coherent One-Way (COW) protocol using optical fibre as a quantum link for a distance of 307 km [9, 34, 35].

Long distance communication using optical fibres as channels suffer from the effects of signal loss and decoherence. In classical communication, amplifiers are used to fortify the signal during long distance transmission, however in quantum communication amplifiers cannot be used because they go against

the no-cloning theorem [13, 14]. The use of optical fibres as quantum link has some limitations. For example, losses of light energy, absorption, depolarisation errors and many more are observed as the size of the link increases [36]. The state of the photon or the photon itself cannot be conserved if the link is longer, hence the bit rate is reduced [36].

3.1.2. Free-Space Links

Although free-space links work the same as optical fibre links, the former depends on line of sight between users instead of connection by an optical fibre [22, 37, 38]. Free-space links typically support higher transmission rates than optical fibre links and do not face the polarisation scrambling caused by optical fibre [29].

Free-space links use telescopes or even space links such as astronomical telescopes for global scale. For polarisation encoding specific, losses are insignificant in the atmosphere therefore, the implementation of a QKD system using free-space channels offer a more promising approach [38, 39]. Figure 3.3 shows how an entangled pair of photons was created and distributed over a 144 km free-space channel [24].

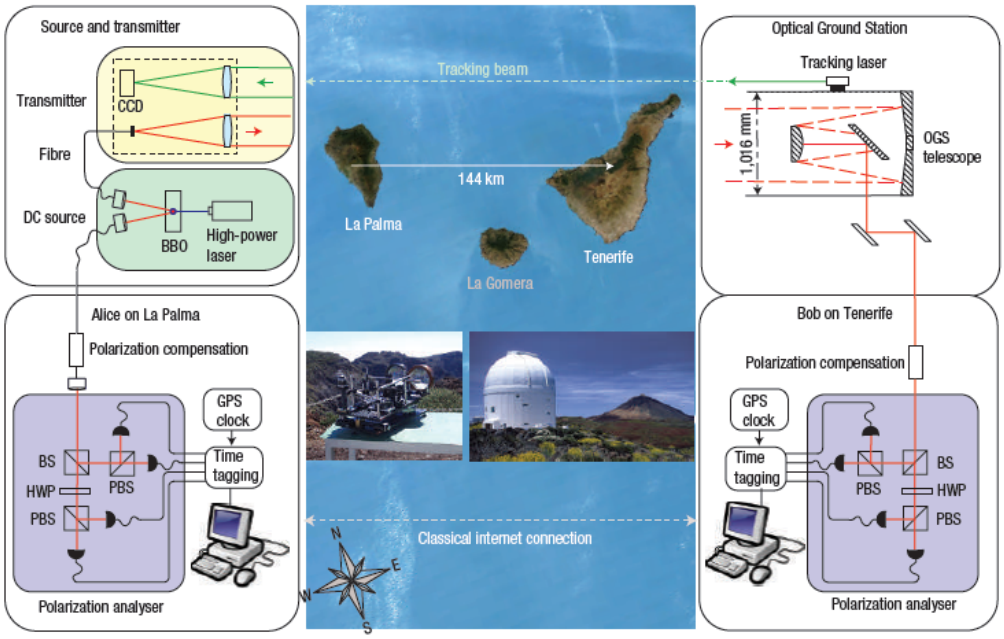

Figure 3.3. The implementation of quantum key distribution where entangled photons were exchanged between two islands using a free-space link of 114 km long. The picture was taken from a satellite [24].

Entangled photons and entanglement swapping offer a suitable solution to overcome losses or errors encountered at long distance in optical communication. Therefore, instead of exchanging an entangled photons throughout the entire distance, quantum repeaters are used to allow the quantum teleportation of a pair of entangled photons at long distant nodes [36]. The long quantum link might be tens or hundreds of kilometres and it is divided in shorter segments connected to each other. At each segment, entangled pair of photons is created.

For example, between the system $|A\rangle$ and $|R_a\rangle$ the entangled state is constructed, and between $|R_b\rangle$ and $|B\rangle$ another entangled state is constructed [40]. These initial entangled states can be easily obtained by using parametric down conversion process . To construct entangled state between $|A\rangle$

and $|B\rangle$ a Bell measurement is performed on $|R_a\rangle$ and $|R_b\rangle$ and the quantum state of $|R_a\rangle$ is teleported onto $|B\rangle$ even if particle $|A\rangle$ does not interact with particle $|B\rangle$, they become entangled [41]. This is called entanglement swapping and it is a simple procedure such that $|A\rangle$ and $|B\rangle$ are now entangled at long distances. Therefore, a network of such as repeaters can be used to establish entanglement over long distances [40].

3.1.3. Classical Links

As we have mentioned before, the implementation of QKD requires users to be linked by the quantum link and the classical link. A classical link (usually called a public channel) is a communication link used to exchange classical information between users. Although this classical link is not completely secure, the operation of QKD requires the classical link to be authentic. This means that Eve is aware of the exchange of information between Alice and Bob but there is no interference on her part. Otherwise Eve might impersonate Bob in order to tamper with the information. An example of a classical link can be a telephone line, a computer network or a radio.

3.2. Quantum Key Distribution Protocols

There exist many different protocols which can provide a secure key. The implementation of these protocols applies the Heisenberg uncertainty principle [12] and the No-cloning theorem to protect the quantum transmission from the interference of an eavesdropper [23].

In 1984, the first QKD protocol was implemented and given a name of BB84 according to the surnames of the authors and the year when it was introduced [29, 35]. This protocol is still one of the most famous and widely

used protocols. The qubit based protocols require their implementation to be based on the exchange of one single photon or qubit from Alice to Bob. Other protocols introduced after the BB84 protocol such as B92 [42], E91 [43], SARG04 [44, 45] and COW [46], which will be discussed below, are the modification of BB84 for the purpose of improving the security of QKD [29, 35].

The principle of these protocols is based on the transmission of a random chain of bits from Alice to Bob by encoding the bits into photon polarisation states. Let us note here that bits are sent one by one [10, 29]. The implementation of these protocols also guarantees the detection of any eavesdropping interference. Any interference of Eve is revealed by the errors noticed in the key string received by Bob.

3.2.1. BB84 Protocol

The BB84 protocol is implemented by using two bases: a rectilinear basis (+) and a diagonal basis (×) which correspond to four photon polarisation states [10, 29, 35]. Alice generates a random chain of bits with value 0 or 1. Prior to the quantum transmission, each photon polarisation state is assigned a corresponding bit value according to the basis used [10, 29, 35]. Figure 3.4 illustrates how this process is performed.

Alice transmits bits to Bob one by one through the quantum link and every time she does that, she records the time, the state and the basis of each photon sent [10, 29, 35]. Figure 3.4 describes how the vertical and horizontal polarisation states encode the quantum bit of value 0 and 1 respectively and the -45^0 and $+45^0$ polarisation states encode 0 and 1 respectively.

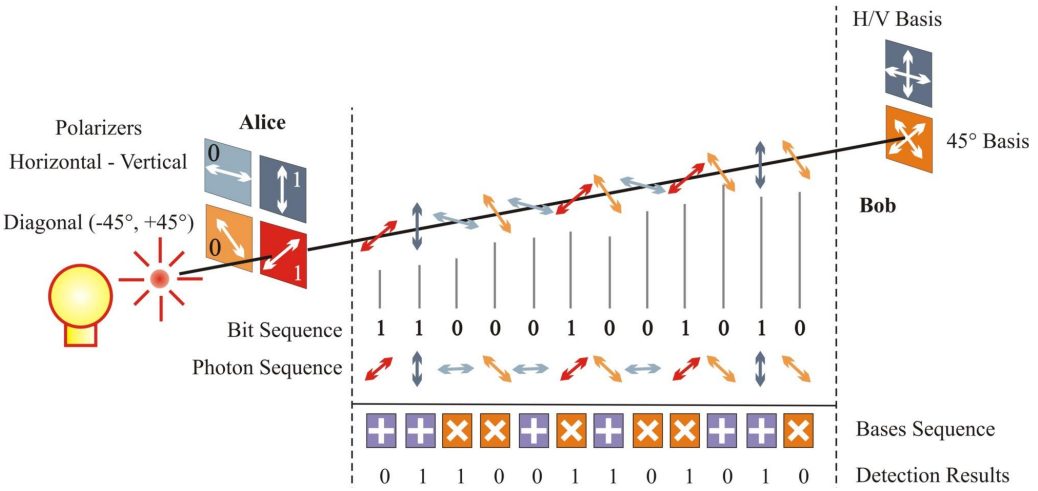

Figure 3.4. The BB84 protocol for Raw Key Exchange. According to this figure, if Alice sends a bit of value 0 in the rectilinear basis, it is encoded in vertical polarisation state and if she sends a bit of value 1 in the diagonal basis,it is encoded as $+45^0$ state, so on and so forth [47].

Bob on the other end doesn't know the encoding of each incoming photon. All he does is selecting a random basis in which the measurement is performed, either rectilinear or diagonal. During this process Bob records the time, the basis and the result of each incoming photon he received [10, 29, 35].

After the quantum transmission, Alice and Bob perform what is called sifting. It is the step where they compare their results and leave out the bits where they both have applied different bases. The shared key becomes the remaining bits where Alice and Bob used the compatible bases.

According to Table 3.1, the implementation of the BB84 protocol gives Alice and Bob 50% probability of measuring the photon using compatible bases and 50% probability of measuring the photon using incompatible bases.

Table 3.1. Illustration of the key sifting stage for the BB84 protocol

Bits of Alice	0	1	1	0	1	0	0	1
Bases used by Alice	+	+	×	+	×	×	×	+
Polarisation of Alice	↑	→	↘	↑	↘	↗	↗	→
Bases used by Bob	+	×	×	×	+	×	+	+
Public discussion								
Shared key	0		1			0		1

Alice and Bob now randomly select a sample of bits in the shared key and reveal their values in order to calculate the percentage of errors obtained in the quantum transmission. If there is no error, the shared key has to be similar for Alice and Bob which means there is no interference from Eve. Then the shared key becomes the secret key [10, 29, 35]. In the presence of the errors, Alice and Bob perform the post-processing procedure which will be discussed in the next chapter.

3.2.2. B92 Protocol

The B92 protocol is a modification of the BB84 protocol. It uses two photon polarisation states, but they are non-orthogonal quantum states [42]. The author of this protocol concluded that only two quantum polarisation states were needed, unlike the four states used in the BB84 [42].

Figure 3.5 illustrates how the B92 protocol was implemented using free space as a quantum link [48]. The quantum transmission process of the B92 protocol goes as follows: Alice randomly selects one of her bases with a bit value corresponding to that basis. Alice also selects one of her photon polarisation states for the encoding of the bit, according to the basis chosen and the bit value. Thereafter, she transfers the encoded bit to Bob.

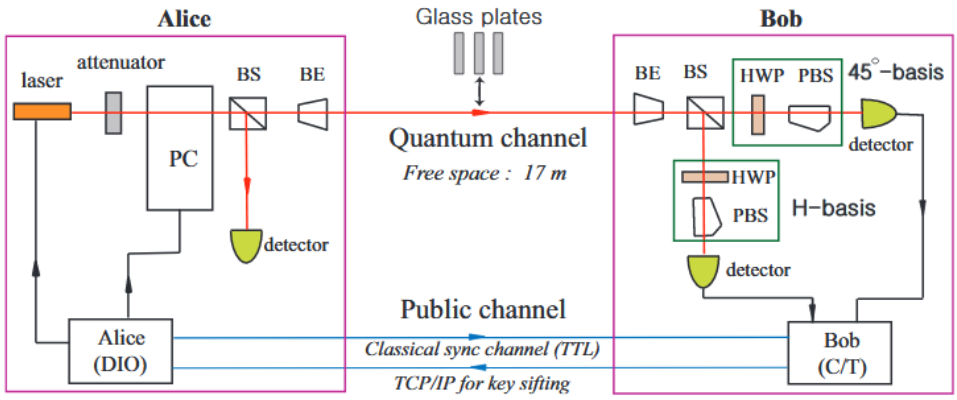

Figure 3.5. The description of the B92 protocol. This figure describes how the B92 protocol was implemented using free space as quantum link of 17 m long [48].

Bob on his side has two techniques of identifying the incoming photons, either he will get a "detection"on the photon detector of H - basis or "no detection"on the other photon detector 45^0 - basis [42, 48].

Bob has a probability of detecting a photon equal to 1/2 when his polariser is not orthogonal with one of Alice's. These instances are explicit as they occur when the polarisation settings of Alice and Bob were not orthogonal hence, their bit values were both 1 or 0 [42].

There exist other instances when Bob detects no photons. These instances are called ambiguous. They occur when Bob's polariser was orthogonal to Alice's or not but still Bob failed to detect a photon with 1/2 probability [42] as illustrated in Table 3.2.

Table 3.2. Illustration of Key Sifting Stage for B92 Protocol

Alice's bit string	1	0	1	0
Alice's polarisation	45^0	0^0	45^0	0^0
Bob's polarisation	-45^0	-45^0	90^0	90^0
Bob's bit string	0	0	1	1
Bob's bit detection	No	No	Yes	No

During the key sifting stage, Bob uses the public channel to reveal the time when he obtained a detection, but not the exact result. Therefore 25% of the bits are successful and 75% are unsuccessful and discarded [42]. The second column of Table 3.2 shows that Bob failed to detect a photon while his polarisation settings are not orthogonal with Alice's.

3.2.3. SARG04 Protocol

The SARG04 protocol was introduced after noticing some weaknesses of the BB84 protocol when exposed to the photon number splitting attacks (PNS) which are performed by Eve over the quantum link [44]. The different attacks that Eve might perform to tamper with the communication of Alice and Bob are discussed later on in this chapter [49]. The SARG04 protocol functions as the BB84 protocol but has proven to be strong to oppose the PNS attacks. It uses four non-orthogonal quantum states for key transmission. There is another version of the SARG04 protocol which applies an entanglement approach [45].

The functioning of SARG04 is the same as BB84 on the quantum scale: Alice uses one of her four photon polarisation states to encode the bits and send them to Bob [44]. Then Bob arbitrarily chooses one of his two particular filters α_y and α_x to detect the incoming photons. But the radical changes are observed at the encoding and decoding stage [44].

During the encoding stage, Alice uses two states to encode one bit. In other words, bits are encoded in the bases since two states constitute one basis. For example, both states $|+y\rangle$ and $|-y\rangle$ conceal the bit 0 and both states $|+x\rangle$ and $|-x\rangle$ conceal the bit 1 [45].

Given the four sifting sets are the four non-orthogonal photon polarisation states used to send the bits in:

$$\begin{cases} A_{++} = \{|+y\rangle, |+x\rangle\}, \\ A_{--} = \{|-y\rangle, |-x\rangle\}, \\ A_{+-} = \{|+y\rangle, |-x\rangle\}, \\ A_{-+} = \{|-y\rangle, |+x\rangle\}, \end{cases} \quad \text{where} \quad \begin{cases} |+y\rangle = |0\rangle\,; \\ |-y\rangle = |1\rangle\,; \\ |+x\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,; \\ |-x\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\,. \end{cases}$$

If Alice sends $|+y\rangle$, then she announces $|+x\rangle$, so in this case for Bob to guess correctly he has to measure α_x and find $|-x\rangle$. However, if he measures α_y and finds $|-y\rangle$, then he would have guessed incorrectly [45]. In the absence of errors, the size of the key resulting from the sifting stage is $\frac{1}{4}$ of the raw key, but in the presence of the errors this size is greater [45]. Errors in the quantum transmission can be caused by:

- depletion of photons in the quantum link,
- the transformation of the state by Eve,
- or dark counts at the receiver's station.

The SARG04 protocol offers almost the same security as the BB84 protocol in terms of single photon transmission. The performance of SARG04 protocol becomes less than the one of the BB84 protocol in presence of losses. However, in the presence of PNS attacks, the SARG04 protocol has proven to offer better security than the BB84 protocol [44].

3.2.4. E91 Protocol

In 1991 Artur K. Ekert introduced a protocol which uses entangled states. Later on, this protocol was named E91 referring to its founder surname and the year in which it was introduced [43]. The entangled pair of photons used to implement this protocol, can be created either by Alice, or by Bob. The pair of entangled photons can also be created by a source distant from both of them, including Eve. The quantum transmission is done in such way that each user has one photon from each pair [43]. The objective of this protocol is to detect the activity of an eavesdropper by using Bell's inequalities [43]. Ekert designed the protocol with a source emitting pairs of spin particles in singlet states:

$$\phi = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle \ . \tag{3.1}$$

The entangled pair of photons is created by the spontaneous parametric down conversion process observed when the light passes through a non-linear crystal such as a BBO crystal which is able to split the UV light into two entangled photons one called the signal and the other one called the idler with a wavelength twice that of the source as shown in Figure 3.6.

In the case of using the BBO crystal type II as illustrated in Figure 3.7, if Alice and Bob use consistent bases and Alice measures a particle with spin up, Bob measures a particle with spin down with 100% probability. The same if Alice measures a particle with spin down, Bob detects a particle with spin up with 100% probability [43]. Things will be different if Alice and Bob apply inconsistent bases to detect their particles. For example, if Alice measures a particle with spin up in the 45^0 basis, there exits an equal probability of Bob to measure a particle with spin up or down in the 90^0 basis [43].

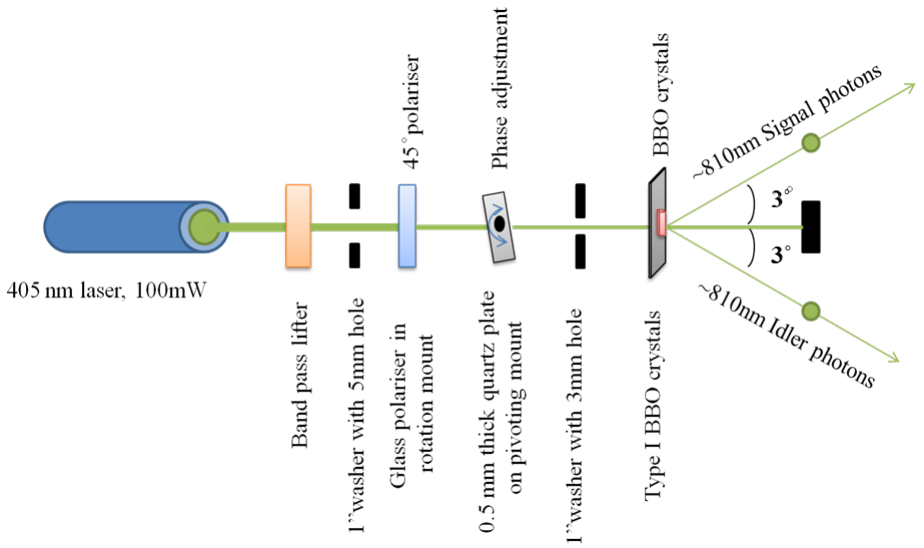

Figure 3.6. Creation of entangled photons. The light at the source has a wavelength of 405 nm, after passing through the BBO crystal, two entangled photons are created with a wavelength of 810 nm each [27].

The implementation of QKD using the process of quantum entanglement takes place as follows: neither Alice nor Bob control the source or the encoding. If Alice receives a photon and performs a measurement on it, this instantaneously influences Bob's outcome [43].

Figure 3.7 indicates how entangled photons A and B are created when the light hits the BBO crystal. Bob will measure a photon B with vertical or horizontal polarisation state. Some part of the light which goes through the BBO crystal is reflected back and creates photons C and D again at the BBO crystal. The photon D goes to the detector and indicates the photon to be teleported exists. Alice will check the coincidence counts on her two detectors.

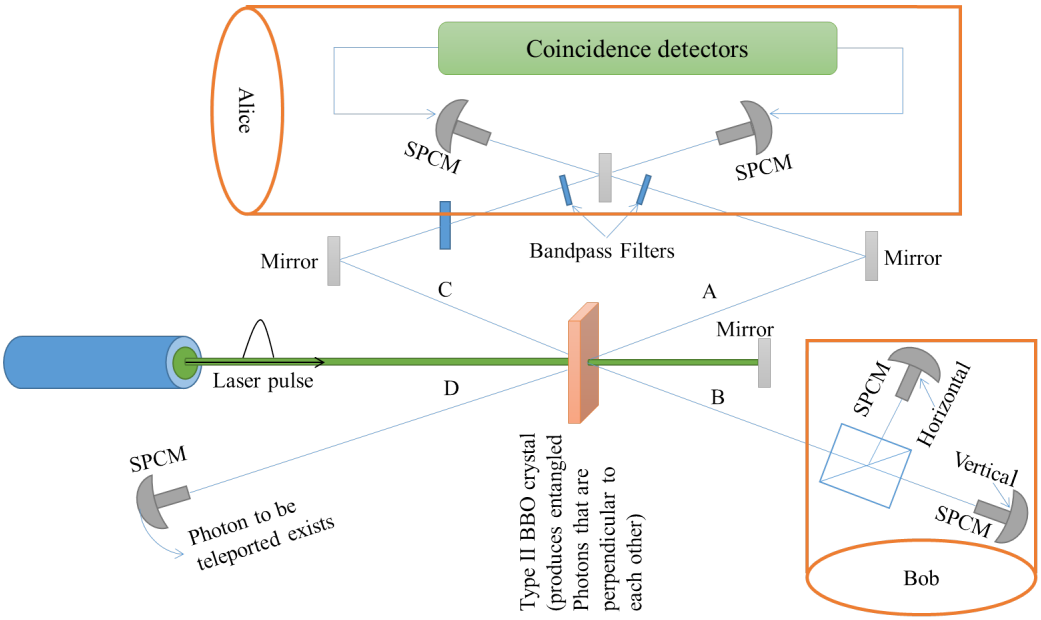

Figure 3.7. Illustration of the E91 protocol using quantum entanglement scheme. Two entangled photons A and B are produced after the light passes through the BBO crystal. Photon B goes to the detectors at Bob's side be be measured. Photons A goes to Alice to allow her to measure coincidence counts. There is a portion of the light which is reflected back to the BBO crystal after Photon A and B are produced. This light will produce two entangled photons C and D. Photon C goes to Alice to be enable her to observe coincidence counts. D is measured locally to ensure the process was perfect [27].

Continuum based protocols

These protocols use coherent states for the quantum transmission process. The quantum states are obtained when the intensity of the laser output gives a single pulse. Normally the quantity of photons in one single pulse is random but the implementation of these protocols requires for the quantity of photons in one single pulse to be an average number [35].

3.2.5. Coherent One-Way Protocol

The Coherent One-Way (COW) protocol is a recent protocol for quantum key distribution introduced by Nicolas Gisin *et al* in 2004 [46].

The implementation of the COW Protocol is performed by encoding logical bits in time. The protocol is constructed with a small number of standard telecom tools [46, 50, 51].

Alice sends a continuous sequence of pulses where this sequence can be divided into two sets and in each set the logical bit of information can be at the start, $\mu - 0$ for a logical "1"or the logical bit of information can be at the end $0 - \mu$ for a logical "0"[50, 51]. The implementation of the COW protocol is shown in Figure 3.8.

For the detection of eavesdropping activity Alice sends decoy sequences $\mu - \mu$. Bob uses the data line to get the raw key by measuring the time each photon reaches the detector D_B. The security of the protocol is checked when Bob arbitrarily determines if there is any constructive or destructive interference with the interferometer and detectors D_{M1} and D_{M2}.

Bob always gets constructive interference in D_{M1} whenever the direction of the beam from the laser and the phase of the interferometer are well positioned. But if Bob detects destructive interference in D_{M2} this means there is a loss of coherence therefore, the presence of an eavesdropper is revealed. In this kind of situation, users have to reject the key in order for the information to be kept hidden [46].

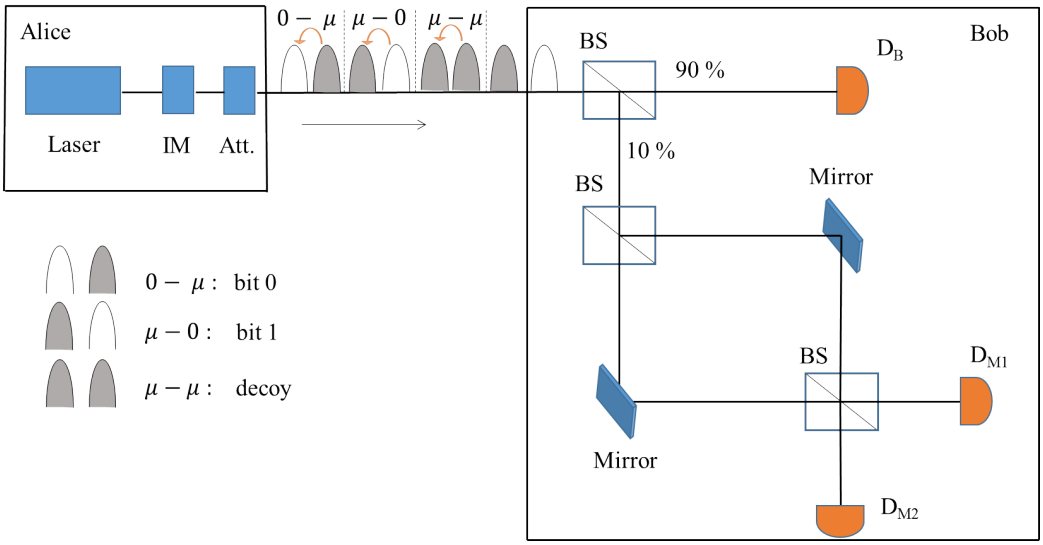

Figure 3.8. Scheme of the COW protocol. The raw key is obtained from the data line by measuring the time arrival of photons on D_B. To check for the interference of Eve, Bob uses the monitoring line by detecting the pulse coherence with the interferometer and the detectors D_M. The symbol IM stands for the intensity modulator, Att. stands for the attenuator and BS is the beam splitter [46]

.

The sifting process is done by Bob identifying detections he received in the detector D_B in time slot i and i+2 and assigning them the bit value 0. The bits Bob received in the detector D_M in time slot i and i-2, he assigns the bit value 1. Thereafter, Bob reveals the results he obtained and if the results agree with what Alice sent, they keep the bits, otherwise they discard the incompatible bits. Therefore, the bits used for decoy sequences are also discarded. The COW protocol has been proven to resist PNS attacks and even the intercept-resend attack introduced by an eavesdropper [46, 50, 51].

3.3. Eavesdropping Attacks

As mentioned earlier, imperfection in the equipment used in the implementation of a QKD system introduce errors in the quantum transmission. Errors are also introduced by the activity of an eavesdropper. In the following paragraphs, we examine some of the strategies used by an adversary to obtain information from the quantum transmission.

3.3.1. Intercept-Resend Attack

An intercept-resend attack is a simple strategy used by Eve by capturing each incoming photon from Alice's station and measuring it using one of her bases. Afterwards, Eve sends a new photon to Bob depending on the result obtained in measuring the photon coming from Alice as illustrated in Figure 3.9.

This attack is classified as one of individual attacks performed by Eve, occurring when single photon transmission is involved [35]. If Eve uses the same basis as Alice there will be no error in Bob's measurement and her presence will not be detected.

But each time Alice sends a qubit to Bob, she randomly chooses the basis. Which means there is a high possibility of Eve using the wrong basis for measuring the incoming photon, hence Bob will have errors in his string bit even if he uses a compatible basis as Alice to measure photons he gets from Eve [35].

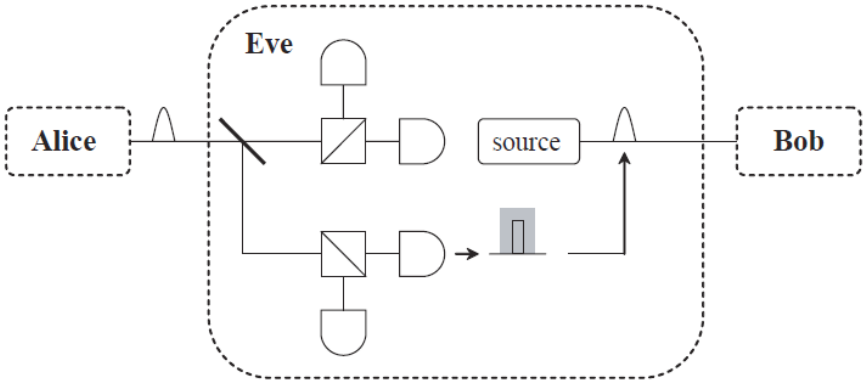

Figure 3.9. Illustration of the intercept-resend attack performed by Eve over the quantum link [52].

Assuming the implemented protocol was BB84, the probability of Bob getting the right result is 50% as for Eve, she get the right basis with 50% probability. These outcomes will induce the error rate of 25% which is more than the failure threshold for this protocol, hence the presence of Eve is noticed. To overcome this problem, Alice and Bob reject the key and start again with the quantum transmission process [35].

3.3.2. Photon Number Splitting Attacks (PNS)

Let us assume Alice and Bob are performing a single photon transmission using the BB84 protocol. The laser used to produce photons is attenuated so that it gives a single photon per pulse. Practically, the pulse sent from Alice to Bob might contain more than one photon [49]. This attack is demonstrated in the Figure 3.10.

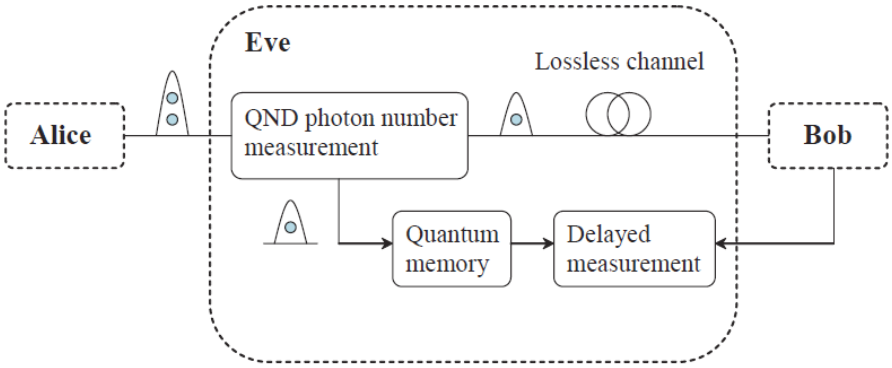

Figure 3.10. Illustration of the photon number splitting attack executed by Eve over a quantum link [52].

In the cases of multi photon transmission, Eve performs what is called a polarisation splitting operation or an active arrangement of beam splitters alongside with quantum non-demolition (QND) measurements, then she detains one photon and the remaining ones are sent to Bob. These techniques performed by Eve will not modify the state of the photons reaching Bob, instead they will enable Eve to have full knowledge of the quantum transmission process without revealing her presence [49].

Therefore for each pulse sent containing more than one photon, Eve will gain full information without introducing error in the sifted key. These types of attacks get worse if users are operating with a high lossy quantum link, because Eve might be able to substitute the quantum link with a perfect one. Hence, she can control the signal Bob receives [49].

To overcome these kinds of situations, researchers proposed the SARG04 protocol to fight against PNS attacks. As mentioned earlier, this protocol is implemented using attenuated laser pulse and four non-orthogonal states unlike the BB84 protocol [44]. Another protocol built to overcome PNS attacks is the COW protocol, it is executed in such a way that the encoding

of bit is done in time. This protocol is constructed in a simple way allowing Alice and Bob to have a secure quantum transmission as well as to detect the presence of Eve [46].

3.3.3. Trojan-Horse attacks

The Trojan-Horse attack consists of Eve introducing a brighter light into Alice's settings. Eve will measure the back reflection of that light, enabling her to get all the information about the polarisation or phase modulator which are responsible for the encoding of the bits; if the BB84 protocol is the one being implemented [35, 53].

To prevent this, it is recommended to put a monitoring line at Alice's station which controls incoming light and gives a notification to Alice every time Eve introduces such a pulse. Alice and Bob can also insert an optical isolator into their set-ups to prevent that incoming brighter light [35, 53].

3.3.4. Man-in-the-Middle Attacks

Although we mentioned that Eve cannot interfere with the conversation of Alice and Bob over the public link as long as this channel is authentic, Alice and Bob might fail to authenticate this channel. Therefore, Eve will be able to impersonate both of them and obtain crucial information without Alice and Bob realising it. This type of eavesdropping strategy is called the man-in-the-middle (MITM) attack a illustrated in Figure 3.11. It consists of Eve introducing malicious software through the classical channel and intercepting information shared between Alice and Bob [54].

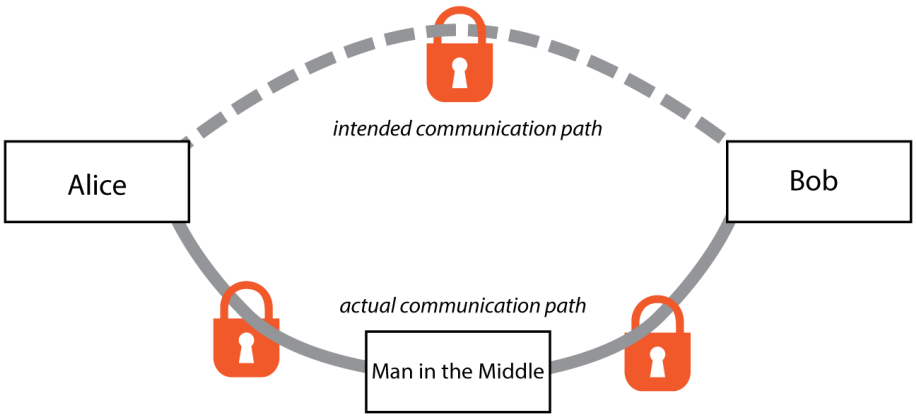

Figure 3.11. The man-in-the-middle attack [55].

MITM attacks are caused by Address Resolution Protocol (ARP), Cache Poisoning, Domain Name System (DNS) Spoofing, Session Hijacking, and Secure Socket Layer (SSL) Hijacking. Assume Eve can create fake messages and send them to Alice, for example, Eve can ask Alice her Internet Protocol (IP) address by pretending to be Bob. Alice will reply to Eve thinking that the message was sent by Bob. Eve will do the same to Bob, then all the network traffic will be controlled by Eve and she will be able to get all the information she needs [54].

MITM attacks is also observed when a client is trying to be connected to the server while the attacker has created a fake web page which will give wrong information. Every time a client opens a web page, a DNS request is sent to the server of that web page. Therefore, the client to be connected to the website, a reply has to come from that same server. If the attacker was able to get the identification number related to DNS request and the reply, the attacker will use ARP Cache Poisoning to direct the client to a fake web page and the client will lose the important information [54].

This attack can be observed when a client opens a website and is required to provide a user name and password for authentication and to establish a network session. As long as the session is still open, the attacker might intercept all private information of the client.

In conclusion, MITM attacks occur when users fail to strongly authenticate the classical channel they are using for communication. MITM attacks might also happen when one is connected to an untrustworthy communication network.

Chapter 4

Post-Processing

The quantum transmission through optical fibre or in free-space suffers from the interference of an eavesdropper introduces errors in the system. The errors can also be caused by noise in the equipment. To overcome that, users have to discuss over the classical channel which technique to apply for the correction of those errors [56]. The post-processing procedure is composed of three steps: the first step is called error estimation. It involves finding the percentage of wrong bits in the sifted key. The second step is error correction and it involves in removing the wrong bits in the sifted key. The third step is called privacy amplification and its goal is to minimize information leaked to a small arbitrary value. This work only focuses on the two first steps of post-processing: error estimation and error correction.

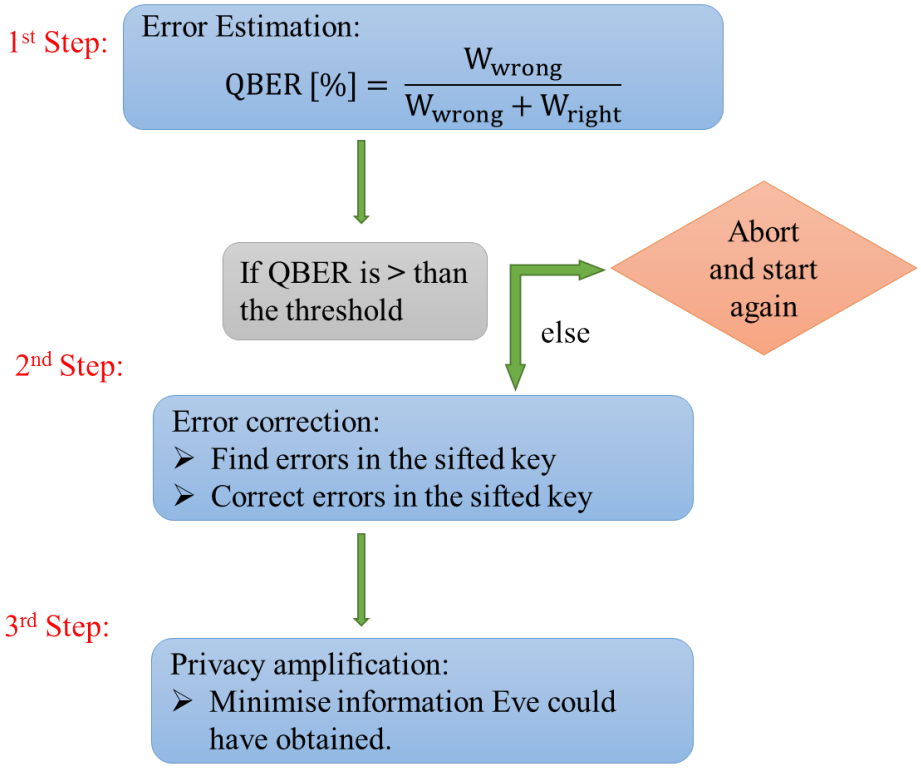

Figure 4.1. Illustration of the different steps which constitute the post-processing operation.

4.1. Error Estimation

As mentioned before, the error estimation involves finding the percentage of errors committed during the quantum transmission. Therefore, Alice and Bob calculate the Quantum Bit Error Rate (QBER).

Quantum Bit Error Rate

The quantum bit error rate is given by the quotient of the erroneous bits to the total number of bits in the sifted key and it is always expressed as

a percentage [35]. The value of the QBER varies according to the protocol implemented:

$$\mathrm{QBER} = \frac{\mathrm{W_{wrong}}}{\mathrm{W_{right}} + \mathrm{W_{wrong}}} = \frac{\mathrm{R_{error}}}{\mathrm{R_{sift}} + \mathrm{R_{error}}} \approx \frac{\mathrm{R_{error}}}{\mathrm{R_{sift}}}, \tag{4.1}$$

where $\mathrm{W_{wrong}}$ represents the total of the wrong bits and $\mathrm{W_{right}}$ represents the total of the right bits. $\mathrm{R_{error}}$ stands for the total of erroneous bits and $\mathrm{R_{sift}}$ stands for the total of bits after the sifting process. The equation 4.1 is represented as a ratio, to express it as a percentage, it is multiplied by 100.

The calculation of the QBER goes as follows: Alice randomly select a sub-string of the key and sends Bob the corresponding bits and their values. Bob compares this sub-string to the corresponding one in his sifted key and reveals the result [35]. This sub-string is used to calculate the QBER and its bits are discarded.

There exists an alternative method Alice and Bob may use to calculate the QBER. They calculate the QBER for each basis used. With this method, the key rate is increased and the number of times where the incompatible bases were used is decreased [57].

The bits disclosed by applying the second method are also discarded but the errors introduced by Eve are easily detected [35]. The QBER is an important feature for the implementation of a QKD system. It determines the security and the efficiency of the system, and also reveals the existence of an eavesdropper and how much information they have learnt from the key as shown in Figure 4.2.

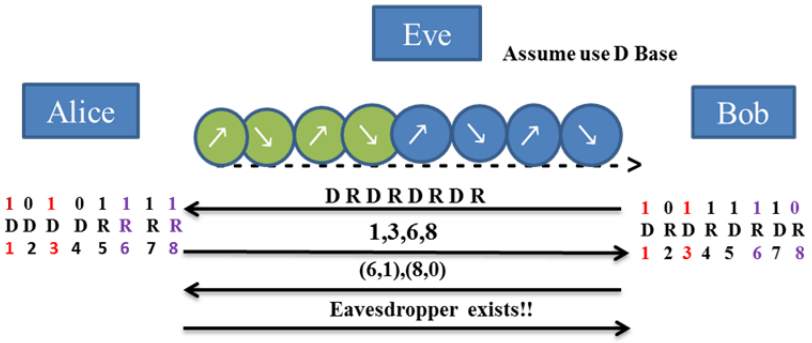

Figure 4.2. The Detection of Eve's presence. After comparing the bases used and discarding bits with incompatible bases, the shared key still has some errors in it. Taking the example of this figure, the photon number 8 shows that the same basis was used but different results were obtained. This demonstrates that Eve tampered with the transmission.

4.2. Error Correction Process

An error correction process is the step where users rectify errors in the sifted key [58]. Note that the QBER is the parameter which determines if the error reconciliation stage can be applied or not. There is a parameter called a failure threshold for any QKD protocol. It is the percentage of errors any QKD protocol shouldn't exceed.

This percentage of errors is different for each QKD protocol. Therefore, the QBER has to be less than the failure threshold, in order to execute the error correction stage. Otherwise, if the QBER is more than the failure threshold the transmission has to be aborted and started from scratch. If necessary the quantum link is modified.

The most important goal of the error correction process is to allow users to efficiently locate and fix errors in the sifted key while revealing as little

information as possible over the public classical channel [59]. Actually, Eve gains more information of the key over the classical channel however she cannot interfere, the only thing she can do is listen to the communication of Alice and Bob [59].

An efficient error correction protocol has to satisfy the following characteristics:

- be capable of working with a high QBER (e.g. 1% - 5%),
- be capable of minimising the information leaked to Eve (the revealed bits during the error correction process are discarded).

There exist many error correction protocols which can successfully correct errors in the sifted key. Some have a recursive structure, which means they require multiple iterations to correct all errors (e.g. Cascade, Winnow) [15, 18]. Others have a non-recursive structure, which means they require only one iteration and all the errors are corrected (e.g. LDPC Codes, Turbo Codes) [16, 17, 60]. At the end of the error correction process, users should have the identical keys.

4.2.1. Cascade Protocol

The Cascade Protocol is a reshaped protocol from another protocol named BBBSS introduced in 1991 by Bennett, Bessette, Brassard, Salvail, and Smolin [59]. BBBSS is an interactive reconciliation protocol, allowing Alice and Bob to locate and fix errors. The BBBSS protocol is composed of a number of passes, random permutations applied on the sifted key.

Table 4.1. An example of a parity bit

7 bits of a string	Counts of 1-bits in the string	8 bits including the parity bit	
		Even Parity	Odd Parity
0000000	0	00000000	00000001
0001000	1	00010001	00010000
1101001	4	11010010	11010011
0110111	5	01101111	01101110

The goal of these permutations is to isolate the erroneous bits randomly so that the even parities capable to mask each other will be revealed and also to prevent burst errors in the sifted key [59]. For the Cascade error correction protocol or for any other error correction protocol which uses parity checking process an odd parity is 1 and the even parity is 0.

The error correction process of BBBSS starts by dividing the sifted key into blocks of M_1 according to the calculated QBER for a purpose of having one error in each block. A parity bit for each block is calculated and exchanged publicly. A bit added at the end of a string of bits so that the count of 1-bits in that string is an even number or an odd number is called a parity bit. This operation is demonstrated in Table 4.1.

However, during the BBBSS operation no bit is added to the sifted key, the users only perform a parity checking . For blocks with same parities it means there is no error in that block. But if the parities are different, there has to be an odd error because even errors disguise each other. The parity checking operation is demonstrated in Figure 4.3.

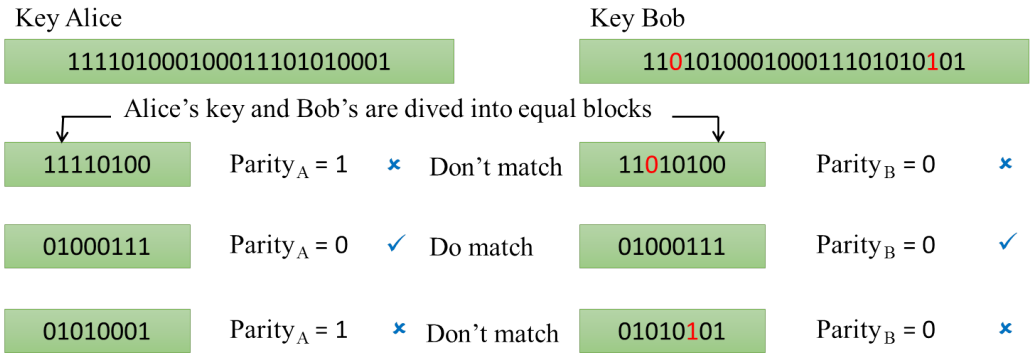

Figure 4.3. Description of the parity checking

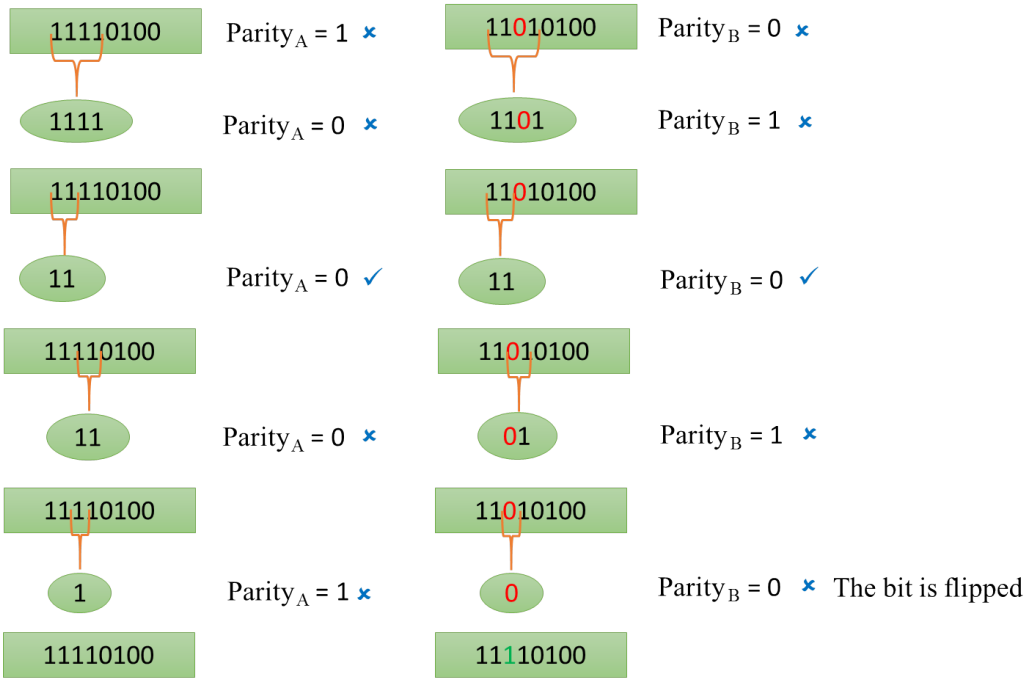

Figure 4.4. The binary search operation. It is applied on the block of Alice and on the block of Bob. The green bit is the flipped bit.

The block with a mismatching parity is split up into two sub-blocks with size of $\frac{M_1}{2}$ and the parity check is run again. This method is called "binary search" and it is shown in Figure 4.4 [59].

By using the first block of Alice's string of bits and the first block of Bob's string of bits shown in Figure 4.3, the binary search can be performed as shown in Figure 4.4.

The permutation of the sifted key is applied and the binary search operation is conducted again to identify masked errors. Since the parity check and the binary search are performed over a the classical channel, the authors of this protocol assumed that these processes offer the information about the key to the attacker. They proposed to leave out the bit at the end of each block and sub-block where the parity was shared, in order to reduce the information an attacker could have gained during the error correction process. This is called "Privacy maintenance" [59]. To decrease the amount of bits discarded during the parity checks, the binary search protocol uses a method called confirm and bisect, which loses fewer bits during the last passes. The BBBSS protocol requires 20 parity check passes, for Alice and Bob to be confident they have the same reconciled keys in the end.

Cascade was introduced in 1994 by Brassard and Salvail [15]. The Cascade protocol is like the BBBSS protocol because they both perform a binary search operation and parity checking process but their differences are remarkable. Similarly to the BBBSS protocol, by applying the Cascade protocol for the first pass the sifted key is divided into equal blocks M_1, depending on the calculated QBER, and the parity check of every block is shared as shown in Figure 4.3 [15] .

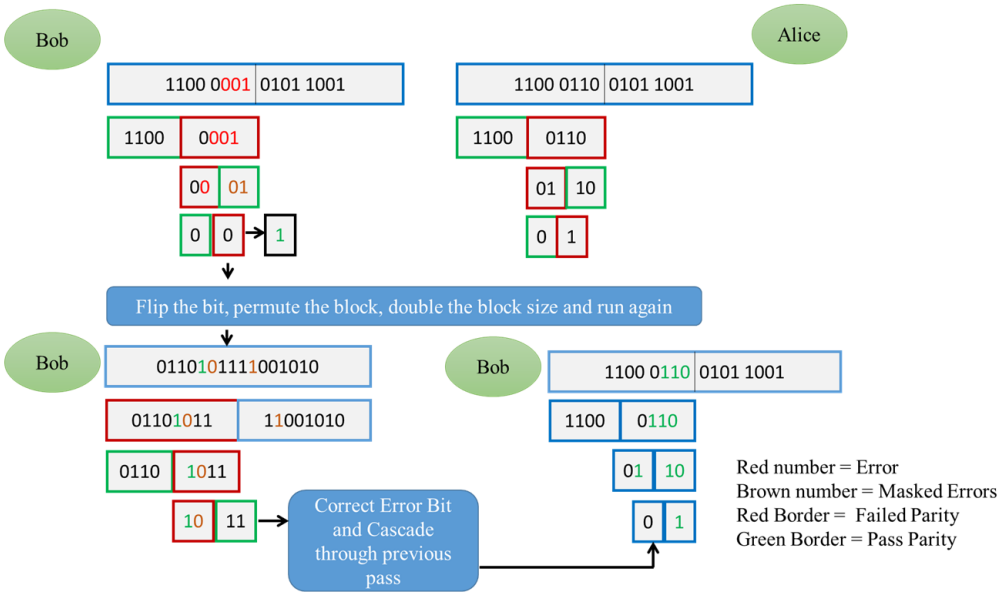

Figure 4.5. Illustration of the Cascade protocol. According to this figure, Alice and Bob have divided their string bit in equal blocks. The first block on Bob's side is not the same as Alice's. The binary search is run on this block by dividing this block into small blocks until the single error is located and fixed. For the next pass, this block with error is doubled in size and the binary search is run again. If a new error is found, it means that, this error was masked in the previous pass. Then the error is corrected and cascade goes back to the previous pass to try locate the matching error.

Also similarly to the BBBSS protocol, a binary search is conducted to find a single bit error for blocks which parities are different. The binary search consists of dividing the blocks with mismatching parities into sub-blocks and running the parity check on those sub-blocks again (see Figure 4.4). However, no bit is discarded on this pass instead the errors are fixed then a permutation is applied and the length of blocks with errors is increased to $2M_1$.

The second pass is started the same as the first one. Any error located and fixed in the second pass indicates there is at least one equivalent error in the previous pass on the same block because neither error was revealed or corrected in that pass [15].

Whenever a new error is found, it indicates the ability of having masked other errors in the previous pass, hence the process is repeated to detect and correct errors in all the previous passes. That's where it gets the name "Cascade". The authors of this protocol recommended four passes be used because in every pass after the first one, an average of two errors will be corrected which means the number of errors are decreased exponentially. The Cascade protocol has been investigated since the day it was introduced, it suffers from a high amount of information exchanged which can be leaked to the eavesdropper but it has been proven to be productive in correcting all the errors if implemented appropriately.

4.2.2. Winnow

There exists another error correction protocol which offers low rate of interaction and the same productivity as Cascade. This protocol is named Winnow and it was introduced in 2003 by Buttler, Torgerson, Nickel, Donahue, and Peterson [18]. It uses Hamming Codes to correct errors [60]. The Winnow protocol consists of a parity check, a conditional Hamming hash, and a privacy maintenance steps [61].

Hamming Codes are composed of two matrices, a generator matrix G and a parity check matrix H connected as $H \cdot G^T = 0$. If G is a $k \times n$ matrix, the code's rate is $r = \frac{k}{n}$ where k and n represent the columns and rows respectively, and in the standard form the first k columns of G represent an identity matrix.

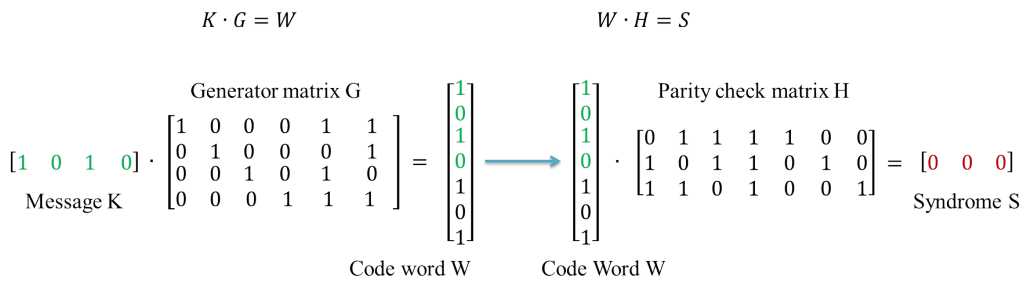

Figure 4.6. Description of the Hamming Codes. The sender calculates the dot product of the message K and the generator matrix G which results in the code word W and it is forwarded to the receiver. The receiver uses the code word W by calculating its dot product with the parity check matrix which will result in what is called a syndrome vector S. If the syndrome is equal to a zero vector then the receiver is sure that the message reached its destination without being tampered with. But the opposite result (i.e the syndrome is not equal to a zero vector) indicates there is at least one error in the message and the receiver will attempt to correct the message in order that the syndrome be equal to zero.

Hamming Codes have the capacity to detect two errors and correct one [18]. The Figure 4.6 shows how one can send a message using the Hamming codes. But how do Alice and Bob use Hamming Codes as the Winnow error correction protocol in QKD? In order to answer this question there is an important aspect that should be considered first. The Hamming Distance is the space separating two valid code words. Therefore, the minimum distance d_{min} becomes the small space separating two valid code words. If the number of errors in a code word is less than d_{min} then these errors will be located because they are not to change the code word into another valid code word. But this code word might not be the correct one that is why there must be some limits which one should consider.

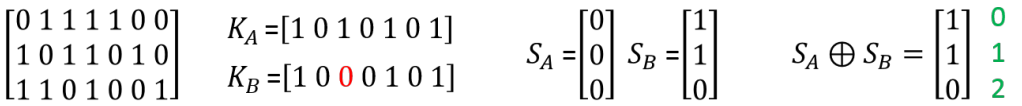

Figure 4.7. Error correction using Hamming Codes. There are errors in the syndrome that Bob calculated in position 0 and in position 1. So Bob should correct his key string in position $2^0 + 2^1 = 3$. Transmitting the syndrome over the public channel is the same as exchanging parity blocks in the Cascade Protocol, and this exchange is what the authors of this protocol called Winnow.

If the amount of errors in a code word is less than this bound $\left(\frac{d_{min}}{2}\right)$, the code word will be decrypted and the closest to that bound will be the correct code word. But if the amount of errors are greater than this bound, the code word might seem like another code word but not the correct one [61].

In QKD, for Alice to transmit the key string in a secure way, she has to make some changes so that the interaction with Bob will reveal less information to Eve. First Alice calculates her syndrome by using the dot product of the parity matrix and her key string $(H \cdot K)$ and sends it to Bob. On the other hand, Bob also calculates his syndrome by using the dot product of the parity matrix and his key string $(H \cdot K')$ and compares the two syndromes as illustrated in Figure 4.7.

If the two syndromes are equal $S = S'$, it means the syndrome he received from Alice was not tampered with and there is no error in it since it matches the one he calculated on his own. But if they are not the same there must be an error, then Bob will have to locate the error and correct it [61].

Similarly to the Cascade protocol Alice and Bob have to split the string of bits into equal blocks with the size k, the authors suggested $k = 8$. Thereafter, they have to compare their block parities to check if there is any difference. Instead of performing the binary search like in the Cascade protocol, Alice and Bob create a parity check matrix $H_{i,j} = \left(\frac{j}{2^{i-1}}\right) \mod 2$, and calculate

the syndrome S of each block B with a mismatching parity where $S = H \cdot B$. After Alice sends all her syndromes to Bob, who calculates his own syndromes and compares them to the ones received from Alice in the purpose of correcting any single error [18].

To minimize the information leaked in the parity/syndrome exchange Alice and Bob have to perform what we call privacy maintenance. The authors of Winnow suggested discarding one bit for every parity/syndrome shared publicly because those bits seem to be bit errors anyway but the selection of the syndrome bits is not random. It is recommended to remove bits on each block at position 2^j where $j \in \{0, ..., m-1\}$ because these bits do not depend on the syndrome calculation and they are the most visible.

After the first pass, Alice and Bob perform a permutation over their key string and the procedure is repeated because this parity check used in this protocol is only capable of locating an odd amount of errors and there are still an even amount of errors in the key string. The block size has to be increased and the parity check matrix recreated. The minimal passes needed to correct all the errors or the block size for each pass have not be agreed on, they are still a subject of discussion [18].

The disadvantage of Winnow is its dependency on the Hamming Codes which can be the cause of errors if the error count in each block is too high. This means the amount of errors detected has already grown bigger than the d_{min} and the probability of the protocol to detect the valid code word from the invalid one is also too high. To avoid the amount of even errors to be high, the authors recommended to avoid the permutation for the first pass.

4.2.3. Low-Density Parity Check Codes

The Low-Density Parity Check (LDPC) Codes are used as another error correction protocol, first established by a researcher named Robert Gallager in 1960 [16] however, LDPC Codes were not given so much consideration in that time. Almost 40 years after, when the Turbo codes were becoming popular [62], LDPC Codes were reintroduced by McKay in his paper named "Good Error-Correcting Codes Based on Very Sparse Matrices"published in 1999 [17].

LDPC Codes are linear block codes operating like Hamming Codes. LDPC are composed of a parity matrix H and a generator matrix G and also, like Hamming Codes, the minimum distance plays a major role because it establishes the limits of the code [63].

An LDPC Code can be described in two different ways. It can be described as a matrix with $n \times m$ dimension and with W_r representing the amount of 1's in each row and W_c representing the amount of 1's in each column as shown in Figure 4.8. To have an LDPC matrix two conditions must be fulfilled: $W_r \ll n$ and $W_c \ll n$ [63].

An LDPC Code can also be described by graphic representations named Tanner graphs [64]. Tanner graphs also called bipartite graphs, are composed by two separate and distinct sets, check nodes(C-nodes) and variable nodes(V-nodes) respectively. The construction of this graph consists of representing the amount of parity bits as check nodes and representing the amount of bits in a code word as variable nodes [63]. This type of description of LDPC Codes is illustrated in Figure 4.9 and Figure 4.10.

$$H = \begin{bmatrix} 0\,1\,0\,1\,1\,0\,0\,1 \\ 1\,1\,1\,0\,0\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,1 \\ 1\,0\,0\,1\,1\,0\,1\,0 \end{bmatrix}$$

Figure 4.8. Description of an LDPC Code as a matrix of dimension (8 ×4). Here $W_r = 2$ and $W_c = 4$ [65].

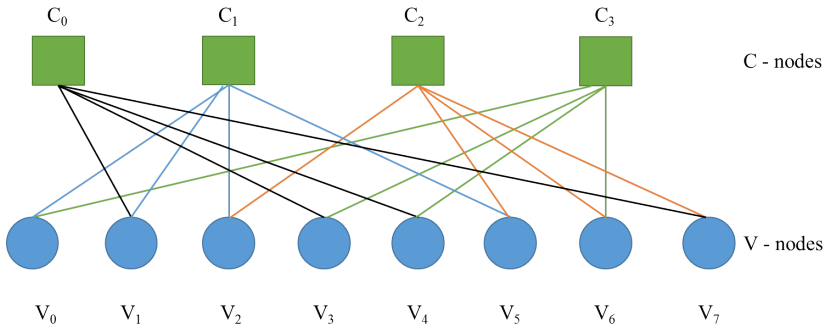

Figure 4.9. Description of the Tanner graph. The amount of lines on each C-node is constant and the amount of lines on each V-node are constant. This figure represents a regular LDPC Code [65].

There exist two types of LDPC Codes: some can be regular codes or other can be irregular codes. Gallager, when he first introduced them in 1960, he described these codes as regular codes whenever the amount of 1's in each row or in each column is fixed and $W_r = W_c \times (n/m)$.

With a graphic representation, one can observe the uniformity of LDPC. The number of lines coming from each C-node is the same, as well as the number of lines coming from each V-node (see Figure 4.9).

LDPC Codes are irregular when the amount of 1's in each column or in each row is no longer consistent. This means for the Tanner graph, the number of lines coming from each C-node is not consistent as well as the number of lines coming from each V-node. Figure 4.10 describes an irregular LDPC Code in Tanner representation [60].

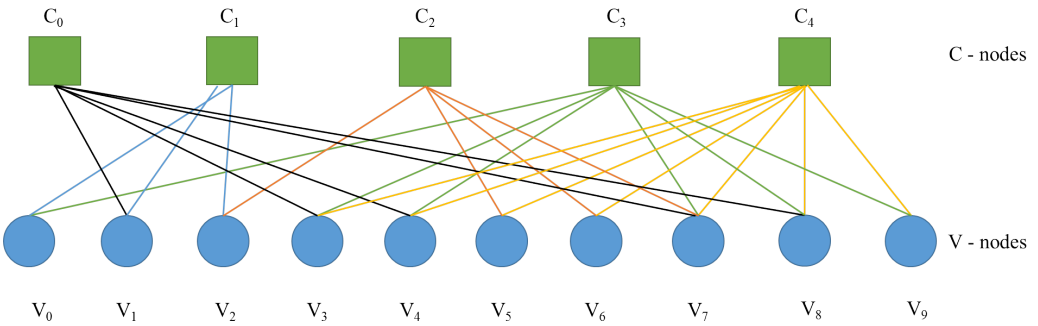

Figure 4.10. Irregular LDPC Code. The amount of lines on each C-node is no longer constant, the same applies to each V-node [65].

Taking an example from Figure 4.9, a path coming from one node C: the path from $C_0 \rightarrow V_1 \rightarrow C_1 \rightarrow V_5 \rightarrow C_2 \rightarrow V_7 \rightarrow C_0$ or the path from $C_0 \rightarrow V_3 \rightarrow C_3 \rightarrow V_4 \rightarrow C_0$ are called a cycle. The girth is the shortest cycle in the graphic representation of an LDPC code [60].

Encoding a message using LDPC Codes is the same as using Hamming Codes. Alice calculates the code word using the dot product of the message and the generator matrix and sends it to Bob. Next, Bob will multiply the parity check matrix by the code word received from Alice to form a syndrome vector. If the syndrome vector is zero then Bob assumes that the message reached him unchanged. The LDPC Codes are different from Hamming Codes on how Bob transforms the code word into the original message if the syndrome is not a zero vector which means there are some errors in the code word [60].

4.3. Privacy Amplification

Privacy amplification is the final procedure of QKD performed after error correction to minimise the information Eve has obtained while the quantum transmission process was taking place as well as the error correction process [66]. During error correction process Alice and Bob disclose some amount of

information which can enable Eve to reconstruct the important part of secret key as the error reconciliation process is performed on a public channel. However, Eve can also gain information during the quantum transmission process [67].

As mentioned earlier, the Winnow protocol discards some bits during the error correction process but Cascade and LDPC do not. Therefore, these bits are used to estimate the information leaked to Eve. At this stage, Alice possesses an identical key to Bob but which Eve has some information about. The privacy amplification stage is performed by using a universal hash function to reduce the knowledge Eve has gained about the key [68, 69].

The goal of privacy amplification is to construct a shorter random and secret key even if Eve has a partial information about it, trying to compute this hash function will introduce errors in her version of the key. A universal hash function is randomly chosen from a class of hash functions, and is used by taking an input data with the length of the reconciled key and reducing it to a shorter length according to the amount of information leaked to the adversary [69].

The privacy amplification process is used to achieve many goals such as, to keep the integrity of the transmitted data by signing the document. The privacy amplification process falls out of the scope of this study however, it might be considered for future research outcomes.

Chapter 5

Implementation of Cascade Correction Protocol

The implementation of Cascade protocol used in this work was performed in the C++ programming language using Microsoft Visual Studio 2015 environment. The Cascade protocol is executed by a main class which calls on two external classes. The first external class is a Random Number Generator (RNG) which creates a common random seed according to Mersenne Twister Algorithm [70] however, this class on its own cannot manage the permutation. Cascade uses another permutation class which maintains a sequence of integers, randomly created, within the range of the key size. This is done with the purpose of locating the block where the error is and even the error itself in the string bit.

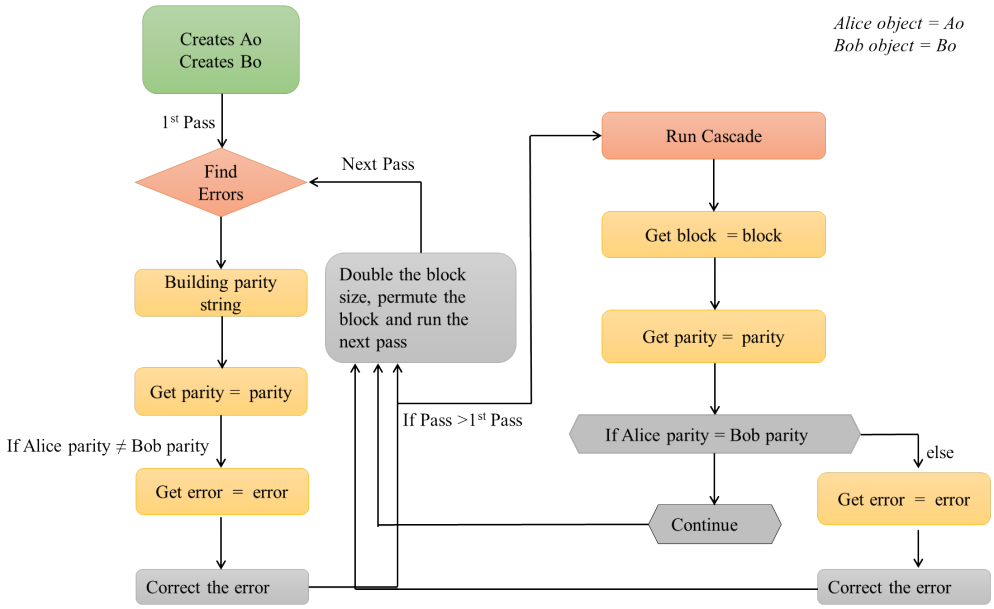

Figure 5.1. Cascade operation. It is a chain of one function calling the other starting from creating Alice object and Bob object. The function responsible to find errors is given Alice object and Bob object. This function calls another function responsible to build parity string, the latter function calls another function responsible to get the parity. If Alice parity doesn't match with Bob parity, a call is made to the Get error function. The error is found and corrected. If the current pass is not the first pass, cascade function is called to get the block containing the error in previous pass; hence the parity of that block for Alice and Bob. If the Alice parity matches with Bob parity the operation continue to the next pass but if, Alice parity does match with Bob parity the program has to find the error on that block; corrects it and after goes to the next pass.

The main class has seven functions. The first function has to create two objects, one for Alice and another for Bob. The second function is to find the errors in Bob' sifted key. The third function is to build the parity. The fourth function returns the parity built at the current pass. The fifth function gives the block containing the error. The sixth function locates the error. The seventh one does cascade after the first pass is finished. In other words, what the last function does; is to look into other passes after the first one to locate the error.

Finding an error in any other pass after the first one means there is a matching error in the previous passes but they were masked (see Figure 5.1).

To create an object for Alice, three arguments are used: the sifted key of Alice, the common seed and the QBER. The value of the QBER determines the size each block should have at the first pass. The object for Bob is created using four arguments: the sifted key of Bob, the common seed, the QBER and the address of the object of Alice.

The permutation for the first pass is omitted to prevent burst errors because the goal of the permutation is to spread out the errors so that they will not be masked during the parity checking. The Cascade operation only runs five passes at once, to correct all the errors in Bob's key. Every time the parity is built the maximum and the minimum of bits leaked are tracked. The actual bits leaked are also tracked to be used later in finding information Eve could have gained during the error correction process. After the five passes are completed, the corrected key (reconciled key) of Bob is plotted and it is identical to Alice's.

5.1. Key parameters for the effectiveness of the Cascade error correction protocol

5.1.1. Shannon Entropy and Shannon Limit

According to Claude E. Shannon, every channel has a limited capacity to transmit information [1]. The maximum capacity for a noisy channel to successively transmit information at a certain rate with high probability is given by

$$\mathrm{C} = 1 - \mathrm{H(X)}\,, \tag{5.1}$$

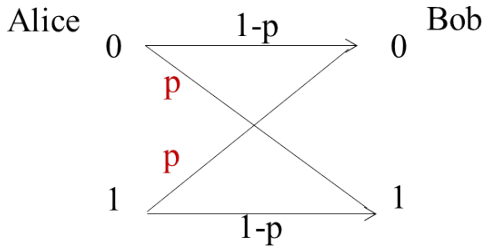

Figure 5.2. The possible values of X for a binary symmetric channel. A probability of Alice sending a bit with value 0, but that bit gets flipped and Bob receives 1 is given by p. A probability of Alice sending a bit with value 1 and Bob receives 1 is given by $1 - p$.

where H(X) represents the Shannon entropy which is given by:

$$\mathrm{H(X)} = -\sum_{i=1}^{N} p_i \log_2 p_i \,, \tag{5.2}$$

where p_i represents the probability of a given symbol. For a binary symmetric channel (BSC) as shown in Figure 5.2, X can only take two possible values with probability p and $1-p$. Therefore the Shannon entropy H(X) of a BSC is given by the following form:

$$\mathrm{H(X)} = -p \cdot \log_2 p - (1-p) \cdot \log_2 (1-p) \,. \tag{5.3}$$

The capacity of a BSC then becomes:

$$\mathrm{C} = 1 + p \cdot \log_2 p + (1-p) \cdot \log_2 (1-p) \,, \tag{5.4}$$

where C is also called the Shannon limit (or Shannon Information) and if the rate of transmission is greater than C, there is a failure in the transmission. However if the rate of transmission is less than C, there is high probability of the information to be transmitted effectively. By increasing the value of p in a equation 5.4, the Shannon limit for a BSC is described by the following:

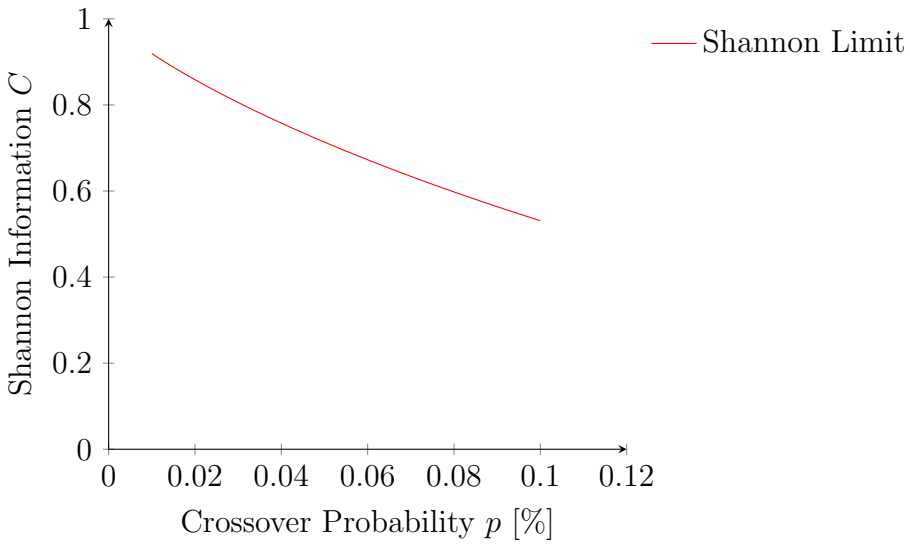

Figure 5.3. The Shannon limit with respect to a change in p.

The value of p used to plot Figure 5.3 ranges form 0.01 to 0.1. Since this work uses the Shannon limit to evaluate the performance of Cascade algorithm in terms of correcting errors in the sifted key, it is fair to set similar initial conditions for comparison by using the value of p in the same range as the QBER. As the value of p increases, the Shannon limit decreases. The closer a protocol is to the Shannon limit, the higher is its effectiveness to reduce the information leaked. That is why in this work a comparison between the Shannon limit and the Cascade error correction protocol is performed.

5.1.2. Efficiency and Information leakage of the Cascade error correction protocol

The evaluation of Cascade efficiency is done by performing a comparison between the Shannon limit and the Cascade error correction protocol when

the QBER increases. The increase of the QBER affects the information leakage considered to be bits exposed during the Cascade error correction process. The higher the QBER, the bigger is number of bits exposed. The information rate of the protocol decreases.

The information rate is connected to the effectiveness of the Cascade error correction protocol, in a such way that working with high QBER reduces the efficiency of the Cascade error correction protocol. The information rate of the protocol is given by:

$$\mathrm{IR} = 1 - \frac{\mathrm{BR}}{\mathrm{TB}}\,, \tag{5.5}$$

where IR is the information rate, BR is the amount of the redundancy bits and TB is the amount of all bits. The quality of an error correction scheme is determined by the efficiency parameter f which can be defined by:

$$\mathrm{f(p)} = \frac{\mathrm{m}}{\mathrm{nH(p)}}\,, \tag{5.6}$$

where m is the bits exposed, p is the QBER and nH(p) is the minimum information needed for the error correction process. The efficiency parameter f has a value $\geqslant 1$ and for $\mathrm{f} = 1$ stands for the perfect reconciliation.

5.1.3. Advantages of the Cascade error correction protocol

The implementation of the Cascade error correction protocol is easily performed and adjustable. This means it is able to work with different quantum bit error rates which change the block sizes. The Cascade efficiency is closer to the Shannon limit and the amount of information leakage is kept small. The Cascade error correction protocol is a permanent interactive protocol which means it requires multiple interactions between users until the error correction process is completed.

5.1.4. Limitation of Cascade Error Correction Protocol

The limitations of the Cascade error correction protocol are observed when the QBER is wrongly estimated. As the QBER is responsible to set the size of the blocks and the Cascade algorithm will fail to rectify all the errors in the sifted key.

5.2. Results

The Cascade error correction protocol implemented in this work was run on different sifted keys with different QBER. The first sifted key inserted into the Cascade algorithm had 1 % of QBER with a length of 1000 bits. This sifted key was used to compare the effectiveness of the Cascade error correction protocol and the Shannon limit. The other remaining sifted keys with high QBER were used to demonstrate how the information rate deceases when the Cascade algorithm is performed on sifted keys with high QBER. They were also used to demonstrate how the efficiency parameter increases each time the amount of the bits exposed increases. The use of different sifted keys with different QBERs has the objective of identifying the impact high values of the QBER might have on an error correction protocol such as The Cascade protocol in terms of performance.

5.2.1. Evaluation of Cascade Error Correction Protocol

The evaluation of effectiveness of the Cascade error correction protocol performed in this work considers two parameters. The first parameter is the comparison between the Cascade error correction protocol and the Shannon limit. In order to achieve that, the Cascade algorithm was performed on the sifted key with 1 % of QBER.

After five passes were completed, the QBER was increased. The increase of the QBER was performed in range of 0.010 - 0.100. Each time the QBER was increased, the bits exposed were tracked to be used for the calculation of the information rate using a equation 5.5. The results obtained are shown in Table 5.1.

According Table 5.1 when the QBER was low (0.010) the Information rate of the Cascade algorithm (0.864) was closer to the Shannon Limit (0.919) because the difference between these two value is 0.055. However, when the QBER became high (0.100), the information rate of the Cascade algorithm (0.366) was no longer closer to the Shannon limit (0.531) since the difference between the Shannon limit and Cascade algorithm is 0.165.

Using the results in Table 5.1, the graph showing how the effectiveness of the Cascade error correction decreases when the QBER increases, was plotted as shown in Figure 5.4.

According to Claude E. Shannon, a good error correction protocol should be closer to the Shannon limit [1]. By referring to Figure 5.4, the Cascade algorithm is closer to the Shannon limit when the value of the QBER is lower. However, when the value of the QBER increases the Cascade algorithm moves away from the Shannon limit.

Table 5.1. The comparison between the Shannon limit and Cascade algorithm

Key Length	QBER	Shannon Limit	Information Rate
1000	0.010	0.919206864	0.864
1000	0.013	0.899917925	0.844
1000	0.015	0.88763929	0.836
1000	0.018	0.869941154	0.807
1000	0.020	0.858559457	0.795
1000	0.023	0.842031453	0.757
1000	0.025	0.831339069	0.749
1000	0.028	0.815739407	0.725
1000	0.030	0.805608142	0.719
1000	0.033	0.790779522	0.705
1000	0.035	0.781122273	0.697
1000	0.038	0.766954107	0.690
1000	0.040	0.757707811	0.686
1000	0.043	0.744118084	0.663
1000	0.045	0.735234966	0.659
1000	0.048	0.722160426	0.626
1000	0.050	0.713603043	0.618
1000	0.053	0.700993422	0.617
1000	0.056	0.69273164	0.557
1000	0.058	0.680546034	0.550
1000	0.060	0.672555081	0.549
1000	0.063	0.660759558	0.543
1000	0.065	0.653018712	0.530
1000	0.068	0.641584675	0.528
1000	0.070	0.634076349	0.521
1000	0.073	0.622979373	0.520
1000	0.075	0.615688456	0.514
1000	0.078	0.604907439	0.500
1000	0.080	0.59782081	0.492
1000	0.084	0.587337344	0.483
1000	0.085	0.580443504	0.471
1000	0.088	0.570241391	0.437
1000	0.090	0.563530183	0.435
1000	0.093	0.553595062	0.387
1000	0.095	0.547057452	0.379
1000	0.098	0.537376508	0.375
1000	0.100	0.531004406	0.366

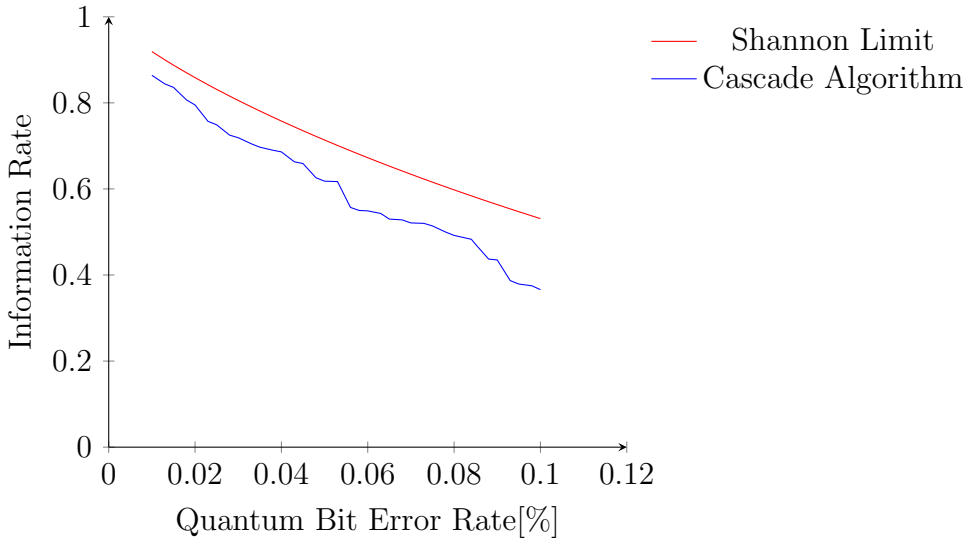

Figure 5.4. The performance of the Cascade Algorithm

The second parameter to consider is the information leakage. Applying the Cascade algorithm to a sifted key with a high QBER affects the information leakage. This is verified by the increase of bits exposed resulting in the decrease of the information rate. To demonstrate this statement, the remaining sifted keys with a length of 1000 bits each were run into cascade one by one, the bits exposed of each sifted key were registered and Table 5.2 indicates the results obtained.

The results presented in Table 5.2 indicate how the increase of the QBER causes the information rate to decrease. The values of information rate were obtained using a equation 5.5. Therefore, by using equation 5.6 and the values of information rate in Table 5.2, the efficiency parameter f was calculated. The results obtained for the efficiency parameter f are illustrated in Table 5.3.

Table 5.2. Effectiveness of the Cascade Algorithm in presence of high information leakage

Key Length	QBER	Bits exposed	Information Rate
1000	0.036	315	0.685
1000	0.037	327	0.673
1000	0.041	347	0.653
1000	0.044	378	0.622
1000	0.046	392	0.608
1000	0.049	402	0.598
1000	0.050	421	0.579
1000	0.056	496	0.504

Table 5.3. Efficiency parameter of Cascade Algorithm

Key Length	QBER	Bits Exposed	Efficiency parameter
1000	0.036	315	1.408
1000	0.037	327	1.431
1000	0.044	378	1.451
1000	0.046	392	1.456
1000	0.056	496	1.593

Table 5.3 shows that the efficiency parameter of the Cascade algorithm is high when high values of QBER are used.

Cascade error correction protocol requires multiple iterations which consist of parity checking of blocks and sub-blocks. Therefore, an amount of information is exchanged between users over the classical channel. Although this channel is authentic, it allows an attacker to know what is going on between users. Therefore, during the error correction process, information can be leaked to an eavesdropper which will allow them to correct their version of the key obtained during the quantum transmission process.

With a high QBER, the size of the block to start with, for the error correction process becomes small. This will require users to exchange many parity bits

in order to correct their sifted key. Therefore, the high amount of bits will be exposed during error correction process (see Table 5.2).

The application of the Cascade error correction protocol on a QKD system of high values of QBER is not recommendable because the cascade protocol loses its efficiency as the QBER increases (see Table 5.3).

Chapter 6

Conclusion

6.1. Summary

Chapter 1 gives an introduction of how information can be measured and exchanged amongst legitimate users in the presence of an adversary. It also gives a definition of the cryptographic encryption and examines different types of cryptographic encryptions one could use to protect the information exchange. This chapter discusses the need of shifting from classical cryptography to quantum cryptography.

Chapter 2 discusses how the classical mechanics deals with elements on the macroscopic scale and how it fails to describe the behaviour of some elements (e.g photons, electrons) on the microscopic scale. Therefore, quantum mechanics was introduced as an alternative field to deal with the behaviour of some elements on the microscopic scale.

In this chapter, the laws of quantum mechanics are defined and how they are applied to guarantee security of the implementation of a QKD system.

Chapter 3 describes the background of QKD including different protocols one can use to produce a secure key. This chapter defines different channels which connect users in order to exchange the transmission. It also describes different types of eavesdropping attacks which users can encounter.

Chapter 4 describes different steps followed when performing the post-processing operation, and it presents the value of performing the post-processing operation. This chapter also describes various types of error correction protocols and point out their differences.

Chapter 5 presents the implementation of the Cascade error correction protocol as one error reconciliation protocol applied in this work. This chapter also presents the results obtained and how they were compared to the Shannon limit to test the effectiveness of the Cascade.

Chapter 6 provides the summary of what is contained in each chapter. It also provides the conclusion of the whole thesis demonstrating how the QBER plays a major role in the implementation of a QKD system. This chapter reminds the reader that the implementation of the Cascade error correction protocol requires users to be working with low values of the QBER. This chapter also provides recommendations on other fields of study.

The implementation of a QKD system requires an appropriate protocol, nevertheless the quantum transmission can be intercepted by an eavesdropper and this will introduce errors in the transmission. The errors also come from the devices used. Therefore, an adequate error correction protocol is needed for QKD. The Cascade error correction protocol is the most widely used.

It was chosen in this work for that purpose, to evaluate its effectiveness in the presence of different values of the QBER. We have mentioned that the QBER is an important parameter for any QKD system because it determines its security and efficiency.

- For the security: the value of the QBER reveals the presence of Eve and Alice and Bob will decide if they have to abort the whole process or to continue with the error correction process and later on the privacy amplification process.
- For the efficiency: the value of the QBER indicates how efficient the system is. It determines if the system is closer to the theoretic bound (the Shannon limit) or not, it determines the information leaked during the error correction process, and if the error correction process performed is perfect or not.

The implementation of the Cascade correction protocol uses the value of the QBER to divide the sifted key into blocks with equal size so that users would start building the parity string. However, if the estimation of the QBER were wrongly performed, the Cascade algorithm would fail to correct all the errors in the sifted key.

In the presence of a high QBER, the block size decreases and causes an increase in the parity string exchanged between Alice and Bob. Therefore, the information which could be leaked (bits exposed) to Eve becomes high.

Working with high values of the QBER affects the Cascade error correction protocol in terms of its effectiveness because the Cascade algorithm moves away from the Shannon limit. The high values of the QBER also causes the information rate of the Cascade algorithm to decrease. Therefore, the efficient parameter of the Cascade algorithm is more than 1 which should not be the case for a perfect reconciliation process.

Therefore, for this reason it is recommended to apply the Cascade error correction protocol to a sifted key with a low QBER as its efficiency is closer to the Shannon limit and the information leaked is small. Cascade error correction protocol demands many interactions between parities, it is feasibly efficient and easy to implement.

6.2. Recommendation for future field of study

The purpose of the post-processing stage is to identify errors obtained during the quantum transmission process and to correct those errors by applying an adequate error correction protocol to the sifted key. Lastly, users have also to remove the information an eavesdropper could have obtained through the quantum link during the quantum process, as well as information leaked during the error correction process.

The major focus of this work was to apply the Cascade error correction protocol to a sifted key obtained through a QKD system constructed using an experimental set-up. This operation was to identify and correct errors obtained during the quantum transmission process. This work also tested the Cascade error correction protocol in terms of effectiveness by comparing the Shannon limit to Cascade in presence of a high QBER.

The next step would be to perform the privacy amplification process by removing the information the attacker could have gained, with the purpose of obtaining a secret (private) key. This private key is used to encode and decode a message. In the future, it would be better to extend our research to a free space QKD outside the laboratory where there is actual noise instead of adding noise in the system. This means, the users will be working in the presence of high QBER and the Cascade error correction protocol will not be an appropriate protocol to use. According to our results, we noticed

that Cascade error correction protocol moves away from the Shannon limit as the QBER increases. Another point we noticed is that the efficiency of the Cascade error correction protocol decreases as the QBER increases. Therefore the error correction protocols such as LDPC codes or Tubo Codes have been proven to be efficient to work with high values of QBER might be the appropriate ones in such case.

Bibliography

1. Claude E Shannon. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(1):3–55, 2001.

2. Claude E Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

3. Peter Zoller, Th Beth, D Binosi, R Blatt, H Briegel, D Bruss, T Calarco, J Ignacio Cirac, D Deutsch, J Eisert, et al. Quantum information processing and communication. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 36(2):203–228, 2005.

4. Hans Delfs and Helmut Knebl. *Introduction to cryptography*, volume 2. Springer, Berlin, Heidelberg, 2002.

5. Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of Applied Cryptography*. CRC press, Florida, US, 1996.

6. Ueli Maurer. Information-theoretic cryptography. In *Annual Interna-*

tional Cryptology Conference, pages 47–65. Springer, Berlin, Heidelberg, 1999.

7. Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.

8. H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.

9. Richard J Hughes, George L Morgan, and C Glen Peterson. Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547, 2000.

10. Charles H Bennett and G Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

11. David Bohm and Basil J Hiley. *The Undivided Universe: An Ontological Interpretation of Quantum Theory*. Routledge, Abingdon, UK, 2006.

12. Paul Busch, Teiko Heinonen, and Pekka Lahti. Heisenberg's uncertainty principle. *Physics Reports*, 452(6):155–176, 2007.

13. William K Wootters and Wojciech H Zurek. The no-cloning theorem. *Physics Today*, 62(2):76–77, 2009.

14. Vladimir Bužek and Mark Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54(3):1844, 1996.

15. Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423. Springer, Berlin, Heidelberg, 1993.

16. Robert Gallager. Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28, 1962.

17. David JC MacKay. Good error-correcting codes based on very sparse matrices. *IEEE transactions on Information Theory*, 45(2):399–431, 1999.

18. William T Buttler, Steven K Lamoreaux, Justin R Torgerson, GH Nickel, CH Donahue, and Charles G Peterson. Fast, efficient error reconciliation for quantum cryptography. *Physical Review A*, 67(5):052303, 2003.

19. Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. Number 27. Oxford University Press, 1981.

20. Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

21. Anthony P French and Edwin F Taylor. *An introduction to quantum physics*. CRC Press, Florida, US, 1979.

22. KJ Resch, M Lindenthal, B Blauensteiner, HR Böhm, A Fedrizzi, C Kurtsiefer, A Poppe, T Schmitt-Manderbach, M Taraba, R Ursin, et al. Distributing entanglement and single photons through an intracity, free-space quantum channel. *Optics Express*, 13(1):202–209, 2005.

23. Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2): 865, 2009.

24. Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, 2007.

25. Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

26. Werner Heisenberg. *The physical principles of the quantum theory*. Courier Corporation, 1949.

27. David Prutchi. *Exploring quantum physics through hands-on projects*. John Wiley & Sons, New Jersey, US, 2012.

28. William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

29. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

30. Fabian Furrer, Torsten Franz, Mario Berta, Anthony Leverrier, Volkher B Scholz, Marco Tomamichel, and Reinhard F Werner. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Physical Review Letters*, 109 (10):100502, 2012.

31. Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

32. Harry JR Dutton. *Understanding optical communications*. Prentice Hall PTR, New Jersey, US, 1998.

33. Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 9(3):163–168, 2015.

34. C Gobby, ZL Yuan, and AJ Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(19):3762–3764, 2004.

35. Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145, 2002.

36. H-J Briegel, Wolfgang Dür, Juan I Cirac, and Peter Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

37. Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185–188, 2012.

38. Markus Aspelmeyer, Hannes R Böhm, Tsewang Gyatso, Thomas Jennewein, Rainer Kaltenbaek, Michael Lindenthal, Gabriel Molina-Terriza, Andreas Poppe, Kevin Resch, Michael Taraba, et al. Long-distance free-space distribution of quantum entanglement. *Science*, 301(5633):621–623, 2003.

39. Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

40. W Dür, H-J Briegel, JI Cirac, and P Zoller. Quantum repeaters based on entanglement purification. *Physical Review A*, 59(1):169, 1999.

41. N Lütkenhaus, J Calsamiglia, and K-A Suominen. Bell measurements for teleportation. *Physical Review A*, 59(5):3295, 1999.

42. Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121, 1992.

43. Artur K Ekert. Quantum cryptography based on bells theorem. *Physical Review Letters*, 67(6):661, 1991.

44. Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting

attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

45. Cyril Branciard, Nicolas Gisin, Barbara Kraus, and Valerio Scarani. Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72(3):032301, 2005.

46. Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner, and Valerio Scarani. Towards practical and fast quantum cryptography. *arXiv:quant-ph/0411022v1*, 2004.

47. Sheila Cobourne et al. Quantum key distribution protocols and applications. Technical report, Royal Holloway, University of London, Surrey TW20 0EX, England, 2011.

48. Youn-Chang Jeong, Yong-Su Kim, and Yoon-Ho Kim. Weak-pulse implementation of b92 quantum cryptography protocol in free-space. Available online from: qopt. postech. ac. kr/publications/B92_ver3. pdf, 2007.

49. Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85(6):1330, 2000.

50. Damien Stucki, Claudio Barreiro, Sylvain Fasel, Jean-Daniel Gautier, Olivier Gay, Nicolas Gisin, Rob Thew, Yann Thoma, Patrick Trinkler, Fabien Vannel, et al. High speed coherent one-way quantum key distribution prototype. *arXiv:quant-ph/0809.5264v1*, 2008.

51. Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden. Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87(19):194108, 2005.

52. Eleni Diamanti. *Security and implementation of differential phase shift quantum key distribution systems*. Stanford University, 2006.

53. Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, 2006.

54. Franco Callegati, Walter Cerroni, and Marco Ramilli. Man-in-the-middle attack to the https protocol. *IEEE Security & Privacy*, 7(1):78–81, 2009.

55. Steven J Murdoch. Insecure by design: protocols for encrypted phone calls. *Computer*, 49(3):25–33, 2016.

56. Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

57. Mohammed Ardehali, HF Chau, and Hoi-Kwong Lo. Efficient quantum key distribution. *arXiv preprint quant-ph/9803007*, 1998.

58. Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-Correcting Codes*. Elsevier, 1977.

59. Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

60. Todd K Moon. Error correction coding. *Mathematical Methods and Algorithms. John Wiley & Sons, New Jersey, US*, 2005.

61. Andrew M Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793, 1996.

62. Claude Berrou, Alain Glavieux, and Punya Thitimajshima. Near shannon limit error-correcting coding and decoding: Turbo-codes. 1. In *Communications, 1993. ICC'93 Geneva. Technical Program, Conference Record, IEEE International Conference on*, volume 2, pages 1064–1070. IEEE, 1993.

63. Amin Shokrollahi. Ldpc codes: An introduction. *Digital Fountain, Inc., Tech. Rep*, page 2, 2003.

64. R Tanner. A recursive approach to low complexity codes. *IEEE Transactions on information theory*, 27(5):533–547, 1981.

65. Bernhard MJ Leiner. Ldpc codes–a brief tutorial. *American Political Research APR*, 8:1–9, 2005.

66. Charles H Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2): 210–229, 1988.

67. Charles H Bennett, Gilles Brassard, Claude Crepeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

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

69. Gilles Van Assche. *Quantum cryptography and secret-key distillation*. Cambridge University Press, 2006.

70. Makoto Matsumoto and Takuji Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 8(1):3–30, 1998.

Index