Quantum Key Distribution for the Undergraduate Curriculum

by

Samukelisiwe Purity Phehlukwayo

Supervised by

Prof F. Petruccione and Dr Y Ismail

A thesis submitted to the Department of Physics, Faculty of Science and Engineering, University of KwaZulu-Natal, in fulfillment of the requirement for the degree of Master of Science

6 December, 2017

Dedications

To my baby Pallo.

Abstract

Quantum Key Distribution (QKD) is one of the technological applications of quantum mechanics. The technology allows two users to securely establish an unbreakable key. The key is used to encrypt and decrypt sensitive information such as online banking and emails. This technological application has matured in an industry as it provides real world implementation. It offers a provably secure key based on the principles of quantum mechanics. There are products that are available that can be used to implement this technology.

This study demonstrates the implementation of the QKD process for the undergraduate physics curriculum. We outline the procedure of QKD in a convenient way for students to follow and understand. To this end, a comprehensive manual has been developed to enable undergraduate students to learn the foundations of QKD. Students will gain knowledge that using quantum mechanical properties, two remote parties can securely establish a communication by exchanging keys which can then be used as an encryption. We present the QKD system such as the id 3000 as a learning tool in the physics 3rd-year laboratory, to introduce undergraduate students to applications in quantum information science. We demonstrate a typical experiment which undergraduate students can perform using the id 3000 system in the 3rd physics laboratory. Our vision is to see students exploring quantum mechanics in more depth and learning practical work alongside theories taught in the curriculum.

Preface

The work contained in this thesis was carried out from June 2015 to December 2017 in the School of Chemistry and Physics, University of KwaZulu-Natal, Westville campus, South Africa, under the Supervision of Professor Francesco Petruccione and Co-Supervision of Doctor Yaseera Ismail.

As the candidate's supervisor, I have approved this thesis for submission.

Student Signed: _____ Name: _____

Date: _____

Supervisor Signed: _____ Name: _____

Date: _____

Co-Supervisor Signed: _____ Name: _____

Date: _____

Declaration 1- Plagiarism

I, Samukelisiwe Purity Phehlukwayo declare that

i. This work has been composed solely by myself, except where stated otherwise by reference or acknowledgement, the work presented is entirely my own.

ii. This work has not been submitted, in whole or in part, in any previous application for a degree.

Signed: _____

Declaration 2- Publications and Presentations

Publications

S Phehlukwayo, Y Ismail, F Petruccione, 2017, 'Quantum Key Distribution for the Undergraduate Curriculum', SAIP 2017 Conference Proceedings (submitted).

Oral presentations

S Phehlukwayo, Y Ismail, F Petruccione, 2017, 'Quantum Key Distribution for the Undergraduate Curriculum' SAIP July 2017.

Poster presentations

S Phehukwayo, Y Ismail, F Petruccione, 2016 'Characterisation of a Quantum Key Distribution over An Optical Fibre', November 2016 Research Day,

University of KwaZulu-Natal.

Schools attended

8th Winter School on Practical Quantum Cryptography Les Diableretes, Geneva, Switzerland 15-26 January 2016.

Signed: _____

Acknowledgements

I am thankful to the Almighty God who gave me the strength to complete my studies.

I would like to express my sincere gratitude to my Supervisor Prof F Petruccione and Co-Supervisor Dr Y Ismail for expecting not less but the best from me and demanding that I excel.

Special thanks to the National Research Foundation (NRF) of South Africa for financial support for the entire research.

I thank Mr Uriri and Miss Adams for proofreading my work I am grateful.

Nobody has been more important to me than my family. I thank my parents (Tholakele and Sthembiso Phehlukwayo), my uncle (Bheki Makhanya) and his wife (Cindy Makhanya) whose love and guidance are with me in whatever I pursue.

Contents

List of Figures

List of Tables

List of Abbreviation

QKD: Quantum Key Distribution

SOP: State of Polarisation

QRNG: Quantum Random Number Generator

APD: Avalanche Photo-diode

BB84: Bennett and Brassard 1984

B92 : Bennett 1992

BS : Beam Splitter

LED: light Emitting Diode

QKDS-A: Quantum Key Distribution Station A

QKDS-B: Quantum Key Distribution Station B

LD: Laser Diode

DL: Delay Line

PM: Phase Modulator

VA: Variable Attenuator

CD: Classical Detector

FM: Faraday Mirror

Chapter 1

Introduction

1.1 Overview

Quantum mechanics is a branch of physics that deals with the mathematical laws that govern the microscopic properties of physical objects [1]. Quantum mechanics showed that light with other forms of electromagnetic radiation comes in small particles known as photons. The photons energy, spectral intensity and colours can also be determined by the laws of quantum mechanics. Physicists at the end of 19^{th} century were certain that most of the fundamental physical principles had been demonstrated and proved accurate. They expected very few improvement to obtain an extra decimal place of accuracy. Thus, the discovery of quantum mechanics and Einstein's discovery of relativity transmogrify the field of physics in the early 20^{th} century [2].

The development of quantum mechanics was initially motivated by two scientific hypotheses which demonstrated the inadequacy of classical physics. These are the ultraviolet catastrophe [3] and the photoelectric effect [4, 5, 6]. Max Planck in 1900 put up a mathematical model that demonstrated the thermal radiation was at equilibrium with a set of harmonic oscillators, a theory that was used to describe the properties of black body radiation [7].

Thereafter, Albert Einstein in 1905 elaborated the photoelectric effect by postulating that a beam of light is a stream of particles known as quanta or photons that possessed an energy that equals the product of its frequency and a numerical constant called the Planck constant [8]. This led to some major discoveries into the understanding of how physical objects behave at the microscopic level: Wave-particle duality where light propagates as wave and in some respects like particles [9, 10, 11, 12] and the Uncertainty Principle [13].

In quantum mechanics, the Uncertainty Principle can be easily described as the more closely one determines one measurement (for instance the position of a particle), the less precise another measurement relating to the same particle (momentum) must become. The wave-particle duality theory was first demonstrated in a double slit experiment in 1827 by Augustine Fresnel [14] and was later observed in the Stern-Gerlach in 1922 [15]. The Stern-Gerlach experiment shows many important aspects of quantum mechanics:

the aspect of the natural world has been shown to be quantised, and only able to take certain discrete values, quantum mechanics is probabilistic [16]. In 1925 Erwin Schrödinger constructed the mathematical equation that elaborates the behaviour of a quantum mechanical wave [17]. The Schrödinger's construct (equation) is important to quantum mechanics. The equation provides an allowable constant state of a quantum system and details how the quantum state of a physical system change in time.

To date, based on some of these theories of quantum mechanics, many technological applications have been developed [18, 19]. The applications of quantum mechanics are numerous, but we will only mention one that is the focus of this work. Using the laws of quantum mechanics, a secure key can be generated. A term now known as Quantum Key Distribution (QKD) [20, 21, 22, 23].

Quantum Key Distribution is a process or a scheme that enables two distant parties named Alice (transmitter) and Bob (receiver) to transfer a secure random key. The secure key is then used to encrypt or decrypt confidential communication taking place over the Internet such as online banking and emails. Physical processes are utilised to transfer information using a quantum carrier in the form of single photons through a quantum channel. Such a channel can be either fibre optics or free-space. The security of QKD is based on the general the principles of quantum mechanics which are invul-

nerable to mathematical algorithms [24] and increases computational power [13, 25, 26, 15]. QKD effectively addresses the challenges confronting classic key distribution approaches, by offering a provably secure cryptographic building block for remote parties to generate cryptographic keys. Quantum Key Distribution can be performed by various protocols. The fundamental protocol is known as the BB84-Bennett and Brassard 1984 [20, 27]. There are products available which can be used to perform this protocol, for example, the id 3000 system [28].

1.2 The objective of this study

This study demonstrates the implementation of the QKD process for the undergraduate physics curriculum. We describe QKD in steps which can be easily followed by the undergraduates students. As a result, a comprehensive manual has been developed. The manual enables undergraduate students to learn the foundations of QKD. The undergraduate curriculum for quantum mechanics course covers subjects such as the wave function, observables, operators and the Uncertainty Principle. For students to be able to follow and understand the process of QKD, they also require an understanding of a quantum bit (qubit), quantum states, quantum measurement, interferometers and no-cloning theorem. We present the id 3000 system as a learning tool in the 3rd year physics laboratory, to introduce undergraduate students to applications in quantum information science. We demonstrate a typical

experiment the undergraduate students can perform in the physics laboratory using the id 3000 system. The study ensures that students gain knowledge of QKD by learning how to implement a QKD protocol and further gain exposure to QKD systems.

1.3 The structure of this study

This study is organised as follows: In Chapter One we give an overview of QKD. In Chapter Two we discuss the fundamental concepts and formalism of quantum mechanics needed for a proper understanding of this technological application. Chapter Three provides the description of QKD and details the steps including the devices required for a successful implementation of QKD. In Chapter Four we present the id 3000 QKD system as a learning tool to improve students understanding of QKD. In Chapter Five we provide methods for utilising the id 3000 system. We then describe a typical experiment that undergraduate students can perform followed analysis and discussion of the results acquired. The last Chapter Six gives the summary and conclusion of the thesis.

Chapter 2

Basics building blocks of QKD

The basic element that provides a mathematical structure in which to understand QKD is known as a quantum state. To any isolated quantum state in quantum mechanics there exists a complex vector space called state space (Hilbert space) [29]. The system can be entirely described by it state vector which is a unit vector in the Hilbert space. In quantum mechanics, a quantum state (state vector) is written as $|\psi\rangle_x$, with inner product given as,

$$\langle\psi|\psi\rangle, \tag{2.1}$$

where $|\psi\rangle$ is called the *ket* and denotes as the transpose of the complex conjugate of $\langle\psi|$ and called the *bra*. The time evolution of a given closed quantum mechanical system is easily depicted by the Schrödinger model or

equation [17] and denoted as,

$$\mathrm{i}\hbar\frac{\mathrm{d}|\psi\rangle}{\mathrm{dt}} = H|\psi\rangle, \tag{2.2}$$

where H, is the Hamiltonian and $\hbar$ is given by $\frac{h}{2\pi}$ where h is the Planck's constant. Thus, the time evolution of a constant quantum state is given as,

$$|\psi'\rangle = \mathrm{U}|\psi\rangle, \tag{2.3}$$

where U, is a unitary operator. Alternatively, a quantum state can be introduced with a density operator which is presented as,

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

where the coefficients P_j are non-negative and add up to one. The next section deals with one of the simplest quantum mechanical systems called a qubit.

2.1 A qubit

A qubit or more accurately a quantum bit is a unit of quantum information. It is the quantum version corresponding to a classical bit that can be used for communication [18]. A classical bit has a state of either 0 or 1, however a qubit is defined as a two level system $|0\rangle$ and $|1\rangle$. The difference between

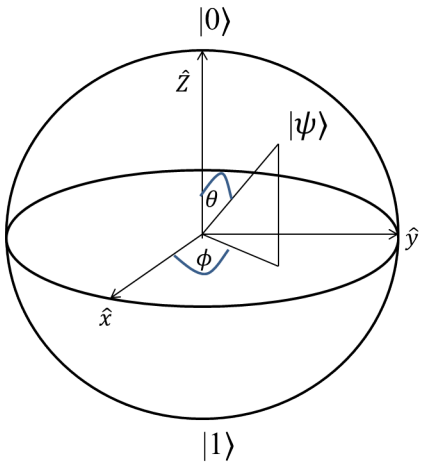


Figure 2.1: The schematic diagram known as the Bloch sphere, shows a qubit, the two level system with state $|0\rangle$ and $|1\rangle$ [18].

the classical bit and qubit is that a qubit can exist in a super-position (that is, the linear combination) given as,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.5}$$

where alpha (α) and beta (β) provide the probability amplitudes of the quantum system. The normalisation amplitude is equivalent to the absolute square that α and β and is given as:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.6}$$

The structure that perfectly represents a qubit is called the Bloch sphere [18]. In the Bloch sphere, states are presented as unit vectors with three

dimensions x, y and z as given in Figure 2.1.

A qubit in a super-position behaves according to a principle which states that: A qubit may be in a number of states simultaneously such as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ until observed at which point the super-position collapses down to a single state [30]. This means the probability for a linear system (qubit) to collapse to a state $|0\rangle$ is normalised to $|\alpha|^2$ and for a state $|1\rangle$ is normilised to $|\beta|^2$. A qubit can also be represented by polarising light. The next section discusses polarisation.

2.1.1 Polarisation of light

Students are familiar with light as an electromagnetic wave in a classical manner. In quantum mechanics, they meet the particle nature of light and the concept of single photons [5, 15]. The property of an electromagnetic wave is the polarisation. The direction of light in which single photons propagate can be positioned into polarisation components namely: horizontal state $|H\rangle$ (0^0), vertical $|V\rangle$ (90^0) and in diagonal ($|-\rangle$ and $|+\rangle$) which corresponds to (-45^0 and 45^0). This can be achieved using a polarisation filter. A filter, can polarise light in a sense that is parallel to the filter axis [31]. For example, a qubit that is in superposition illustrated in equation (2.5) has $|\alpha|^2$ probability to be transmitted in the vertical direction. [31].

Example 1

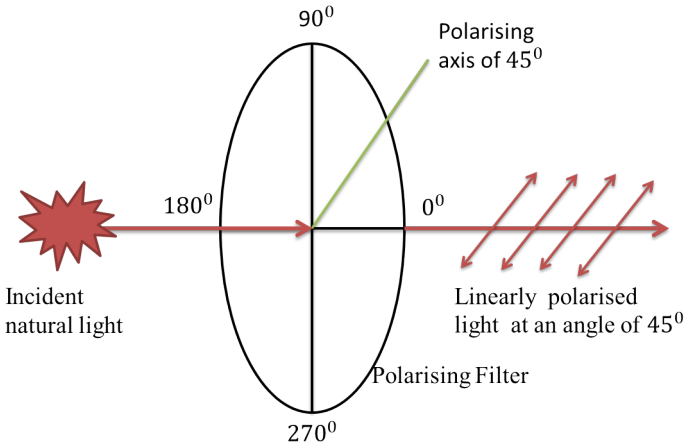


Figure 2.2: In the schematic an incident light is projected through a polariser set at 45^0 which is diagonal state. As illustrated the outcome of the light provides a diagonal 45^0 linearly polarised state $|+\rangle$.

Suppose we have a light with single photons propagating through a polarisation filter that is set at an angle of 45^0. The single photons which will be transmitted are the ones parallel to the polarisation axis, the other light will be blocked. The illustration of a linearly polarised light is shown in Figure 2.2.

Example 2

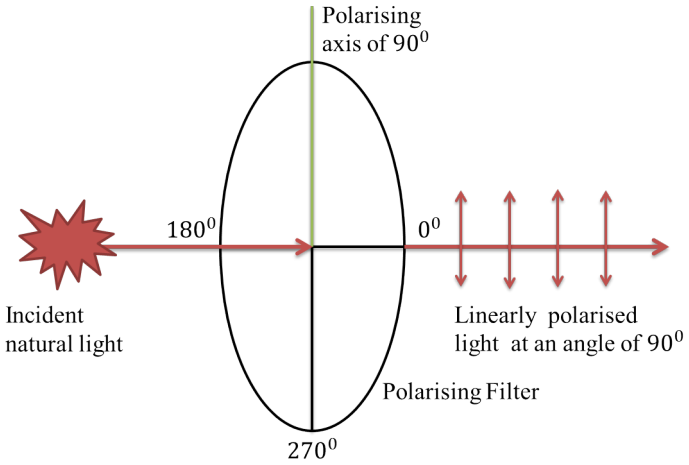


Figure 2.3: The incident light pass through a polarisation filter set at 90^0, a linearly polarised vertical 90^0 light is produced which gives a $|V\rangle$ state.

When a polarisation filter axis is set at 90^0, single photons oscillate in the direction of a polarising filter which is the vertical direction, as illustrated in Figure 2.3.

Example 3

The polarisation filter set at -45^0 transmits a linearly polarised state parallel to the filter axis as presented in Figure 2.4.

Example 4

In the cases where a filter is set to transmit horizontal state $|H\rangle$ at 0^0. It produces a state parallel to filter axis, as illustrated in Figure 2.5

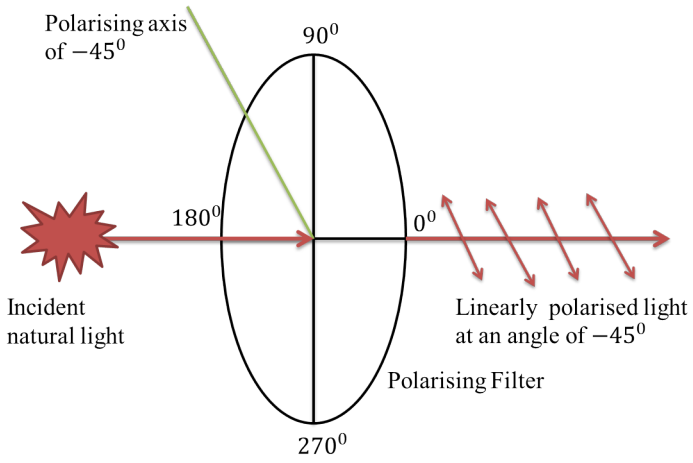


Figure 2.4: A incident light coming to pass through a polariser set at diagonal -45^0, as it illustrated in the diagram a linearly polarised diagonal -45^0 light is produced and it gives a state that is diagonal $|-\rangle$ state.

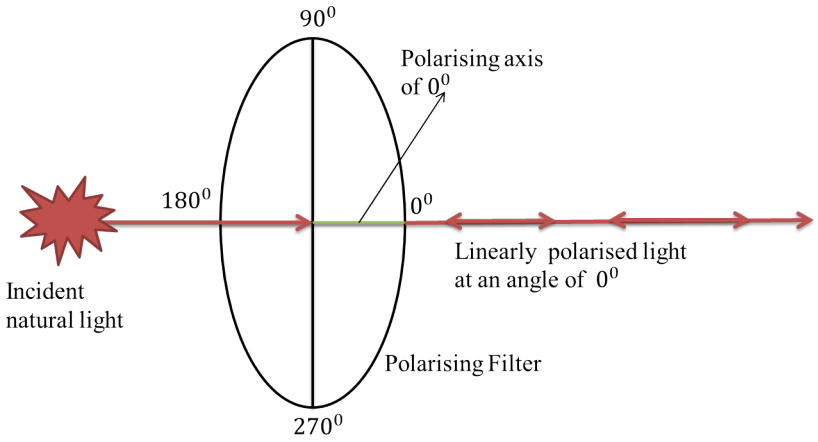


Figure 2.5: The incoming incident light passes through a polariser set at 0^0, then a linearly polarised horizontal and it gives a $|H\rangle$ state.

These linearly polarised states where it comes to measurements, can be mea-

sured in the rectilinear linear basis and diagonal basis. The rectilinear basis is formed by vertical (90^0) and horizontal (0^0) polarisation. The diagonal basis is formed by 45^0 and -45^0, as shown in Figure 2.6. These measurements could be sometimes be affected by a phase. For example, relative phase. This shall be discussed in the next section

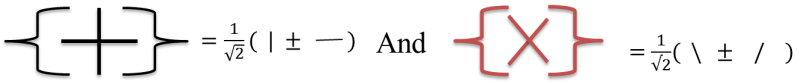


Figure 2.6: The representation a linearly polarised light where a quantum state (qubit) is measured in the rectilinear base and diagonal base [32].

2.1.2 Phase

Phase can be classified into two major types, the global and relative phase. For example, $e^{i\theta}$ $|\psi\rangle$, where $e^{i\theta}$ is the global phase factor for which $|\psi\rangle$ is a real number. During measurement, however, the global phase factor can be ignored, but the relative phase manifests itself. The relative phase is the waveform obtained at a constant frequency (sine wave). In practice, a relative phase shift can be determined with the use of the Mach-Zehnder interferometer [33]. A Mach-Zehnder interferometer is a highly configurable and very flexible interferometer used to demonstrate interference of single photons which is one of the examples of superposition principle [33]. The Mach-Zehnder interferometer is sketched in Figure 2.7. Single photons that

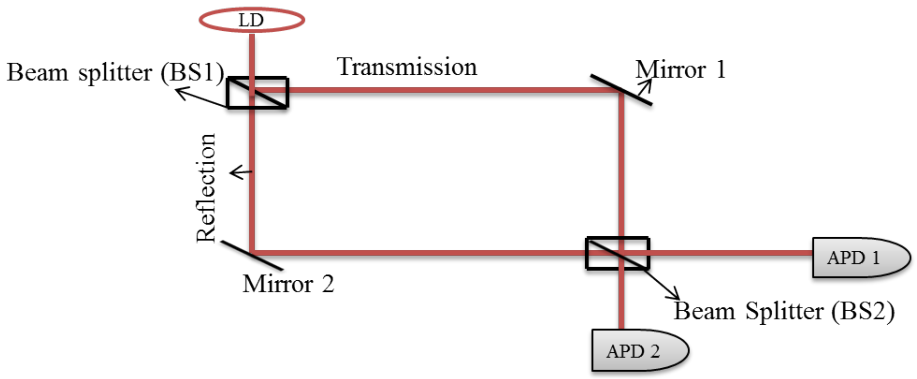


Figure 2.7: The schematic of the Mach-Zehnder interferometer, another example for superposition principle (single photon interference) [34].

are emitted from the laser diode (LD) are split at the first beam splitter (BS1) into two arms or axes: Transmission and Reflection [35]. The single photons in the Transmission and Reflection axis get recombined at the second beam splitter (BS2). The output of BS2 is then measured by either, detectors known as Avalanche Photo-Diode (APD1) or (APD2). The reflection axis carries a relative phase of $\frac{\pi}{2}$. In the Mach-Zehnder interferometer, the path length of the axes (Transmission and Reflection) must be equal in order to clearly see the interference of single photon. The visibility of the single photon interference decreases as the path length differs.

2.2 Heisenberg Uncertainty Principle

In general, the Heisenberg Uncertainty Principle states that: the more closely one determines one measurement (for instance the position of a particle), the

less precise another measurement relating to the same particle (momentum) must become. This explains that one cannot measure the qubit propagating without disturbing the process [36, 37]. For example, if one performs some measurement on the qubit without knowing the position of the state, such a measurement yields an ambiguity (perturbation) in the state. Perturbation means a state is disturbed and has changed to another state which is different to what it was before. This principle around quantum mechanics application makes it possible to achieve things which cannot be done in the classical physics.

2.3 No-cloning theorem

Cloning means making a copy. For example a qubit $|0\rangle$ being transformed to a state $|00\rangle$, the same can be done with state $|1\rangle$ to a state $|11\rangle$. In quantum mechanics, it is impossible to make such transformation (perfect copy) of an unknown state with perfect accuracy. This is called the no-cloning theorem [38]. The no-cloning theorem forms an important property in the security of QKD. The theorem prevents an eavesdropper from tempering the communication channel and making copies of the transmitted quantum state. We shall see in the next chapter how this can be achieved.

These basic concepts and formalism of quantum mechanical properties are useful in today's technology application such as QKD. They are used to

achieve a safe transmission between the remote parties. With this information, students will have a full understanding of QKD.

Chapter 3

Quantum Key Distribution

Quantum Key Distribution is a process that utilises properties of quantum mechanics to enable two distant parties named Alice and Bob to randomly generate and exchange a secure cryptographic key [20]. The goal of QKD is for two remote parties to exchange a secure key which can then be used to encrypt and decrypt information. The description of QKD is illustrated in Figure 3.1. The communication is implemented by applying a protocol to encode information in single photons as qubits. This encoded information is exchanged between Alice and Bob across a quantum channel.

The transmission of single photons (qubits) is protected by the Heisenberg Uncertainty Principle and the no-cloning theorem. Any unauthorised eavesdropper, Eve, who might try to extract the qubits in the quantum channel will be revealed, as this will disturb the state. The unique property of QKD

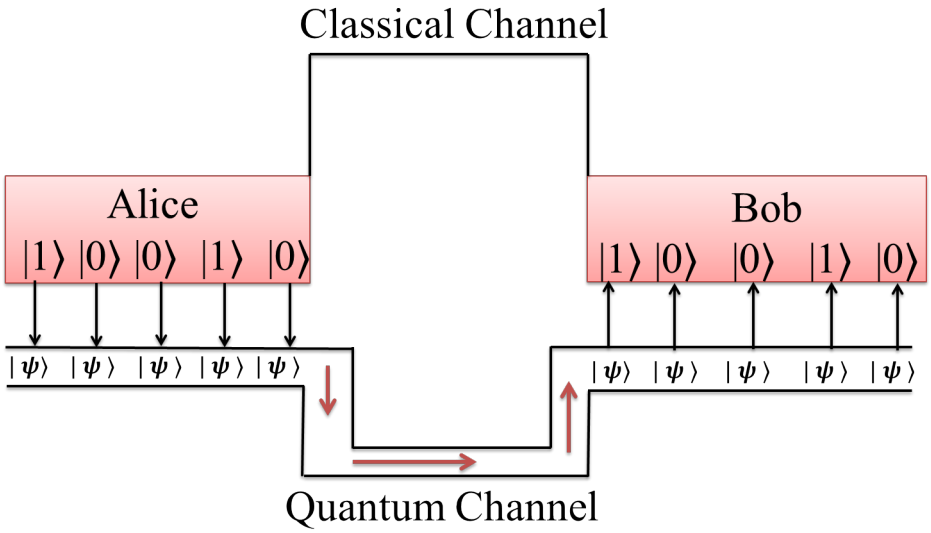


Figure 3.1: The illustration of a QKD scheme, where Alice is the transmitter and Bob is the receiver. The information Alice is transmitting is carried by a state and is sent to Bob.

is that Alice and Bob have the ability to detect eavesdropping. The second channel within the QKD scheme represented in Figure 3.1 is the classical channel which is used to detect the eavesdropping that might have occurred during the key exchange process, this process shall be more detailed in section 3.2.2. A QKD system is achieved with the use of special hardware such as a single photon source, a phase modulator, detectors and a quantum random number generator.

3.1 Devices to build a QKD system

3.1.1 A single photon source

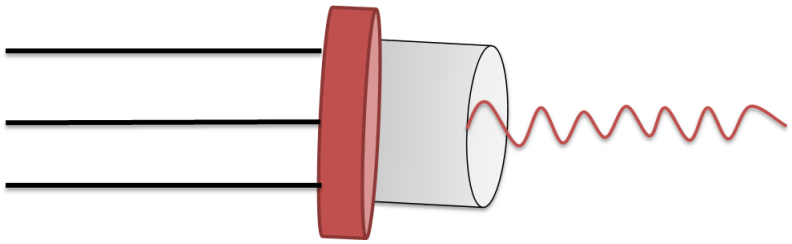


Figure 3.2: The schematic of a single photon source known as laser [39].

A single photon source is a device that emits single photon at a time. The most common source used to perform this task is called an attenuated laser. The attenuated laser weakens a strong light beam to produce a single photon at a given time. An ideal single photon source produces single photon states with 100 % probability. In a QKD system, attenuated lasers are the most important devices, as they generate single photon per light pulse to encode the information. A schematic of a laser source is sketched in Figure 3.2.

3.1.2 A Phase Modulator

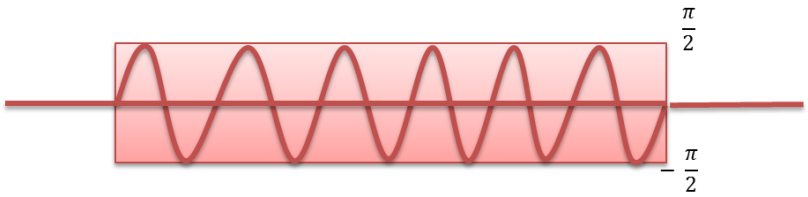


Figure 3.3: A schematic of a Phase Modulator utilised in a QKD system [40].

A phase modulator (PM) is an optical modulator designed to control the phase of single photons by keeping the amplitude of the signal constant as illustrated in Figure 3.3 [40]. Within a QKD system, the PM carries out the phase (pulses) of all single photons emitted from the source. It then maintains the phase such that a constant amplitude is obtained. The modulation of pulses is performed by setting the frequency which can be efficient for pulse emission. This type of optical modulator can also be employed to switch between different phases often called phase shift. It is classified as a tool which can be used for processing information.

3.1.3 A detector

Figure 3.4: Is the image of detector known as the APD used in QKD systems [27].

A detector in QKD systems can be required to count the transmitted single photons and release signal as the output. There exist major counting detectors designed to perform this task, with the Avalanche Photo-diodes (APD) being the most widely used for implementation of QKD [27]. The APD is designed to operate within the wavelength ranges from (900 - 1700 nm). This range makes it possible for an APD to give efficient detection (correct) counts and can easily control dark counts (noise). The APD have a break down voltage ranging from (20 - 40 V). Such low voltages have a potential for providing high and visible single photon detection. The timing detection event of single photons in an APD is achieved up to 100 MHz frequency. We have shown the image of an APD in Figure 3.4.

3.1.4 A Quantum Random Number Generator

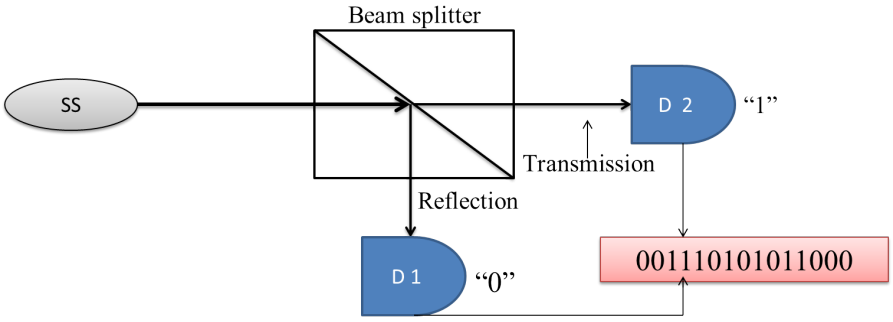


Figure 3.5: Schematic of a Quantum Random Number Generator (QRNG) [41].

A Quantum Random Number Generator (QRNG) is a device which can be utilised to generate a bit sequence based on the probabilistic nature of quantum mechanics [41]. QRNG exploits elementary quantum optical processes as a source of pure randomness. Using quantum mechanical properties, single photons are emitted from a laser and sent through an optical element known as a beam splitter [41]. The light pulses are split into two equal proportion, reflection or transmission. The reflection and transmission light pulses are detected to produce a 0 or 1 as is illustrated in Figure 3.5. Such quantum processes provide instantaneous and true entropy. In a QKD system, this type of a QRNG is exploited to randomly choose the encoding of the bits.

3.2 The steps to produce a secure key

In a QKD system, a secure key (cryptographic key) is produced using quantum mechanical properties together with the devices and channels. The channels are namely: a quantum channel and a classical channel, which play a major role in producing a secure key. There exist steps which need to be followed using these channels in a QKD system.

3.2.1 A quantum channel

A quantum channel is a medium in which single photons are transmitted [42]. A quantum channel is of two forms: memoryless (noisy) and memory (noiseless). A memoryless quantum channel is a type in which single photons flow from the system to the environment whereas a memory quantum channel is one where single photons flow from the environment to the system as shown in Figure 3.6 [43]. In a QKD system, a noisy channel is of particular interest. This is because it has an ability to highlight any eavesdropping.

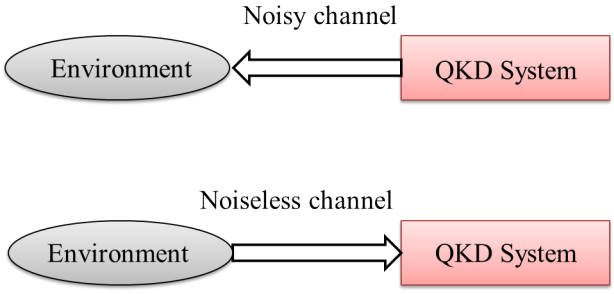


Figure 3.6: The illustration of a quantum channel applicable for the implementation of QKD [42].

The quantum noisy channel can be either free-space or fibre optics. Free-space is a medium that involves the atmosphere (air). Fibre is a medium that implements fibre optics cable to guide single photons from point-to-point. The purpose of these quantum channels in a QKD system is to allow the distribution of single photons to be transferred from Alice to Bob. The distribution of single photons contains the information used by Bob to produce the raw key.

3.2.2 A classical channel

A classical channel is generally known as a public channel which takes place over the Internet. In QKD systems, this particular type of channel is used to authenticate a distributed key. Authentication is known as key distillation, it is the process of addressing errors which may have occurred during the transmission [44]. The implementation of QKD is bound to have these errors. This is due to the imperfection of equipment and disturbance over the quantum channel which can be referred to as noise. Alice and Bob address all the errors by performing post-processing which involves sifting, error estimation, error correction and privacy amplification.

Sifting

A sifting process is a step Alice and Bob perform after exchanging single photons. In this step, Bob discusses the measurement he has used for every single photon received. Alice compares Bob's measurements with the single

photons polarisation sequence for the transmission. If there exists some compatibility in the basis used to prepare and measure the single photon, they keep that bit otherwise the bits of incompatible bases are discarded. This procedure results in the generation of the sifted key.

Error estimation

The error estimation process is a step Alice and Bob perform after obtaining the sifted key. In this step, Alice and Bob find the errors committed during the transmission. Once they have obtained the errors, Alice and Bob apply an algorithm such as the Cascade algorithm [45]. This algorithm allows Alice and Bob to test the small portion of the bits in the sifted key. All the errors are attributed to eavesdropping in the sifted key [27]. The small string tested can be removed and the remaining sifted key is used to perform the error correction.

Error correction

The error correction process is a step Alice and Bob can perform if they have observed errors in the sifted key. The performance of error correction can be applied to the remaining sifted key in which they use an algorithm called the hash function [22]. The algorithm assists in correcting all the errors in the the sifted key. Once this step is achieved, the last step towards a final key is privacy amplification.

Privacy amplification

The privacy amplification process is a step Alice and Bob perform to produce a secure key. Alice and Bob carry out privacy amplification on the corrected sifted key. The privacy amplification comes with a high probability of making sure that all the errors (Eve gaining information) are eliminated in the key [46]. This process applies a universal hash function algorithm to eliminate whatever information Eve might have gained [46, 47]. Hence, a secure key is produced. Figure 3.7 gives the summary of all the steps that are followed in a QKD system to produce a secure key.

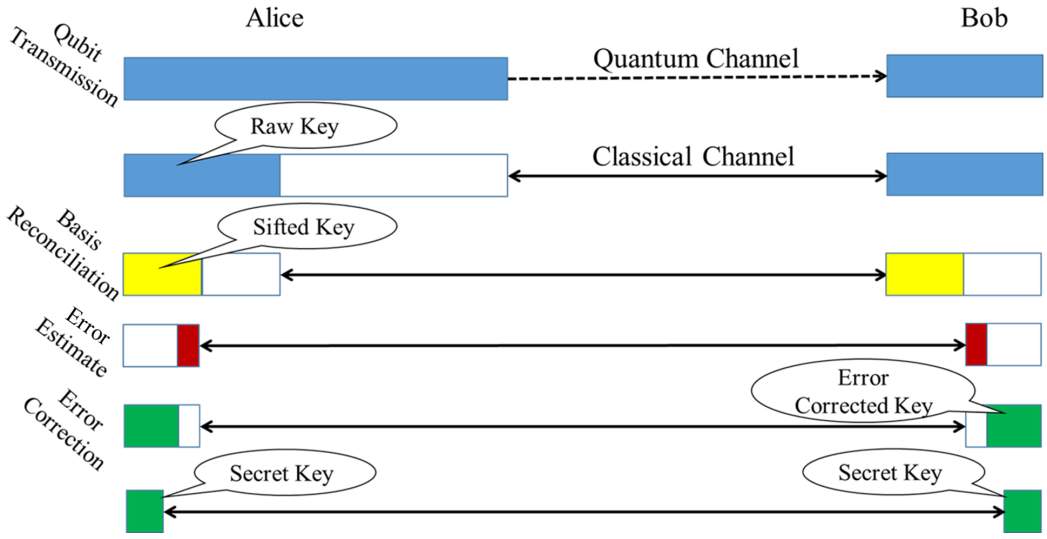


Figure 3.7: The generation a secret key in a QKD system can be summarised by this diagram [28].

3.3 Methods of encoding information

Encoding information can be performed by various methods in QKD systems. The simplest method can be done using either polarisation or the phase approach. These two approaches can be implemented using the BB84 (Bennett and Brassard 1984), SARG04 (Scarani, Antonio, Ribordy and Gisin (2004)) and B92 (Bennett 1992) protocols.

3.3.1 BB84 Protocol

BB84 protocol was invented by Bennett and Brassard in 1984. The protocol is a prepare and measure scheme which employs four quantum states to encode information [20]. The encoding procedures of this protocol shall follow.

Polarisation encoding BB84

A BB84 protocol is implemented using four quantum states based on the pulses of light that contain single photons polarised in vertical, horizontal, $+45^0$ and -45^0 direction. This operation forms two sets of polarisation bases, namely rectilinear (vertical and horizontal polarisation) and diagonal ($+45^0$ and -45^0 polarisation) bases [20, 22]. Alice performs transmission by encoding qubit into single photons through polarisation. For example, bit 0 corresponds to a horizontal (0^0) polarised state, bit 1 to a vertical (90^0), bit 0 to a diagonal (-45^0) and bit 1 to a diagonal (45^0) state. This method is sketched in Figure 3.8. Using a quantum channel, for example, free-space,

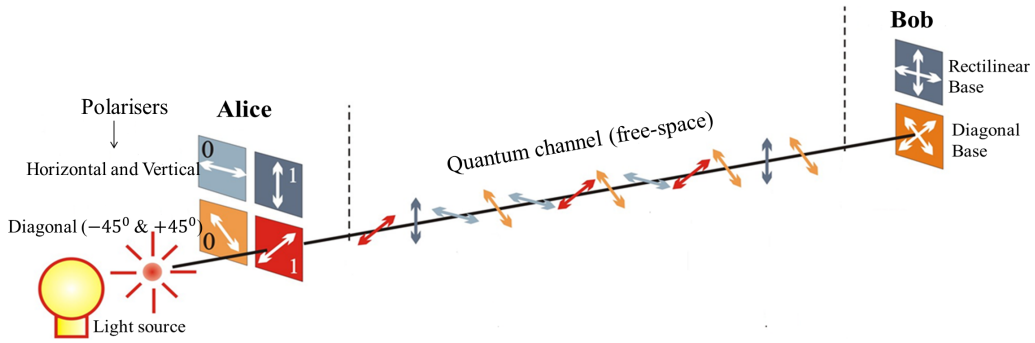


Figure 3.8: Polarisation encoding for a BB84 protocol. Alice encodes the information in the four polarisation states as illustrated in the diagram and Bob measure the polarised single photon using two bases in his location [48].

Alice transmit a string of bits to Bob. For each bit of information, Alice randomly chooses the polarisation state of a single photon. Bob randomly choose a polarisation basis to measure the single photons received. This procedure results in the generation of the raw key.

Using a classical channel, for example, the Internet, Bob discusses the measurement bases he has chosen for every single photon received. Alice compares Bob's measurement with the single photons polarisation sequence that she has implemented for the transmission. If there is compatibility in the base they keep the bit and discard unrelated bases. The compatible bits form a sifted key which then undergoes error estimation, error correction and privacy amplification. Traditionally, these steps result in a secure key. In Table 3.1, we show how the distribution of single photons is accomplished between Alice and Bob.

Table 3.1: The measurements for a polarisation encoding method in BB84 protocol

Alice's bit	1	1	0	0	0	1	0	0	1	0	1
Single photon polarisation	↗	↑	→	↖	→	↗	↖	→	↗	↖	↑
Bob Bases	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊗	⊗	⊕	⊕
Bob detection	0	1	1	0	0	1	1	0	1	0	1
Public discussion	N	Y	N	Y	Y	Y	N	Y	N	Y	Y
sifted key	-	1	-	0	0	1	-	-	1	-	1

Phase encoding BB84

Phase encoding is a method applied using the Mach-Zehnder interferometer [35]. Alice and Bob are separated by a few kilometres. Using an interferometer, maintaining the path length of the two axes can be difficult due to environmental factors. A way to resolve this issue is to apply two different (unbalanced) interferometers. This approach allows the first interferometer to control the single photons picked by the short arm in Alice's interferometer and Bob's interferometer. The second interferometer controls the single photons that taken the long path. Figure 3.9 provides the method of phase encoding applied using BB84 protocol.

The key distribution process is possible using states encoded in four possible phase shifts [35]. Alice generates the bits by applying four possible phases such as 0, $\frac{\pi}{2}$ for bit 0 and π, $\frac{3\pi}{2}$ for bit 1 through the interferometer. For

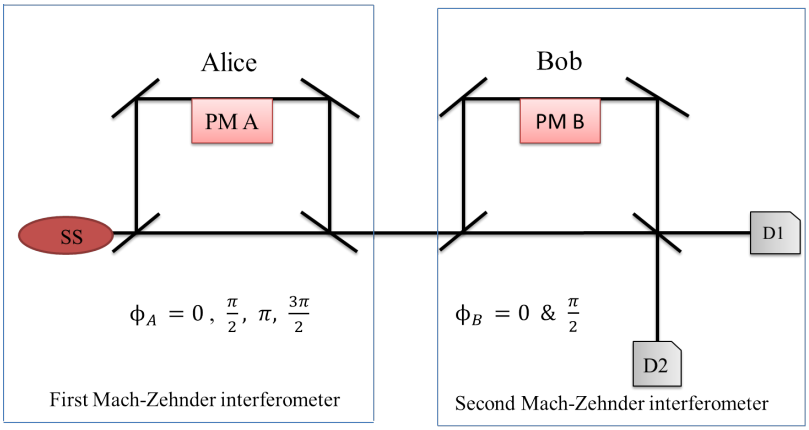


Figure 3.9: The schematic diagram showing phase encoding method for a BB84 protocol, where Alice randomly performs the encoding in the four possible phase shift given in the first Mach-Zehnder. The receiver Bob then perform the measurement using a phase shift shown in the second Mach-Zehnder interferometer [33].

each single photon pulse Alice is transmitting, a phase modulator is applied to randomly shift the pulse to any of the four choices 0, $\frac{\pi}{2}$, π and $\frac{3\pi}{2}$. Bob measures the incoming pulses using a phase choice of $\Phi_B = 0$ and $\Phi_B = \frac{\pi}{2}$. During this process, Bob randomly chooses a basis by performing a 0 or $\frac{\pi}{2}$ phase shift. If there exist interference single photons (super-position), detector (D1) triggers and detector (D2) triggers in the pluses with a phase of $\frac{\pi}{2}$. These detectors D1 and D2 are registered as bit 0 and bit 1 respectively. The two parties discuss their phase measurements. They match the phase difference (Φ_A - Φ_B), in situations where phase difference observed as 0 or π. This indicates compatible bits which results in a distribution of a raw key. Table 3.2 gives the summary of this encoding method.

Table 3.2: Summary of the key exchange when phase encoding is performed based on the BB84 protocol

Bit Value	ϕ_A	ϕ_B	$(\phi_A - \phi_B)$	Bit value
0	0	0	0	0
0	0	$\frac{\pi}{2}$	$\frac{-\pi}{2}$	-
1	π	0	π	1
1	π	$\frac{\pi}{2}$	$\frac{\pi}{2}$	-
0	$\frac{\pi}{2}$	0	$\frac{\pi}{2}$	-
0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	0
1	$\frac{3\pi}{2}$	0	$\frac{3\pi}{2}$	-
0	$\frac{\pi}{2}$	$\frac{\pi}{2}$	0	0
1	$\frac{3\pi}{2}$	0	$\frac{3\pi}{2}$	-
1	$\frac{3\pi}{2}$	$\frac{\pi}{2}$	π	1

3.3.2 SARG04 Protocol

SARG04 protocol was introduced by Scarani, Antonio, Ribody and Gisin in 2004 (SARG04) [49]. The protocol is an improved version of the well known BB84 and was developed with the purpose of strengthening the security of QKD [50]. This protocol is resistant to Photon-Number Splitting (PNS) attacks that takes place when an attenuated laser is used which may emits more than one photon per pulse. SARG04 protocol further allows the implementation of QKD to still function over connections with high losses (noise). In particular SARG04 protocol can achieve high secret key rate at longer distances than BB84.

The procedure of the SARG04 protocol is the same as the BB84 for the transmission of single photons (qubit) in the quantum channel, however, differs in the step where Alice and Bob utilises the classical channel. Using a classical channel, Alice does not reveal the basis of her encoding, however, she reveal a pair of non-orthogonal states she has used. Bob performs measurement in one of the orthogonal states provided by Alice. If Bob used the correct basis, he will measure the correct state. This process leads to Alice and Bob sharing compatible bits. This protocol is implemented within the id 3000 QKD system and will be further discussed in Section 5.2.

3.3.3 B92 Protocol

B92 Protocol was defined by Bennett in 1992. The implementation of the B92 protocol involves two quantum states shall be detailed below [21].

Polarisation encoding B92

A secure key distribution is successful using a two quantum state based on pulses of light that contain single photons with polarised state along with 45° and 90° respectively. In this protocol, Alice and Bob first make an agreement through classical channel (Internet) on how to perform the encoding. The two participants agree that Alice will transmit single photons to Bob using two non-orthogonal polarisations such as 45^0 for diagonal linearly polarised state and 90^0 for a vertical linearly polarised state. These preparations of Alice corresponds to bit 1 and 0 respectively. Bob on the other side uses two non-orthogonal polarisation state in the diagonal direction of -45^0 for bit 0 and horizontal direction 0^0 for bit 1. These polarisation states are orthogonal to one of Alice. The scheme is shown in Figure 3.10. Using a quantum channel, free space. Alice randomly encodes bit 0 or 1 by polarising single photons according to the rule. The linearly polarised light (single photons) is then transmitted to Bob. When Bob receives light (single photons), he performs measurements and detection using a polarisation analyser and a single photon detector. If Bob analyses a single photon for example, along 0^0, he will infer that it was sent in a diagonal direction hence Alice sent a single photon with 45^0 polariser. Bob will register detections of a bit 1 through 0^0

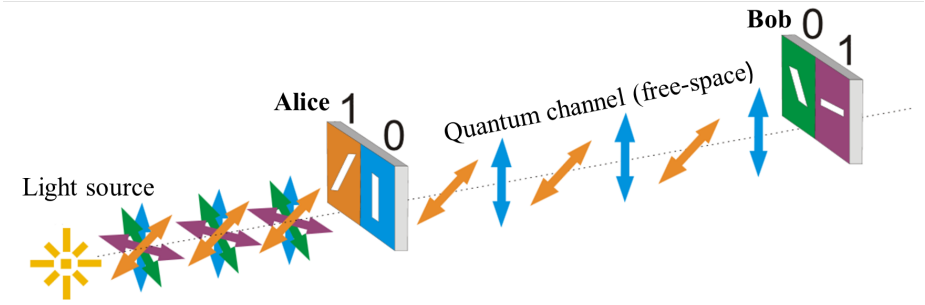


Figure 3.10: Polarisation encoding for a B92 protocol Alice perform the encoding by randomly polarising light either vertical (90^0) or diagonal(45^0) to encode 0 or 1 respectively. Bob perform measurements in the incoming single photons by applying polarisation filter in one of two directions orthogonal to Alice polarisations which are horizontal $0°$ or diagonal $-45°$ to measure 1 or 0 respectively. [51].

and bit 0 through 45^0.

The two participants utilise the Internet as a classical channel. Alice and Bob acquire a sifted key without revealing the polariser used for each measurement. Alice and Bob keep only the detection results which then form a key called the sifted key. The measurements for the B92 protocol is presented in Table 3.3.

Table 3.3: The measurements for a polarisation encoding method in B92 protocol

Alice's bit	1	0	1	0	1	0
Single photon polarisation	↗	↑	↗	↑	↗	↑
Bob's polarisation	↖	→	→	↖	→	↖
Bob's measurement	0	1	1	0	1	0
Bob's result	N	N	Y	Y	Y	Y
sifted key	-	-	1	0	1	0

Phase encoding B92

A phase encoding method for B92 protocol is also implemented with two Mach-Zehnder interferometers [35]. The first interferometer belongs to Alice and the second interferometer belongs to Bob as presented in Figure 3.11. The key exchange process between Alice and Bob for this method is achieved using two quantum states encoded in two possible phase shifts in the first interferometer [35]. Alice generates the bits by applying two possible phase shifts of 0 for bit 0 and $\frac{\pi}{2}$ for bit 1 in the interferometer. Bob measures the incoming single photons pulses using a phase shift of $\Phi_B = \pi$ for a bit 1 and $\Phi_B = \frac{3\pi}{2}$ for a bit 0.

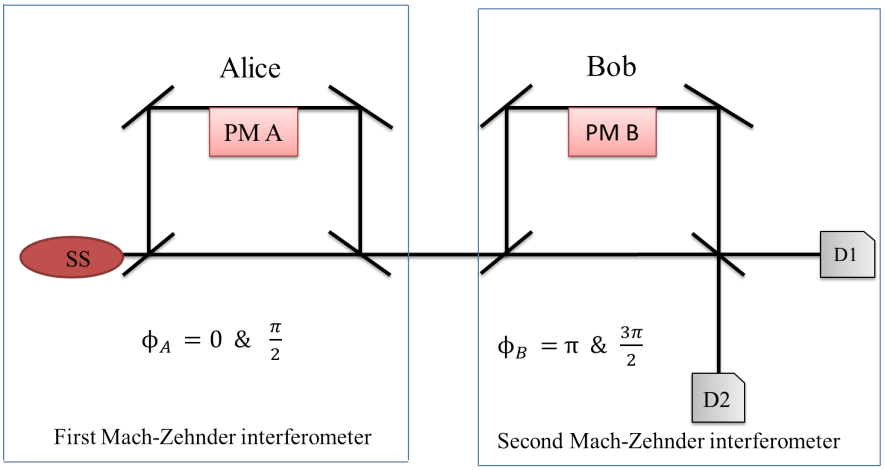


Figure 3.11: Phase encoding for B92 protocol, as provided in the diagram Alice perform two choices of phase shift to encode the bit using the first Mach-Zehnder interferometer. Bob apply phase shift shown in the second Mach-Zehnder to measure the incoming single photons pulses [33].

3.4 Eavesdropping within a quantum channel

There is a probability for Eve to perform attacks in the quantum channel. There exist many ways Eve may try to gain information in a QKD system. The common attacks Eve can use are known as intercept-resend [52] and faked state attack. This work will discuss the intercept-resend attack.The intercept-resend strategy is when Eve aims at obtaining the information without being detected. This attack can be performed either in polarisation or phase encoding.

3.4.1 Polarisation encoding with Eve

The single photons Alice sends can be blocked by Eve. This strategy allows Eve to prepare and send new single photons to Bob as shown in Figure 3.12. This will lead to an error in the transmission line. During this process, there is a 50 % probability to obtain an exact measurement base of the single photons, in cases where Eve used the wrong base to measure. There is also a 50 % probability Eve's measurement could be correct. This means that, there is 25 % probability for single photons successfully measured by Eve to produce an error in the key. They match transmitted bits, over a classical channel to check if the bits were eavesdropped. Since QKD is bound by the laws of quantum mechanics, any attacks made by Eve will lead to errors or disturbances in the transmission which will be detected and removed. Therefore this type of attack can be detected [53].

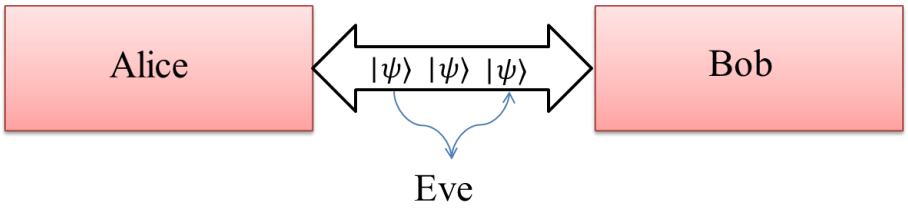


Figure 3.12: Polarisation encoding with Eve in the middle shows Eve extracting states in the quantum channel and it being sent to Bob as a new single photon state [53].

3.4.2 Phase encoding with Eve

A phase encoding method can be eavesdropped by loopholes in the interferometer [54, 55]. This attack is called phase mapping. Eve re-maps Alice's phase shift as demonstrated in Figure 3.13, by transmitting single photon pulses which transmit through the quantum channel towards Bob's location. For example she replaces $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ with $0, \mu, 2\mu, 3\mu$ [55]. However, since Eve can manipulate the phase shift, this means, she can also intercept the phase difference by implementing an intercept-resend attack without remapping the phase. This attack will lead to an error rate of 25 % which will be observed by Alice and Bob. Such high error rate leads to a discarding of information between Alice and Bob. A tolerable error rate for a BB84 protocol is up to 11 %.

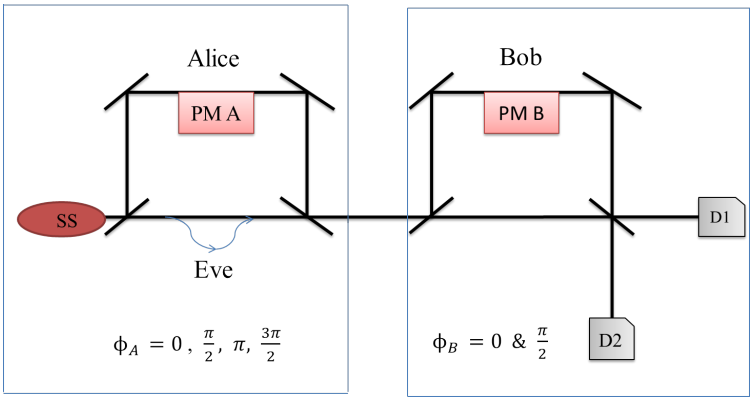


Figure 3.13: Schematic diagram of phase-mapping attack for a BB84 protocol. Eve in this attack tries to re-map phase shifts used by Alice and replaces with her four phase shift given in Alice's location and transmit to Bob

Chapter 4

QKD system as a learning tool

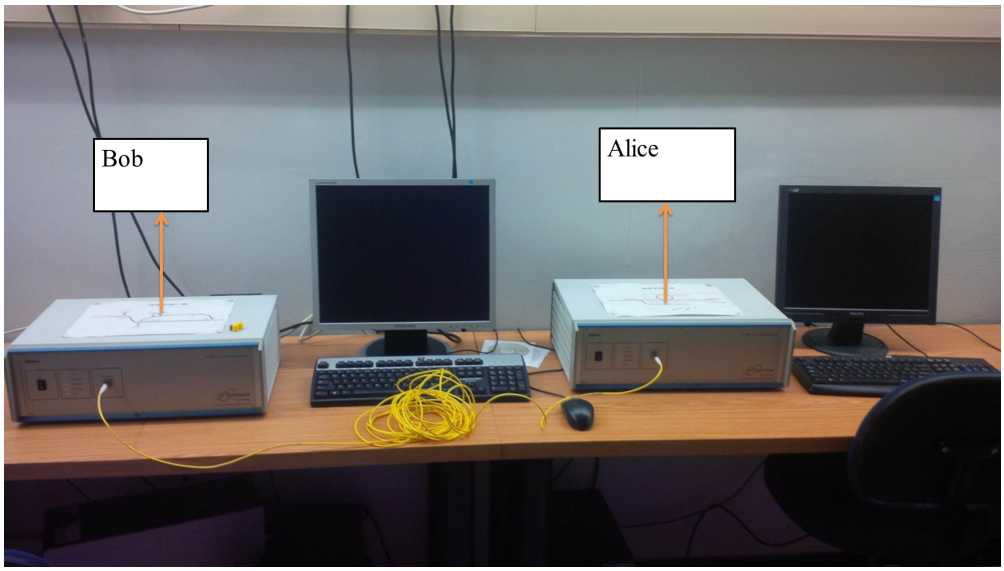


Figure 4.1: The QKD system id 3000 provides two system, Alice and Bob.

Today various platforms have been developed for QKD. A product such as the id 3000 system is available in the market. These systems are designed

based on the phase encoding method to perform QKD. Here we present the id 3000 system as a learning tool. The id 3000 system is a fibre based system developed by IDquantique in Switzerland in the year 2005. The system is designed to implement QKD up to 100 km. It works as an auto-compensating device, which is stable and requires no alignment. It is very easy to utilise and is operated through the use of software specifically written by IDquantique [56]. The system is developed to generate and share random secure keys between two remote parties. The id 3000 system is designed to support the phase encoding of a BB84 and SARG protocol. The key component of id 3000 system is the interface which allows participants to electronically record experimental data. The interface comprises of Alice's system and Bob's system which is controlled via two computers and employs fibre optics as a quantum channel to link the two users. The id 3000 system is presented in Figure 4.1, Alice is the transmitter and Bob is the receiver.

4.1 Alice's system

Figure 4.2: The image present Alice's system, inside the box there is a 12 km fibre roll planted in the system and electronic devices next to a fibre roll.

Alice's system consists of the optical and electronic components as shown if Figure 4.2. The optical components are responsible for performing the transfer of single photons to Bob's system. The electronic components provide high-level operation in monitoring the available devices in the system. The entire scheme of Alice's system will be discussed later in the chapter.

4.2 Bob's system

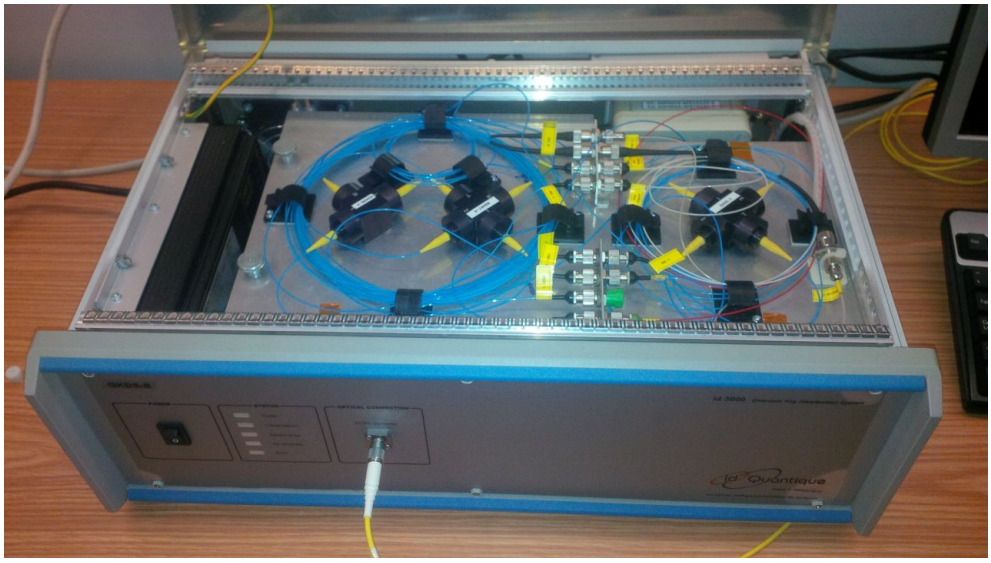


Figure 4.3: This image provides Bob's system. Inside the box there exist optical components which are connected through fibre optic.

Bob's system also comprises of optical and electronic components which are dedicated to performing the measurements of the single photon. The optical components assist in ensuring that the light pulses are transferred to Alice and received back as single photons for measurement. As it can be seen in Figure 4.3, the connections within the system are performed using the fibre. The electronic component provides high-level operation in monitoring all the devices in the system. The rest of the system will be discussed in section 4.4.

4.3 Fibre optics

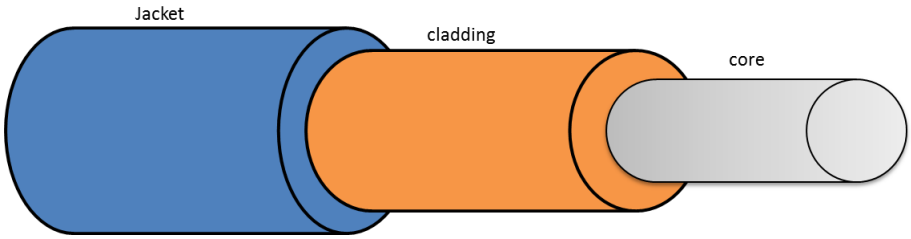


Figure 4.4: A schematic of a fibre optic cable [57].

A fibre is utilised to transmit information in the form of single photons from point to point. The centre of the fibre is called the core which is surrounded by a layer of cladding, and provides a path for light to travel. The difference in refractive indices of the core and the cladding ensures that the light (single photons) is contained within the core of the fibre [57]. Such a fibre cable is illustrated in Figure 4.4.

Fibre optics are characterised by transmission wavelength and it varies from 800, 1310 and 1550 nm. Fibres with a wavelength around 800 nm have high losses, due to the fact that they are employed for short distances. Due to this, they are employed for short distances. Whereas optical fibres with a wavelength of 1300 and 1550 nm provide a very low loss of about 35 dB and 20 dB respectively. Such fibres are utilised for long transmission distances and are ideal for quantum signals.

The disadvantage of fibre optics is its birefringence. The birefringence occurs due to stress within the fibre as light propagating in the fast axis travels at a higher group velocity and therefore splits between the polarisation which can yield to dispersion [57]. The dispersion is the major effect that broadens pulses hence causing them to overlap. This is one of the reasons polarisation encodings is not the choice in fibre based QKD systems. Due to such challenges, fibres with 20 dB losses limit the transmission when the distance is very long. The id 3000 system utilises 1550 nm wavelength as information carriers which is called single-mode fibre. [58].

4.4 Internal design of the id 3000 system

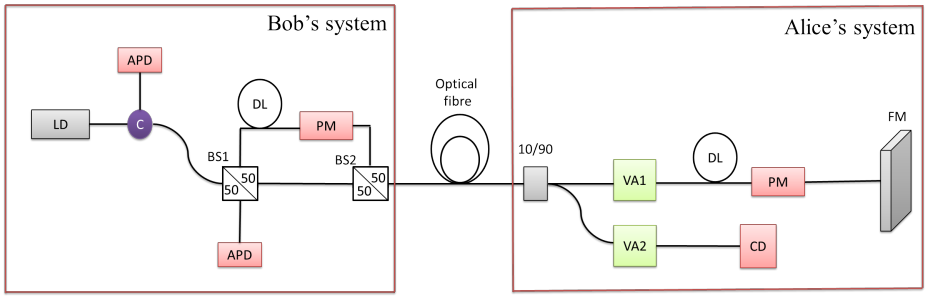


Figure 4.5: The internal schematic diagram of the id 3000 system. The active components are shown: Laser Diode (LD), a Avalanche Photo-counting Diodes (APD's), Delay Line (DL), Phase Modulator (PM), Variable Attenuator (VA), Classical Detector (CD) and Farraday Mirror (FM) [56].

The following section offers a detailed overview of the internal structure of the system focusing on the optical scheme. The optics operates with the electronics interface in performing the key distribution process. Figure 4.5 shows the arrangement and connection of Bob's system to Alice's system, connected through an optical fibre channel [56]. Each component of the system is listed below starting from Bob's system moving towards Alice's system.

4.4.1 Laser Diode (LD)

This laser diode (LD) is monochromatic in the sense that the light produced has a single wavelength and is in phase [39]. The LD utilised in the id 3000 Laser generates light pulses in the range of 300 - 2500 ps. The schematic of

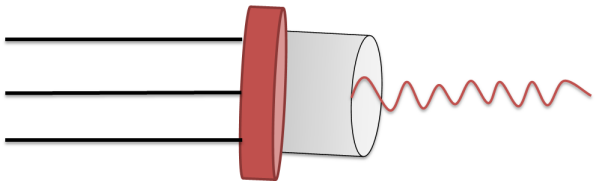


Figure 4.6: The schematic diagram of an LD utilised in the id 3000 system

an LD is provided in Figure 4.6.

4.4.2 Circulator (C)

A circulator is a passive three or four port device in which light enters any port, gets rotated and then transmitted. Normally, a three port device is formed from a Y-junction in which the circulation flows as illustrated in Figure 4.7, in a clockwise direction to perfectly guide light pulses [40]. In the id 3000 system, this circulator is utilised to randomly direct the light pulses through port 3 going towards the beam splitter.

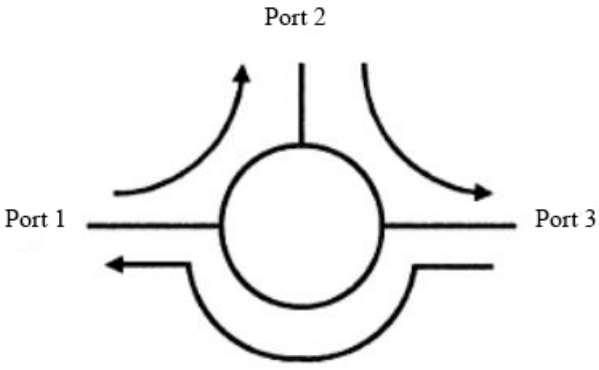


Figure 4.7: The schematic of a circulator used in the id 3000 system [59].

4.4.3 Avalanche Photo-Diode (APD)

Avalanche Photo-diode detectors (APD) detects information which has been sent and produces signals. In the id 3000 system an APD detects returning pulses and count the transmitted single photons including the noise. The generation of fake signals is possible when APD's are operated, in which an APD generate a signal without Alice sending some pulses. The image of APD is presented in section 3.1.3.

4.4.4 Beam Splitter (BS)

A Beam Splitter (BS) is an optical device used to split a laser beam into two equal paths, transmission and reflection [60]. Figure 4.8 provides a diagram of a beam splitter.

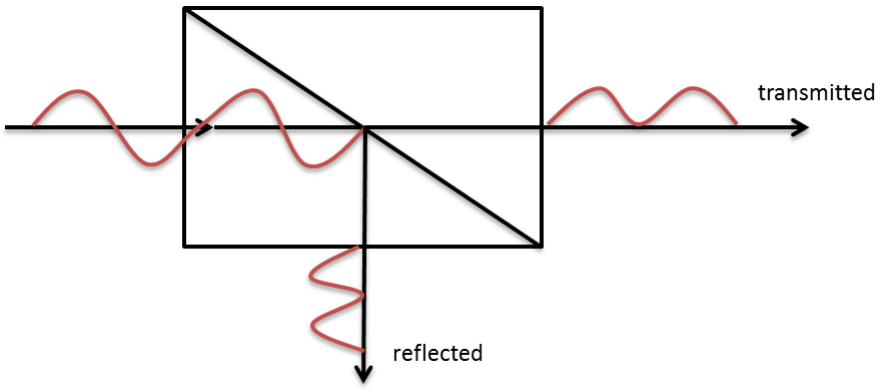
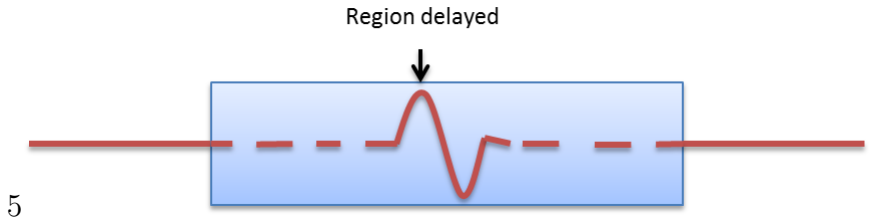


Figure 4.8: The schematic of a BS shows the 50 % of the light transmitted and 50 % of the light reflected [35].

4.4.5 Delay Line (DL)

A Delay Line (DL) is a device designed to enable a signal to be delayed by a number of samples in order for an id 3000 system to obtain perfect transmission. A DL comprises of an input and output to collect light into a fibre. Figure 4.9 illustrate how the pulses can be delayed. These delay lines are operated electronically.



5

Figure 4.9: The structure of a delay line demonstrating how pulses can be delayed in the id 3000 system [61].

4.4.6 Phase Modulator (PM)

Phase modulation (PM) in the id 3000 system maintains the amplitude of the single photon pulses and encodes bit values on the pulses. It is created to perform a phase of every photon emitted to carry the information. The illustration of this PM is provided in section 3.1.2

4.4.7 Coupler 10:90 (10/90)

The coupler 10 : 90 is the fibre coupler which splits the light pulses into 10 % and 90 % intensity. Figure 4.10 provides the image of the coupler utilised in the id 3000 system.

Figure 4.10: The schematic diagram of a fibre coupler 10:90 in the id 3000 system [62].

4.4.8 Classical Detector (CD)

Classical Detector (CD) is used to check for security as it prevents an eavesdropper from injecting light into the system. Since Eve can time-shift single pulses that arrives at the phase modulator earlier or later by applying phase-remapping attack. The classical detector monitors the incoming energy pulses in a sense that when Eve try to send the signal larger than the threshold an alarm can trigger. For the id 3000 system, a CD operate at a bias voltage of about 0 - 60 V. [63].

4.4.9 Variable Attenuator (VA)

A Variable Optical Attenuator (VA) is a device that lowers the intensity of the light signal in an optical fibre. Figure 4.11 shows the schematic of

a VA. VA is used mostly in fibre based communications to literally reduce power level by calibrating the amount of signal loss or supplied such that the transmitter and a receiver level is matched [64]. The id 3000 system provides the variable attenuators (VA1 and VA2) to attenuate light pulses to single photons, operating at a range of 1.5 - 20 dB.

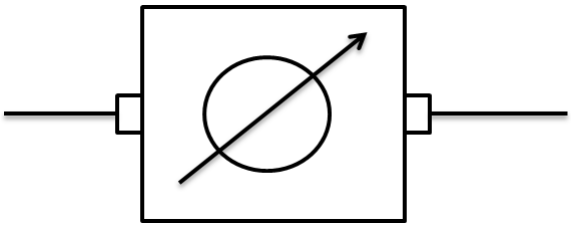


Figure 4.11: The schematic of a variable attenuator used in the id 3000 system [65].

4.4.10 Faraday Mirror (FM)

A Faraday Mirror (FM) is designed to reflect the light pulses. It is used in the id 3000 system to ensure that the polarisation of light is maintained [59]. Figure 4.12 gives the schematic of a Faraday mirror.

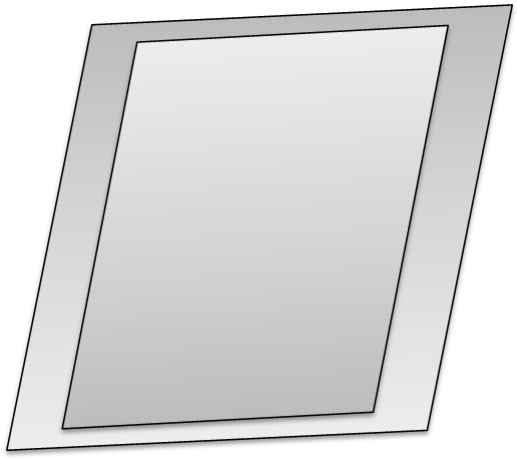


Figure 4.12: An image of a passive mirror [59].

4.5 Transmission in the id 3000 system

Bob sends strong pulses of light which pass through a circulator. In the circulator, it then randomly chooses the port that goes through the first beam splitter (BS1) and splits to 50/50 of transmission and reflection. Half transmitted (50 %) light pulses travel through the short arm and the half reflected (50 %) takes through the long arm. The short arm travels straight while the long arm passes through the delay line, it then passes through the delay line where pulses are delayed for some seconds to prevent noise. The propagation continues to the PM which is inactive during the first pass. The light pulses from the short and long arm thereafter recombine at BS2 and travel as one pulse. This process is illustrated in Figure 4.5.

The light pulses travel via a channel fibre and reach Alice where the light pulses separate at 10/90 fibre coupler. The intense (90 %) light pulses go through the path toward VA1 and the weak (10 %) light pulses go through the path towards VA2. The pulses get attenuated by VA1 and VA2 to single photons in both paths. Single photons in the path VA1 are delayed for some time in the delay line to prevent noise. The single photons in the path VA2 travel through a classical detector (CD), which monitors for the eavesdropping..

Two paths combine and pulses are reflected by the FM which is at the end

point of Alice's system. FM ensures that propagation and the polarisation of light pulses in the fibre are maintained such that the light pulses are reflected back to Bob. The propagation is reversible. The returning single photons pass through the PM within Alice's device, it is modulated and travels to Bob to be detected by APD1 and APD2 to provide the raw key.

The effectiveness of the system during transmission is determined by the bits measured by Bob known as the Raw Key length and the error rate called Quantum Bit Error Rate. The Raw Key refers to the bits measured by Bob from single photon pulses sent by Alice and is denoted as,

$$R_{\text{raw}} = qf\mu t_{\text{ab}} t_b \eta, \tag{4.1}$$

• $q \longrightarrow$ is a factor that relies on the protocol implemented for example, in the BB84 where most of the time 50 % of Alice and Bob's bases do not match. This factor is represented as $\frac{1}{2}$ for the BB84 protocol.

• $f \longrightarrow$ corresponds to a frequency of a signal pulse.

• $\mu \longrightarrow$ refers to the mean value of single photons in each pulse.

• $t_{\text{ab}} \longrightarrow$ corresponds to transmission line from Alice to Bob.

• $t_{\text{b}} \longrightarrow$ refers to Bob's transmission which normally around 0.6.

• $\eta \longrightarrow$ refers to detection efficiency.

The Quantum Bit Error Rate (QBER) refers to the errors obtained dur-

ing the transmission. The QBER is an essential parameter in QKD systems as it is applied to determine the security during the transmission and can be expressed as a percentage. This parameter is defined as the ratio of the wrong bits and the total bits after the sifting process as shown by an equation (4.2).

$$\text{QBER} = \frac{W_{\text{wrong}}}{W_{\text{wrong}} + W_{\text{right}}} = \frac{R_{\text{error}}}{R_{\text{sifted}}}, \tag{4.2}$$

where W_{wrong} corresponds to the errors obtained after the sifted key and is denoted as R_{error}. The $W_{\text{wrong}} + W_{\text{right}}$ corresponds to the bits in the sifted key is given as R_{sifted}. The QBER percentage varies according to the protocol implemented during the transmission. The threshold QBER for the BB84 and SARG04 protocols is 11 % and 10.49 % respectively. When is it obtained at a greater percentage than these, the id 3000 system produces a Raw Key that will be discarded.

Chapter 5

Experimental preparation for the id 3000 system

5.1 Method of controlling the system

The operation of the id 3000 system is based on the integration of hardware. Its operating system is designed to work only with Microsoft Windows. The program comprises of two applications packages namely, cryptomenu application and Clavis application. These applications are prototyped to be implemented through commands line of a C++ program.

5.1.1 Cryptomenu application

The cryptomenu application is available for both Alice and Bob after the installation. Alice and Bob access cryptomenu via their respective computers

which can be performed in parallel. The role of this particular property is to allow the setting of the hardware parameters. For an optimal setting it is advisable to access the initialisation file that is placed in the windows in the file named cryptoini. The file enables the settings of all parameters. Once the parameters are set, they can then be saved and viewed on the console screen. The commands used to activate the parameters are given in the Table 5.1. The parameters initiated for Alice and Bob are displayed in Table 5.2 and 5.3.

Table 5.1: Commands used to activate the hardware parameters

Command	Description of the command
X	Open Log [cryptolog.txt]
Y	Open Ini [cryptoini.ini]
Z	Save Ini [crptoini.ini]

Table 5.2: Quantum Key Distribution parameters-Alice

Menu Setup	Menu Setup
(A) Attenuator 1 [11 dB]	(U) Attenuator 2 [0dB]
(B) Detector Bias [76]	(T) Detector threshold 1 [5]
(D) Detector threshold [5]	(E) PM State 1 [28.6%] Z
(S) PM State 0 [0%]	(M) PM State 3 [88.2%]
(P) PM State 2 [57.3%]	(R) PM Coarse delay [1201]
(O) Number of Frames [1680]	(F) Phase adjustment
(N) Number of pulses [624]	

Table 5.3: Quantum Key Distribution Parameters-Bob

Menu Setup	Menu Setup
APD Bias 1 [33.35 V]	APD Bias 2 [32.9 V]
(N) Number of laser pulses [624]	(D) Number of detection pulses [624]
(D) Laser pulse width [500 ps]	(M) PM Pulse width [2]
(S) PM State 1 [47.3%]	(C) Coarse Delay [0]
(P) Waiting Duration 1 [7466]	(E) Fine Delay 2 [0]
(O) Number of Frames [1680]	(I) Waiting duration 2 [1990]
A/B Phase modulator adjustment	(T) Dead time [10 us]

The APD can be set to the value presented in Table 5.3. A value below this measurement can give an error when performing QKD. Some of the parameters take the same measurement in both Alice and Bob. This includes a number of pulses and number of detection events. It is important that both stations apply the same measurement for this purpose to achieve an optimal key exchange. The laser pulse width can be set to a value of 500 ps. When

it is set below this value, there is a high probability to obtain more errors and noise during key exchange.

The detectors are operated to time delay settings namely a coarse delay and a fine delay. The waiting period creates a delay between two or more pulses. Period 2 is set to provide a temporary stop, constituting the end of a frame and the start of the coming frame. The dead time is set to create a delay between two runs of the experiment.
The phase modulator accesses interference of a single photon pulse when Bob releases a train of pulses which Alice attenuates to single photons and perform phase modulation on the individual single photon pulse. The counts will then be recorded through the cryptomenu program at Bob's system.

5.1.2 Clavis application

The main function of this property is to perform the entire process of quantum key distribution. The application is designed to run on both computers. The program running at Bob's system acts as the master while Alice's system is a slave. Bob sends only the required information to Alice. This transfer is managed via an Internet Protocol (IP). The IP address is accessed through Bob's computer. This connection will allow a transfer of data files to be transferred from Bob to Alice. There exist two procedures which are assigned to run simultaneously. One monitors and memorizes all the supplied information (key buffer), the other one performs encryption files. The tasks

which are monitored in the memory include:

• The hardware check-up to check if the subsystems operating in the system are functioning correctly. The subsystems that are monitored are the temperature by checking the power that is supplied by Bob and Alice. The hardware check includes verifying the amount of the emitted power for the laser in Bob's station and confirming the noise probability in the APD's of Bob's system.

• The key buffer plays a role in the measurement of the optical link (line length). The system synchronises the emitted pulses with their detection. Bob then scans the delay during that emission and detection such that it maximises the signal detection. The procedure runs repeatedly, for example, seven to ten scans.

• When the system has achieved the above task it then performs a Raw Key production which is done by exchanging single photon pulses. The statistical tests during the exchange are provided with the detection probability.

• The last task which takes place in the key buffer is the key distillation. Key distillation is important for QKD. The key buffer distillates the Raw Key bits which are stored in the computer's memory to produce the cryptographic key.

5.2 Demonstration of the BB84 and SARG04

As a demonstration of QKD using the id 3000 system, students have a choice of either implementing BB84 or SARG04 protocol in the id 3000 system. Here we show a demonstration of both protocols. It should be noted that the demonstration of these protocols is performed separately in the id 3000 system. It cannot be performed simultaneously. The id 3000 system provides six steps for the accomplishment of QKD. These steps are applicable for both protocols which can be demonstrated in the id 3000 system. Such steps include checking the status, checking the noise, measuring the line length, generating the files and obtaining the raw key.

5.2.1 Checking the status

Checking status is a mode in which the id 3000 system allows the user to validate the temperature of the devices. This step was done in both the systems of Alice and Bob. During the performance of QKD, the system's temperature and the voltage were displayed as shown in Tables 5.4 and 5.5. This performance was obtained through the cryptomenu program of Alice's and Bob's system via their correspondence computers. The results of this step were performed using the first command on both computers. The first command in the system reads as (status) in both systems.

Table 5.4: Temperature at Alice

Read Temperature	BB84	SARG04
TTL Power Supply [5V]	4.97 V	4.96 V
ECL Power Supply [-5V]	- 4.9 V	-4.8 V
Fans Power Supply [12V]	11.92 V	11.92 V
TEC Current [0 - 3.5A]	-1.87 A	-1.98 V
Device Temperature	25^0C	20.3^0c

Table 5.5: Temperature at Bob

Read Temperature (k)	BB84	SARG04
TTL Power Supply [5V]	4.99 V	4.98 V
ECL Power Supply [-5V]	- 4.46 V	-4.51 V
Fans Power Supply [12V]	11.92 V	11.94 V
TEC Current [0 - 3.5A]	1.5 A	1.49 V
Device Temperature	25.9 ^{0}C	26^0C
Cooler Temperature	21.5 ^{0}C	20.7^0C
Error Temperature	-0.1 %	-0.15%

5.2.2 Measuring the noise

The id 3000 system measures the noise in the system by measuring the dark counts. Dark count is a term used for noise probability. This performance was implemented using Bob's computer through the cryptomenu program. When performing this step, a second command was selected in the cryptomenu application and is indicated as (noise measurement). After selecting this command, the program will require a declaration of a dead time to be set by the user for the second time in order for the system to provide the results of this step. Shown in Tables 5.6 and 5.7, are the experimental results obtained by Bob's station while the cryptomenu program was running.

Table 5.6: This table present the noise detected during the implementation of the BB84 in the id 3000 system

BB84	Detector 1	Detector 2
Number of detection	290	115
Statistical error	5.66 %	8.11%
Noise Probability	$2.9\times\ 10^{-4}$	$1{,}5\times10^{-4}$
Total number of gates on both detectors (976927)		

As observed from Tables 5.6 and 5.7, the actual noise measurement was considered as a noise probability. The statistical error percentage observed in both protocols indicates high noise in the id 3000 system. The noise is equivalent to losses which are likely to reduce the raw key.

Table 5.7: This table present the noise detected during the implementation of the SARG04 in the id 3000 system

SARG04	Detector 1	Detector 2
Number of detection	308	134
Statistical error	5.77 %	8.64%
Noise Probability	$3.1\times\ 10^{-4}$	1.3×10^{-4}
Total number of gates on both detectors (978326)		

5.2.3 Checking the line length

Line length, also called optical link, is when the user can approximately measure the length for the key exchange. This step is performed by Bob only via his computer through the cryptomenu program. The principle behind this step is that: a number of pulses are emitted from Bob's system to Alice's system and get reflected back to Bob to be measured. It is a transmission that opens a number a detection in Bob. The phase modulator at Bob's system was set in order to guide the single photons along the two APD's equally. The detection occurs via three line passes. Using the command 3 named (line length measurement), Bob's station scans and locates only the maximum detection. Tables 5.8 and 5.9 below provides the results obtained when running this step in the id 3000 system. From the length of 12 km that was set Bob's system performed gated detection and maximum detection was located as an optical link and was observed as 11.394 km and 11.794 km for BB84 and SARG respectively.

Table 5.8: Line Length detection for 12 km performed through the id 3000 system focusing on the BB84 protocol

Passes	Detector 1	Detector 2
Line pass 1	6.2 %	5.4 %
Line pass 2	0.1 %	0.1 %
Line pass 3	0.1 %	0.8 %

Table 5.9: Line Length detection for 12 km performed through the id 3000 system based in the SARG04 protocol

Passes	Detector 1	Detector 2
Line pass 1	4.5 %	5.6 %
Line pass 2	0.1 %	0 %
Line pass 3	0.1 %	0.8 %

For this performance, the id 3000 system is designed to produce a detection not above 10% for optimal results. A very low detection percentage, in this case, is considered as good results.

5.2.4 Generating files for key exchange

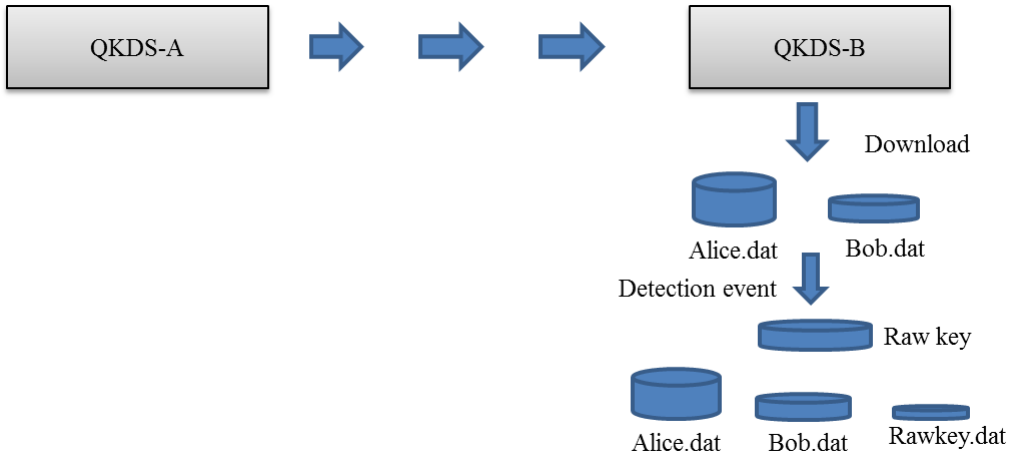


Figure 5.1: The schematic diagram demonstrating the process of the key exchange within Alice and Bob's system. The QKDS-A is referred to Alice's system and QKDS-B referred to Bob's system.

Generating files is when Alice starts the key exchange process. This step was performed after the line length was measured. Alice's system via her

computer using cryptomenu program prepared 14 Mbits by applying the second command in the cryptomenu program. The command is named (generate random file). The system then generated files such as a data providing pseudo random numbers. The Alice data file was sent to Bob as illustrated in Figure5.1. When Bob receives the file, he then starts the measurement. Bob first downloads Alice's data file and Bob's data file to perform a Raw Key exchange. A Raw Key file will then be produced. In the end, Bob has three files of data as seen in Figure 5.1. They are indicated as Alice.data, Bob.data and Raw data. This step demonstrates how the transmission was performed between the two users.

5.2.5 Obtaining the actual Raw Key

This step provides the Raw Key obtained by Bob. Hence, it is the last stage for our demonstration of QKD. This step was performed by Bob through cryptomenu. Here, the system provides the actual measurement during the key exchange. The data obtained for this step was obtained using the sixth command provided as (sifting) in the cryptomenu Bob's computer. Results are presented in Tables 5.10 and 5.11. From Tables 5.10 and 5.11, the id 3000 system presented a total amount of the sent bit as 14629440 and 14358280 respective for BB84 and SARG04.

Table 5.10: Dataset containing the bits sent and Raw key when BB84 was implemented it was observed as:

Measured Values	Counts
Bits prepared	14629440
Detection gates	338280
Detections 1	10188
Detections 2	21630
Raw Key	17310
QBER	3.017 %

Table 5.11: Dataset containing the bits sent and Raw key observed during SARG04 implementation

Measured Values	Counts
Bits prepared	14629440
Detection gates	358280
Detections 1	12188
Detections 2	27630
Raw Key	20120
QBER	2.332 %

From the bits Alice had prepared and sent, a total number of 338280 for BB84 and 358280 for SARG04 bits were detected. From the detection gates performed by Bob during BB84 implementation, detector 1 and 2 manage to detect 10188 and 21630 respectively. In the SARG04 a number of 12188 and 27630 detections were observed respectively in the detector 1 and 2. Finally, the Raw Key in the BB84 and SARG04 protocol were produced to be 17310 bit/s and 20120 bit/s respectively. A 3.017 % error rate known as a QBER was obtained from the system when BB84 was implemented. When SARG04 was realised 2.332 % error rate was observed.

5.2.6 Comparison of BB84 and SARG04

From the demonstration of BB84 and SARG04 in the id 3000 system, the main parameters we checked are the Raw Key and QBER. Comparing the outcomes of these two parameters (Table 5.10 and 5.11) during the implementation of the aforementioned protocols, the SARG04 performed better than the BB84 protocol.

When comparing the results acquired during the implementation of the BB84 and SARG04 protocols. We obtained a raw key of 17310 bit/s from 14629440 bit/s sent when BB84 was demonstrated and 20120 bit/s was obtained from 14629440 bit/s prepared during the implementation of SARG04. From this data the QBER is measured. The threshold QBER for the BB84 and SARG04 protocols is 11 % and 10.49 % respectively. This is the maximum limit of the QBER that infers whether a transmitted key is discarded or kept for further post-processing. We obtained 3.017 % during the implementation of BB84 and 2.332 % for the SARG04 protocol. This was achieved even though there was a high presence of noise in the id 3000 system. The SARG04 protocol has the advantage to provide efficient results in presence of noise. This was observed during the implementation, as indicated in Table 5.11, where a lower QBER was achieved and higher raw key rate in comparison to BB84.

Chapter 6

Summary and Conclusion

We have successfully demonstrated how to introduce QKD into the undergraduate physics curriculum. We have outlined steps which make it more convenient for undergraduate students to understand the relevant processes. We have further performed a typical experiment using the QKD system id 3000. The system we utilised will be available in the physics 3^{rd} year laboratory at the University of KwaZulu-Natal and can be exploited by the students as a learning tool. The experiment can be performed in a typical three hours lab session. This will improve their understanding regarding this application.

QKD technology has a real world implementation and numerous groups have implemented QKD. For example, the University of KwaZulu Natal performed the practical real world QKD over distances 13.08 km at Cato Manor in Durban between Central Application Office and Ethekwini Municipality original

Offices buildings in 2008 [66]. The id 3000 system was employed for this realisation. This was further implemented for the Quantum Stadium Project during the 2010 Fifa World Cup with an upgraded version of the id 3000 system [67].

The real world implementation of this technology encourages students to explore quantum mechanics in more depth. Our demonstration for undergraduate students was carried out in the lab environment. Using the id 3000 system with a 12 km fibre inside the system a secure key was exchanged between Alice and Bob over a distance of 12 km. We demonstrated QKD focusing on the BB84 and SARG04 protocol. The system is designed to be implemented through fibre optic with a 1550 nm wavelength which then acts as a link (quantum channel).

The id 3000 system was set up to perform the key distribution process which was controlled via a computer for Alice and Bob. The setting of the hardware parameters was done using the cryptomenu application. The Clavis application accessed the transfer of data files between the two users, where the transfer was accessed through Internet Protocol.

QKD was demonstrated by following the steps offered in crypomenu application. The first step was employed for the validation of the temperature of the system and the system measured at 47.7 ^{0}C. The second step was per-

formed to measure noise in the system, the detectors detected dark counts which read as noise probability of 2.9×10^{-4} in detector 1 and 1.5×10^{-4} in detector 2 for the BB84. When SARG04 was implemented dark counts (noise probability) for D1 was 3.1×10^{-4} and 1.3×10^{-4} in D2. The third step was employed for the demonstration of the line length in which the users can exchange the key. A length of 12 km was set and measured, where Bob's system performed gated detection and maximum detection was located as an optical link and was observed as 11.394 km and 11.794 km for BB84 and SARG protocol respectively.

The fourth step was demonstrated after the length had been measured and was performed by Alice's system. Alice sent 14 Mbits to Bob to be measured. Bob received a file containing pseudo random numbers. The last step resulted in the generation of the Raw Key and QBER. From the demonstration of the BB84 and SARG04 protocol, a Raw Key rate of 17310 bits/s and 20120 bits/s respectively were measured by Bob. A QBER of 3.017 % from BB84 and 2.332 % in the SARG04 was obtained with the id 3000 system.

The demonstration of QKD in both protocols was successful in the id 3000 system. All the information presented in chapter 5 including the results provided in the Tables are the proof that QKD was successfully implemented using id 3000 system and the system was efficient.

Bibliography

[1] Paul AM Dirac. On the theory of quantum mechanics. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 112, pages 661–677. The Royal Society, 1926.

[2] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[3] Max Tegmark and John Archibald Wheeler. 100 years of the quantum. *arXiv preprint quant-ph/0101077*, 2001.

[4] Niels Bohr et al. *The quantum postulate and the recent development of atomic theory*, volume 3. Printed in Great Britain by R. & R. Clarke, Limited, 1928.

[5] David J Griffiths and Edward G Harris. Introduction to quantum mechanics. *American Journal of Physics*, 63(8):767–768, 1995.

[6] Michael I Mishchenko. The fundamental concept of electromagnetic scattering by particles: a perspective. *Journal of Quantitative Spectroscopy and Radiative Transfer*, 110(14):1210–1222, 2009.

[7] Max Planck. Ueber das gesetz der energieverteilung im normalspectrum. *Annalen der Physik*, 309(3):553–563, 1901.

[8] Victor Guillemin. *The story of quantum mechanics*. Courier Corporation, 2003.

[9] Rusty L Myers. *The basics of physics*. Greenwood Publishing Group, 2006.

[10] Peter E Gordon. Duality of flactuations, fields. *Wave-Particle Duality*, page 69, 2012.

[11] Ervin B Podgoršak. Compendium to radiation physics for medical physicists. 2014.

[12] David Halliday, Jearl Walker, and Robert Resnick. *Fundamentals of Physics, Chapters 33-37*. John Wiley & Sons, 2010.

[13] Werner Heisenberg. *The physical principles of the quantum theory*. Courier Corporation, 1949.

[14] Richard W Sears. Clues from other scientific disciplines. In *The Sense of Self*, pages 89–131. Springer, 2016.

[15] Nouredine Zettili. Quantum mechanics: concepts and applications. American Association of Physics Teachers, 2003.

[16] Michele Barone and Franco Selleri. *Frontiers of fundamental physics*. Springer Science & Business Media, 2012.

[17] Erwin Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23(48):807–812, 1935.

[18] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information. American Association of Physics Teachers, 2002.

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

[20] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing 5. 1984.

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

[22] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000.

[23] Antoine Muller, Hugo Zbinden, and Nicolas Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. *EPL (Europhysics Letters)*, 33(5):335, 1996.

[24] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[25] Werner Heisenberg et al. *Physics and Philosophy*. Prometheus Books, 1999.

[26] Mark Beck. *Quantum Mechanics: Theory and Experiment*. Oxford University Press, 2012.

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

[28] ID Quantique SA. Understanding quantum cryptography, apr. 2005, 12 pages.

[29] Eduard Prugovecki. *Quantum mechanics in Hilbert space*, volume 92. Academic Press, 1982.

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

[31] Hugh D Young, Roger A Freedman, and Ragbir Bhathal. *University Physics: Australian edition*. Pearson Higher Education AU, 2010.

[32] Ronald I Frank. Undergraduate course module on quantum key distribution. In *Proc. Information System Education Conference (ISECON)*, page 10, 2004.

[33] JG Rarity, PR Tapster, and E et al Jakeman. Two-photon interference in a mach-zehnder interferometer. *Physical Review Letters*, 65(11):1348, 1990.

[34] Ping Lu, Liqiu Men, Kevin Sooley, and Qiying Chen. Tapered fibre mach-zehnder interferometer for simultaneous measurement of refractive index and temperature. *Applied Physics Letters*, 94(13):131110, 2009.

[35] MJ Holland and K Burnett. Interferometric detection of optical phase shifts at the heisenberg limit. *Physical Review Letters*, 71(9):1355, 1993.

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

[37] Masanao Ozawa. Universally valid reformulation of the heisenberg uncertainty principle on noise and disturbance in measurement. *Physical Review A*, 67(4):042105, 2003.

[38] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[39] Yukio Narukawa, Yoichi Kawakami, Mitsuru Funato, Shizuo Fujita, Shigeo Fujita, and Shuji Nakamura. Role of self-formed ingan quantum dots

for exciton localization in the purple laser diode emitting at 420 nm. *Applied Physics Letters*, 70(8):981–983, 1997.

[40] Guohua Qi, Jianping Yao, Joe Seregelyi, Stéphane Paquet, and Claude Bélisle. Optical generation and distribution of continuously tunable millimeter-wave signals using an optical phase modulator. *Journal of Lightwave technology*, 23(9):2687, 2005.

[41] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47(4):595–598, 2000.

[42] Sergio Cova, M Ghioni, A Lacaita, C Samori, and F Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Applied Optics*, 35(12):1956–1976, 1996.

[43] Howard Barnum, Michael A Nielsen, and Benjamin Schumacher. Information transmission through a noisy quantum channel. *Physical Review A*, 57(6):4153, 1998.

[44] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, page 136. IEEE, 2004.

[45] 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, 1993.

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

[47] J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. In *Proceedings of the ninth annual ACM symposium on Theory of computing*, pages 106–112. ACM, 1977.

[48] Vadim Makarov. *Quantum cryptography and quantum cryptanalysis*. PhD thesis, Fakultet for informasjonsteknologi, matematikk og elektroteknikk, 2007.

[49] 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.

[50] 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.

[51] WT Buttler, RJ Hughes, PG Kwiat, SK Lamoreaux, GG Luther, GL Morgan, JE Nordholt, CG Peterson, and CM Simmons. Practical free-space quantum key distribution over 1 km. *Physical Review Letters*, 81(15):3283, 1998.

[52] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, 2010.

[53] Richard J Hughes, Jane E Nordholt, Derek Derkacs, and Charles G Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*, 4(1):43, 2002.

[54] 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.

[55] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026, 2010.

[56] Damien Stucki, Nicolas Gisin, Olivier Guinnard, Grégoire Ribordy, and Hugo Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, 4(1):41, 2002.

[57] Joseph C Palais. *Fiber optic communications*. Prentice Hall Englewood Cliffs, 1988.

[58] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5):378–381, 2013.

[59] Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Passive faraday-mirror attack in a practical two-way quantum-key-distribution system. *Physical Review A*, 83(6):062331, 2011.

[60] CK Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044, 1987.

[61] GJ Tearney, BE Bouma, and JG Fujimoto. High-speed phase-and group-delay scanning with a grating-based phase control delay line. *Optics Letters*, 22(23):1811–1813, 1997.

[62] Enrique AJ Marcatili. Dielectric rectangular waveguide and directional coupler for integrated optics. *Bell Labs Technical Journal*, 48(7):2071–2102, 1969.

[63] Ryan S Bennink, Sean J Bentley, and Robert W Boyd. two-photon coincidence imaging with a classical source. *Physical Review Letters*, 89(11):113601, 2002.

[64] B Barber, CR Giles, V Askyuk, R Ruel, L Stulz, and D Bishop. A fiber connectorized mems variable optical attenuator. *IEEE Photonics Technology Letters*, 10(9):1262–1264, 1998.

[65] T Kawai, M Koga, M Okuno, and T Kitoh. Plc type compact variable optical attenuator for photonic transport network. *Electronics Letters*, 34(3):264–265, 1998.

[66] Mpinda Kabeya. *Experimental Realization of Quantum Key Distribution.* PhD thesis, Citeseer, 2009.

[67] Abdul Mirza and Francesco Petruccione. Recent findings from the quantum network in durban. In *AIP Conference Proceedings*, volume 1363, pages 35–38. AIP, 2011.