THE IMPLEMENTATION OF POLARISATION ENCODED QUANTUM KEY DISTRIBUTION IN FIBRE

by

SHARMINI PILLAY

Submitted in fulfilment of the academic requirements for the MSc degree at the School of Chemistry and Physics, Westville Campus, University of KwaZulu-Natal.

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

Name _____

Signed _____

Date _____

ABSTRACT

Quantum Key Distribution (QKD) employs the laws of quantum mechanics for the purpose of cryptography. Two parties, commonly called Alice and Bob, are able to share a random key which is used to encrypt a message. Any eavesdropper trying to intercept their key will have to make measurements, thereby disturbing the system. This can be detected by Alice and Bob and they will then discard their key.

Polarisation encoded QKD protocols use the polarisation of single photons as qubits to generate a cryptographic key. This can be implemented using a fibre optic link between Alice and Bob but the polarisation of light is altered when passed through a fibre due to birefringence caused by asymmetries in the fibre. This causes refractive differences for orthogonal components of the state of polarisation of light, so the polarisation is rotated as the photon is transmitted through the fibre. If the fibre is fixed, the change of polarisation will be unique and constant. This can be compensated by rotating each photon appropriately to its original state. Under typical environmental conditions, such as temperature changes and vibrations, the birefringence effects vary and should be compensated in real time. Therefore, an active polarisation controller is needed in order to maintain the state of polarisation of each qubit.

An investigation was done to first track how the state of polarisation changes over time in a natural environment. Both wavelength-division multiplexing and time-division multiplexing were investigated as testing methods for the compensation system. A time-division multiplexed system was developed to compensate the changes in polarisation. Since QKD protocols such as BB84 and B92 utilise two non-orthogonal bases, two polarisation controllers are usually used for compensation. However, by using a search algorithm, one polarisation controller was able to isolate the plane on the Poincaré sphere that passes through both bases, thus compensating non-orthogonal states with one device.

PREFACE

The experimental work described in this dissertation was carried out at the School of Chemistry and Physics, University of KwaZulu-Natal, Westville Campus, from the period commencing February 2011 to December 2012, under the supervision of Professor Francesco Petruccione.

These studies represent original work by the author and have not otherwise been submitted in any form for any degree or diploma to any tertiary institution. Where use has been made of the work of others it is duly acknowledged in the text.

DECLARATION 1

I Sharmini Pillay declare that

1. The research reported in this dissertation, except where otherwise indicated, is my original research.

2. This dissertation has not been submitted for any degree or examination at any other university.

3. This dissertation does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

4. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:
   a. Their words have been re-written but the general information attributed to them has been referenced
   b. Where their exact words have been used, then their writing has been placed in italics and inside quotation marks, and referenced.

5. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

Signed: ……

DECLARATION 2

DETAILS OF CONTRIBUTION TO PUBLICATIONS that form part and/or include research presented in this dissertation

Publication 1 – Published:
Sharmini Pillay, Abdul Mirza, and Francesco Petruccione. Polarisation encoded quantum key distribution in fibre. Proceedings of SAIP2011, the 56th Annual Conference of the South African Institute of Physics, 2011. University of South Africa, Pretoria, 2011, pp. 426-431
Sharmini Pillay was the principle researcher, conducted the experimental work and authored the paper.
Abdul Mirza supervised the research and co-authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 2 – In Press:
Sharmini Pillay, Abdul Mirza, Timothy B Gibbon and Francesco Petruccione. Compensating *Birefringence Effects in Optical Fibre for Polarisation Encoded QKD.* Proceedings of SAIP 2012
Sharmini Pillay was the principle researcher, conducted the experimental work and authored the paper.
Abdul Mirza supervised the research and co-authored the paper.

Timothy Gibbon supervised the research and co-authored the paper.
Francesco Petruccione supervised the research and edited the publication.

Publication 3 – Published:
Abdul Mirza and Sharmini Pillay, *Polarisation Encoded QKD in Fibre*. Hakin9 eBook, First Edition, Issue 3/2012, pp. 85-91.
Sharmini Pillay was the principle researcher, conducted the experimental work and authored the paper.
Abdul Mirza supervised the research and co-authored the paper.

Signed: ……

ACKNOWLEDGEMENTS

This work is based upon the research supported by the South African Research Chair Initiative of the Department of Science and Technology and the National Research Foundation.

I thank my supervisor, Prof. Francesco Petruccione, for his guidance, motivation and immense support throughout this project.

I thank Abdul R. Mirza for his tireless assistance and mentorship. I thank my colleagues, Reginald Abdul, Yaseera Ismail, Marco Mariola, Makhamisa Senekane and Michael Morrissey for their help and support.

I acknowledge the assistance of Dr. Tim Gibbon and I thank him for his advice and the use of the Fibre Optics Laboratory at The Nelson Mandela Metropolitan University.

I am eternally grateful to my parents, Dixen and Salo Pillay, for their unwavering support and love, and to my sister, Priyoshni, for being awesome. To my family and friends, I thank you for your encouragement and inspiration.

CONTENTS

1. Introduction

The reliance on information technology for global communication has highlighted the need for data security in recent years. Various applications such as online banking and government communications require a secure transmission between the transmitter and the intended recipient. Physical protection of the data is not feasible in terms of the cost and time implications. This type of protection also involves an element of human interaction which may compromise the security of the information. It is therefore essential to develop reliable and secure cryptographic systems (cryptosystems) to encrypt sensitive data. Cryptography allows for information to be encrypted into an unintelligible state so that it may be transmitted across public networks without any risk.

The necessity to keep information secret was realised centuries ago. The first recorded military cryptography, called the *scytale*, was designed by the Spartans in the 5th century B.C. [1]. The substitution cipher, developed by Julius Caesar, became a well known method of encryption and inspired the design of similar techniques, such as the Viganére cipher and the Beauford cipher [2]. Such substitution encryptions can be analysed and decrypted using statistical methods, as proposed by Al Kindi [3]. One of the most famous cryptosystems to date is the Enigma Machine, used by the German military during World War II.

Contemporary encryption methods have included the use of symmetric key and asymmetric key cryptography [4]. Using a symmetric key indicates that the same key is used for both the encryption and decryption processes. When using asymmetric cryptography, also called public key cryptography, the message is encrypted using a publicly known key, but can only be decrypted by a secret key, known only by the receiver. The main purpose of modern cryptography is to ensure [5]:

- **Privacy**
  This ensures that an eavesdropper cannot intercept and alter the message during transmission.
- **Authentication**
  This verifies that the message has been transmitted and received by the correct parties thus preventing an eavesdropper from implementing a *man in the middle* attack.
- **Non-repudiation**
  The identity of the transmitter is coupled with the data, which prevents the transmitter from falsely denying his participation.

The data is initially in the form of plaintext *P*. The transmitter, commonly known as Alice, encodes the plain text with a cryptographic key using an encryption algorithm, *E*. This forms the ciphertext, which may be accessed by any eavesdropper, commonly known as Eve. This ciphertext is then sent across a public channel to the authenticated receiver of the data, commonly referred to as Bob. Bob may decrypt the ciphertext using a decryption algorithm, *D*. This process can be mathematically represented as [6]

$$P = D(E(P)) \, . \tag{1.1}$$

Ciphertext is unintelligible to anyone not in possession of the cryptographic key hence, Alice may use an untrusted, public channel to transfer the ciphertext to Bob. In order for a message to be successfully delivered without being compromised, the security of the cryptographic key is essential. It is vital that only the two authenticated parties have access to the key, therefore, the distribution of the key is of prime importance in the cryptosystem.

Conventional methods of passing a key between two parties can include physically couriering the key or electronically transmitting the key via a classical connection, e.g. the RSA [7]. The only conventional cryptosystem that is theoretically secure is the One Time Pad (OTP). To implement the OTP, the plaintext and the cryptographic key are both represented as a string of bits. The plaintext and the key are combined by a bitwise XOR function. Three important characteristics of the OTP key are [8]:

- The key is required to be the same length as the plaintext.
- The key must be a truly random sequence so that the ciphertext will also be random.
- The key may only be used once.

The OTP has been proven as a secure cryptographic method, due to the above criteria [9].The only possible method to decrypt the OTP would be to attempt every possible permutation of the randomly generated key. This *brute force attack* is not feasible in polynomial time due to the length of the key, making the decryption process more costly than the value of the information [6]. Conventional cryptography therefore provides security that protects against the current technology of potential adversaries. However, with advancement in mathematics and computational technology, contemporary cryptography cannot be regarded as unconditionally secure [10].

2. Quantum Cryptography

The idea of quantum security was initially conceptualised by Stephen Wiesner in the 1970's. This provided a new, theoretically secure method to protect against the forgery of bank notes [11]. Quantum Key Distribution (QKD) was then proposed by Bennett and Brassard in 1984 as a further application to Wiesner's security protocol [12]. QKD relies on the laws of physics to ensure the security of the cryptographic key. This is safer than relying on the complexity of a mathematical algorithm or the security of a physical distribution process.

2.1. The Principle of Quantum Cryptography

The method of QKD encodes information into the physical properties of quantum particles. The laws of quantum physics therefore ensure the security of the key instead of the finite complexity of a mathematical algorithm. The information shared between Alice and Bob is carried by qubits (quantum bits) [13]. The qubit is a quantum two-level system. The state of the qubit, $|\Psi\rangle$, is represented as a linear superposition of two pure states,

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

The basis set, $\{|0\rangle, |1\rangle\}$, represent the two eigenstates that a qubit may be measured as. The probability of a measurement in these respective states is given by $|\alpha|^2$ and $|\beta|^2$, such that

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

Information may also be encoded in any other basis set, in particular,

$$|\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle). \tag{2.3}$$

It is noted that $|+\rangle$ and $|-\rangle$ are orthogonal to each other but the set $\{|+\rangle, |-\rangle\}$ is non-orthogonal to the set $\{|0\rangle, |1\rangle\}$. In terms of polarisation encoding, the basis states $|0\rangle$ and $|1\rangle$ can be represented by the vertical and horizontal States of Polarisation (SOP) and $|+\rangle$ and $|-\rangle$ can be represented by the right and left diagonal SOP's. Since the pairs of basis states are non-orthogonal to each other, any measurements carried out with the incorrect measurement basis will yield an ambiguous result [12]. The security of QKD therefore lies

in the inability to gain total information of the qubit that Alice has transmitted to Bob without first knowing which basis to use for the measurement.

Another advantage that QKD has over conventional cryptography is the ability for the authenticated parties to detect an eavesdropper. The eavesdropper, Eve, may attempt to copy or measure the quantum state of the qubits. However, both these attacks violate the laws of quantum mechanics that fortify QKD.

- **`No Cloning' Theorem** : There is no quantum mechanical device which outputs a perfect copy of an arbitrary pure quantum state while leaving the original unchanged [14]. This means that Eve cannot copy the qubits transmitted from Alice to Bob without creating a disturbance in the quantum properties of the qubit..
- **Heisenberg's Uncertainty Principle:** The measurement of one quantum observable of the qubit intrinsically creates an uncertainty in the conjugate properties of the qubit [15]. The Uncertainty Principle prevents Eve from implementing a *man-in-the-middle* attack, i.e., measuring the transmitted quantum state and passing the same information to Bob.

Any measurements done on the qubits during transmission will cause disturbances to the quantum states which can be observed by Alice and Bob. Therefore, if Alice and Bob observe an unusually high error rate in their transmission, they may infer the presence of Eve [16].

When characterising the security of an encryption method, it is necessary to assume that Eve possesses unlimited computational power. Since QKD exploits the physical quantum nature of particles, it is not vulnerable to technological advances but bound only by the laws of physics. Therefore, any developing technologies that result in increased computing power of Eve will not render QKD obsolete [17].

2.2. The Implementation of QKD

In order to put into practice the above mentioned principles of QKD, quantum cryptosystems require a specialised set of components. Alice must prepare the states of each qubit and transmit them over the quantum channel. For this, she requires a source and an encoder which must be linked to a random number generator. Bob must first decode these qubits in the appropriate basis and then measure the qubits with a device that is sensitive enough to detect quantum particles.

The most commonly used quantum particle is a single photon of light. The single photon can encode information using a number of different schemes. The types of encoding that are implemented in most systems are polarisation and phase. For a phase encoded system, a Mach-Zehnder interferometer is used to introduce phase differences between consecutive photons leaving Alice [18]. The phase is randomly adjusted to one of four predetermined

values. The phase differences correspond to the binary bit values shared between Alice and Bob. For polarisation encoding, the state of polarisation of each photon is equated to a binary bit value. This method will be discussed in chapter 2.2.1.

Entanglement-based QKD is a developing technology that provides a new approach to cryptography. Entanglement allows a pair of photons to be intrinsically correlated, even when separated in space [19]. The most direct method to create a pair of entangled photons is through the process of spontaneous parametric down conversion. The measurement of one photon will allow the observer to gain total information about the correlated photon. It is therefore possible to obtain information about an entangled particle without physically measuring it. The entangled photons are produced by Alice or an untrusted third party source. Alice and Bob each retain one of the entangled photons and share information through the existing correlation. In 1991, Ekert developed a protocol, Ekert91, using entangled photon pairs [20].

2.2.1 QKD Protocols

The protocols outlined in this section focus primarily on implementing QKD with polarisation encoding. The most appropriate protocols for this application are BB84, SARG04, B92 and LM05. These protocols will be discussed in the following section.

BB84 Protocol

A number of QKD protocols have been developed in order to transfer qubits from Alice to Bob. The first and most widely used QKD protocol was developed by Charles Bennett and Giles Brassard in 1984, hence it was called the BB84 protocol [12]. The protocol utilises two non-orthogonal basis states and will be described in terms of polarisation encoding. An example of the two polarisation bases states used for this protocol is the rectilinear (vertical-horizontal) basis, representing $|0\rangle$ and $|1\rangle$, and the diagonal basis, representing $|+\rangle$ and $|-\rangle$. Figure 2.1 shows an example of the bit encoding for each of these four states. Alice randomly chooses a state of polarisation for a single photon and transmits it to Bob. Bob randomly chooses to measure this photon in either the rectilinear basis or the diagonal basis. If Bob chooses the correct basis, he will measure the correct state of polarisation with 100% probability, as shown in Figure 2.2. If Bob chooses the wrong basis, there is a 50% probability that he could obtain either of the possible measurements. After the qubits have been distributed, Alice and Bob announce the basis that they chose for each photon and keep only the measurements for which they used the same basis. The other measurements are discarded. Alice and Bob should now have a string of identical bits, called the sifted key. Table 2.1 shows an example of how Alice and Bob may establish a sifted key using the BB84 protocol.

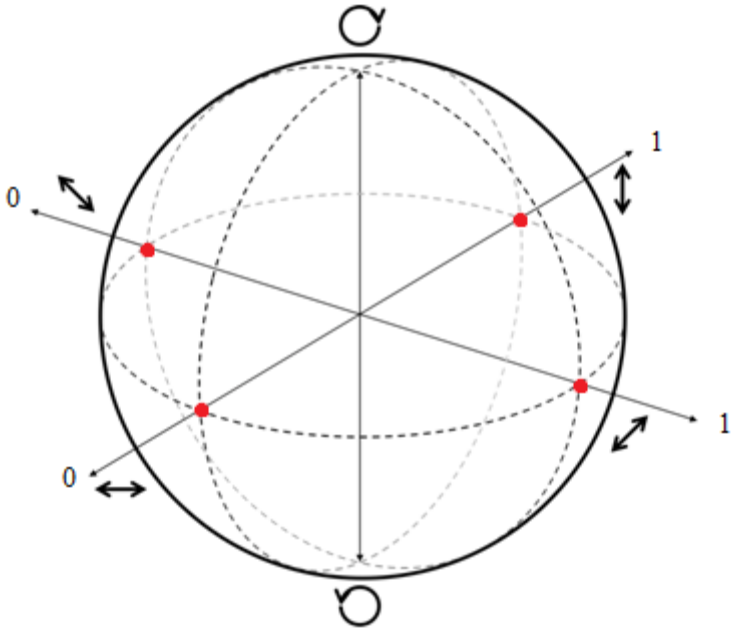


Figure 2.1: An example of the bit encoding used for the polarisation encoded BB84 protocol is shown in this figure. Each polarisation basis, shown on the Poincaré sphere, provides two qubits that may be used in the key distribution process. The rectilinear basis consists of the vertical and horizontal SOP's and the diagonal basis consists of the right diagonal and left diagonal SOP's. An alternative basis set that could be used to encode data consists of the right-circularly polarised and left-circularly polarised SOP's.

Table 2.1: An example of establishing a sifted key using the BB84 protocol.

Bit values randomly generated by Alice	0	0	1	0	1	1	0	1
Alice sends	↑	↖	→	↖	↗	↗	↖	→
Bob's basis	+	×	×	+	×	×	+	+
Bob measures	↑	↖	↗	↑	↗	↗	↑	→
Chosen bits	↑	↖			↗	↗		→
Bit values of the sifted key	0	0			1	1		1

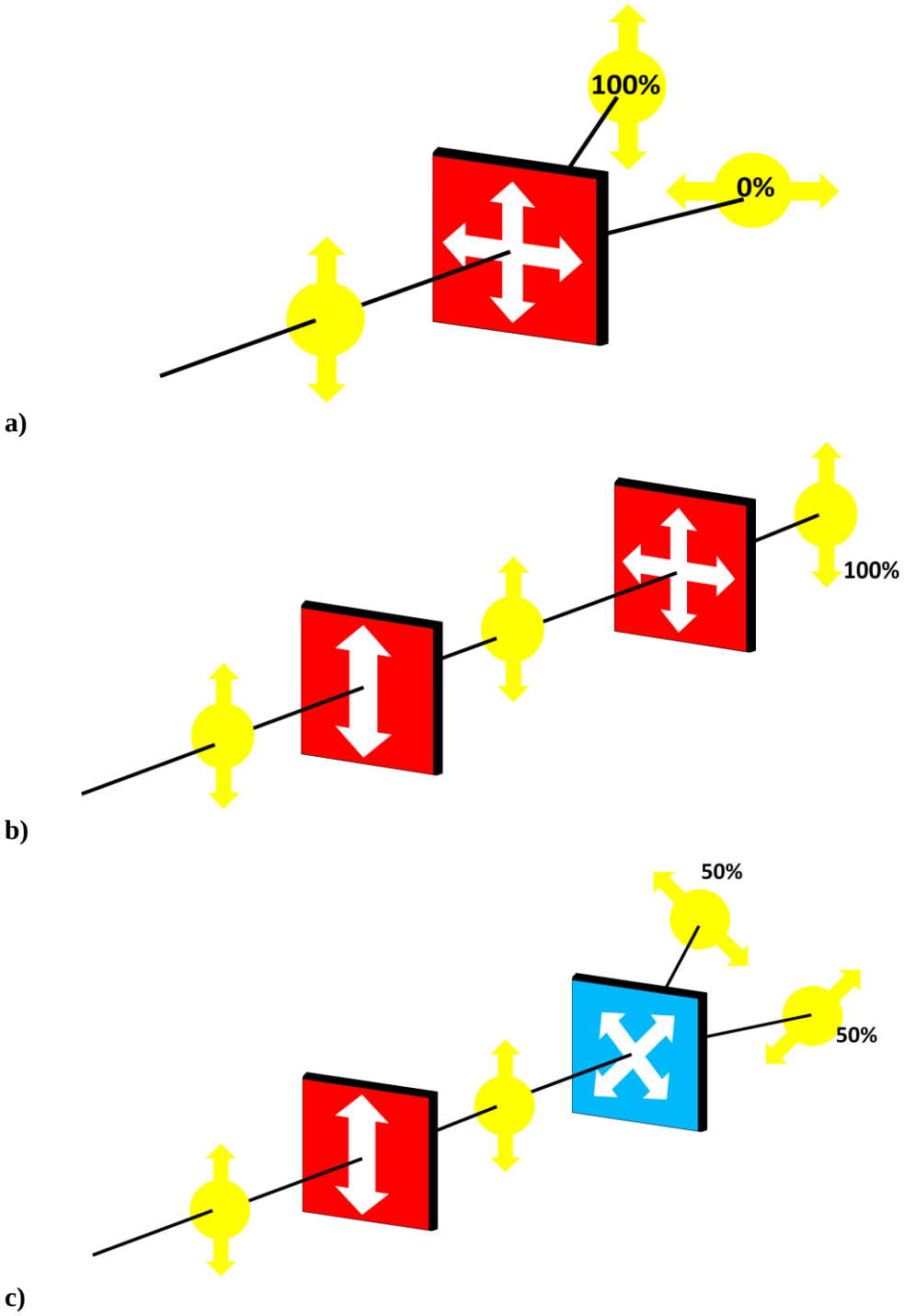


Figure 2.2: a) The possible outcomes of measuring a polarised photon using the correct basis. The outcomes are shown for a vertically polarised photon measured in b) the correct basis and c) the incorrect basis. As shown, a measurement in the correct basis will yield the correct bit value with 100% certainty. A measurement in the incorrect basis will allow the possibility of either bit value being measured, each with a probability of 50%. This image is sourced from [21].

SARG04 Protocol

In 2004, Scarani, Acin, Ribordy and Gisin developed the SARG04 protocol which was similar in principle to the BB84 protocol [22]. SARG04 defers from BB84 only in the classical sifting procedure. After the photons have been transmitted, Bob announces the actual measurement that he received instead of announcing the measurement basis used for each qubit. Alice then creates the key by inferring the measurement basis used by Bob. The SARG04 protocol has proven to be more robust against the photon number splitting attack (discussed further in chapter 2.2.2) in the special case of a *Quantum Bit Error Rate* (QBER) equal to zero. In the case of a non-zero QBER, the SARG04 protocol is proven to be at least as effective as the BB84 protocol.

B92 protocol

The B92 protocol developed by Charles Bennett in 1992 shows that QKD can be realised by using just two non-orthogonal states, instead of the four states proposed in the BB84 protocol [18]. Alice chooses any two non-orthogonal states, eg. $|0\rangle$ and $|+\rangle$, and transmits the polarised photons to Bob. Bob will measure the states using the measurement set $\{|1\rangle, |-\rangle\}$.

Therefore, if Alice prepares state $|0\rangle$, and Bob measures with $|-\rangle$, there is a 50% probability that Bob will get a measurement. However, if Bob had chosen to measure with $|1\rangle$, there would be a 0% probability of Bob obtaining a measurement. Bob announces the instances for which he had valid measurements and Alice and Bob only keep these qubits as their sifted key. The instances without recorded measurements are discarded. Table 2.2 shows an example of how Alice and Bob can establish a sifted key using these states. For an ideal QKD transmission, the B92 protocol has an efficiency of 25% since, on average, one out of four photon transmissions will result in a measurement [23]. An experimental realisation of the B92 protocol is described by Jeong et al [24].

LM05 Protocol

The LM05 protocol, developed by Lucamarini and Mancini in 2005 is similar to the BB84 protocol in the sense that it also requires two non-orthogonal bases and a total of four quantum states [25]. LM05 differs from BB84 and B92 since it is a two-way protocol. The key distribution process begins with Bob randomly choosing and transmitting a quantum state. Alice receives these qubits and chooses to either apply a universal 'NOT' gate, thereby flipping the bit value of the qubit or she can choose to leave the qubit unchanged. The qubits are then transmitted back to Bob. Bob measures each photon in the original basis that he used to encode them. Since Alice does not change the measurement basis of the photons, there is no need to carry out any sifting procedures. The raw key is therefore ready for error correction and privacy amplification.

Table 2.2: An example of establishing a sifted key using the B92 protocol.

Bit values randomly generated by Alice	0	1	1	0	1	0	0	1
Alice sends	→	↗	↗	→	↗	→	→	↗
Bob's basis	↑	↑	↖	↑	↖	↑	↖	↑
Does Bob obtain a measurement?	N	Y	N	N	N	N	Y	Y
Chosen bits		↗					→	↗
Bit values of the sifted key		1					0	1

2.2.2. Postprocessing

The Quantum Bit Error Rate (QBER) of a cryptosystem is defined as the percentage of errors contained in the sifted key [10]. The errors in a key distribution process can arise from misalignments and poor visibility in the optical set up, the dark counts of the single photon detectors and in appropriate cases, inefficiencies of an entanglement source.

The sifted key established in the previously mentioned protocols is not ready to be used as a cryptographic key. Alice and Bob must first compare their keys and establish the level of errors for their transmission. Alice and Bob implement an algorithm that exchanges parities of parts of the key [26]. They can determine an acceptable bit error rate due to the apparatus and background noise. If the bit error rate is found to be much larger than the bit error rate that was agreed upon, Alice and Bob have detected the presence of an eavesdropper. In this scenario, the key would be discarded. After the process of error correction, the key is referred to as the reconciled key. During error correction, Eve may gain more information about the key, therefore, a further precaution is taken to ensure security. This is the process of privacy amplification [27]. The length of the reconciled key is reduced by implementing a further algorithm. This is done to decrease the mutual information between Alice and Eve to an acceptable level. The key is then referred to as the secured key and is ready to be implemented with any algorithm to encrypt the plain text.

2.2.3. Eavesdropping

Theoretically, QKD is proven to be unconditionally secure. Since an eavesdropper cannot violate the laws of physics, in particular, the No-Cloning Theorem or the Heisenberg's Uncertainty Principle, the use of quantum particles allows the transmission of the key to be totally secure. The vulnerability of QKD, however, lies in the physical implementation of the distribution process [28]. Eavesdroppers are able to exploit particular weaknesses in the equipment used for QKD in order to gain information about the cryptographic key. One of the most commonly exploited devices is the single photon detectors used by Bob, since the efficiency of these devices is very low. This section will highlight some of the common attacks that an eavesdropper may implement, as well as the respective countermeasures.

The simplest of these attacks is the intercept and resend attack [29]. In this scenario, Eve intercepts and measures all qubits transmitted from Alice to Bob. She then transmits her measurements to Bob, using a new stream of qubits. Figure 2.3 shows the possible errors that Eve may introduce into the cryptosystem. Since Eve is required to randomly choose a measurement basis, there is a 50% probability that she may obtain the incorrect measurement. If this is the case, the probability of Bob obtaining the incorrect measurement when using the correct measurement basis increases. The presence of Eve will therefore bring the QBER of the system to 25%. The unusually high error rate will be observed by Alice and Bob and the key is discarded.

It is imperative that a QKD system prevents the transmission of pulses with more than one photon. In this scenario, Eve will be able to split the pulse using a beam splitter and measure one of the photons without disturbing the other. This is referred to as the *photon number splitting attack* [28]. Using this attack, Eve will gain information about the cryptographic key without being detected by Alice and Bob. In order to prevent this, the power of the laser pulse used as a single photon source is reduced such that the mean photon number is less than one. The mean photon number will follow a Poissonian distribution, so the probability of obtaining more than one photon per pulse is negligibly small.

The *Decoy State protocol* can be used as a countermeasure against the photon number splitting attack [30]. For this protocol, Alice sets varying mean photon numbers to the laser pulses used as the pseudo-single photon source. The pulses consist of the quantum signal and decoy pulses of a different mean photon number. A portion of the pulses are also prepared containing no photons. Eve does not know which pulse is a decoy and which is a part of the quantum signal, and will therefore be forced to make measurements on all parts of the signal. Due to the varying detection probability of the pulses, any interference from Eve can be detected by Alice and Bob.

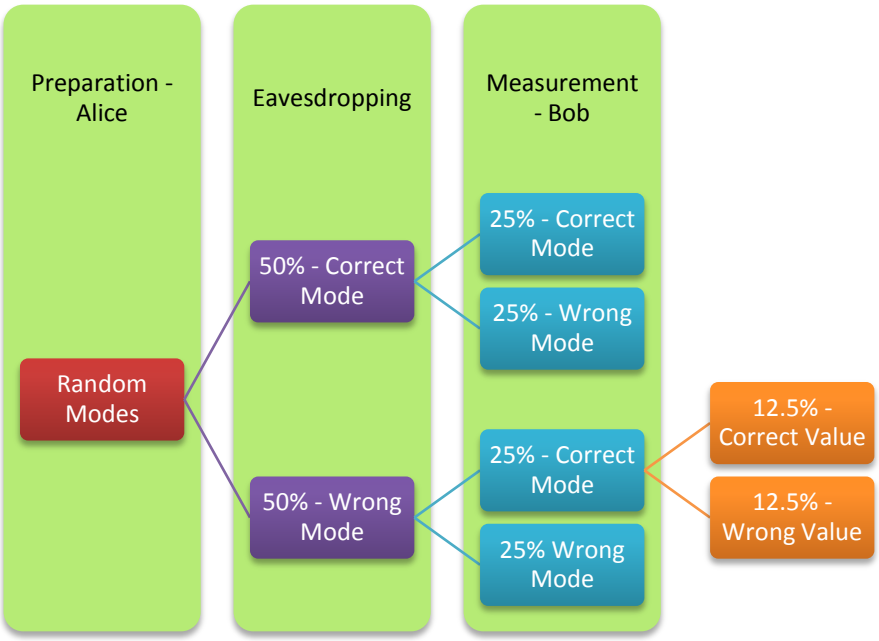


Figure 2.3: This figure shows the potential errors that Eve can introduce into the QKD process using the intercept and resend attack. Assuming that Bob chooses the correct measurement basis for the photon that Alice prepares, he will only obtain the correct measurement with certainty if Eve also chooses the correct measurement basis. In the case that Eve does not choose the correct basis, there is a 50% probability of Bob obtaining the incorrect measurement although he used the correct basis. Due to these instances of Bob choosing the correct basis and Eve choosing the incorrect basis, 12.5% of thr raw key will be incorrectly measured. This will increase the QBER to approximately 25%, which is easily noticed by Alice and Bob.

One of the methods that Eve could use to gain control over Bob's measurement would be to induce double clicks [26]. A double click occurs when both detectors register a photon simultaneously. Eve forces a detection in Bob's apparatus by sending many photons to Bob. If Bob measures in the same basis that Eve transmitted in, he will register a single click. The single photon detectors used by Bob are designed such that a large number of photons in one pulse will still be counted with a single click. Eve exploits this implementational flaw. If Bob measures in the incorrect basis, each of the detectors will measure 50% of the photons, thus resulting in double clicks. Usually, Bob discards double clicks, and will therefore be left with measurements forced by Eve. Bob will not detect any unusual errors in this setup but Eve will have gained all the information about the key. As a countermeasure, Bob should take note of the number of double clicks measured during the transmission and instead of discarding these double clicks, it is safer to assign a random value to this bit. This way, Eve will not gain any information about the key.

Eve could also use the *Trojan-horse attack,* which is implemented on phase encoded, Plug and Play systems [31]. Eve is positioned just outside of Alice's apparatus and she interrogates Alice's phase modulator with bright pulses. Eve is then able to detect any back-reflected portion of the bright pulses. The reflected light will carry the information that Alice has encoded into the single photons used for the key. Eve times her bright pulses between the single photon pulses, so as not to disturb the quantum signal. Alternatively, Eve uses a different wavelength for the bright pulses so that they cannot be detected by Alice and Bob. Therefore, the presence of Eve is not easily detected by the authenticated users.

Some countermeasures that could be used against the Trojan horse attack include using detectors and circulators in Alice's setup in order to protect against classical pulses. Filters for wavelength, polarisation and temperature could also be used to make sure that no external light enters Alice's apparatus. Preventing eavesdropping can also take on a more offensive approach. Alice could transmit bright pulses that would blind Eve's detectors. This would require precise synchronization between Alice and Bob, but would be effective in immobilizing Eve.

A recently developed hacking method called the faked-states attack was designed as an improvement to the intercept and resend attack [32]. Eve situates herself between Alice and Bob and measures the incoming signal from Alice by randomly choosing a measurement basis. Eve then transmits her measurement to Bob and ensures that Bob will obtain the same result. Eve controls which detector Bob receives each measurement with by transmitting bright pulses that will only register a click if measured in the correct basis. If Bob uses the incorrect basis, the optical power of the pulse will be shared between two detectors and neither will register a click. By this method, Eve only allows a detection if the result will match her measurement. This allows Eve full information of the cryptographic key, without significantly increasing the QBER of the system. In order to manipulate Bob's apparatus, Eve exploits timing loopholes in the single photon detector gates. A countermeasure against the faked-state attack would be to implement a finer timing resolution for the detector gates so as to prevent Eve from forcing a detector click outside of the gating interval. However, implementing this countermeasure can prove difficult. Additionally, Bob can install watchdog detectors for Eve's bright pulses.

In summary, it is important to point out that by using the eavesdropping methods discussed above, Eve does not affect the QBER of the system [33]. Therefore, Alice and Bob would not be aware of her presence and will not discard the compromised key. It is necessary to explore the possibilities of different quantum hacking techniques so that countermeasures may be developed. So far, it is relatively easy to prevent a specific attack by implementing so-called *band aid* solutions. However, a general, provable countermeasure for all types of attacks is yet unknown [33].

2.2.4. Current Implementations of QKD

Commercial implementations of QKD use phase encoding schemes, usually with the BB84, B92 or SARG04 protocols. One of the most widely implemented QKD systems is the idQuantique *Plug and Play* system [34]. In this application, bright pulses originate in Bob's apparatus and travel through a closed loop, receiving attenuation and the encoding at Alice. The pulses are then transmitted back to Bob by a Faraday mirror. The system uses polarisation encoding and polarisation beam splitters to control the path that the photons take within the interferometer. The round trip that the photons must make, ensures that any birefringent effects caused by the fibre are reversed. One of the shortcomings of using a bidirectional channel is that the relative phase between pulses can be affected by Rayleigh scattering [35]. This is avoided by precisely timing the train of pulses so that there is no interaction between pulses transmitted in opposite directions. An advantage of the Plug and Play system is that it is stable and polarisation independent.

A number of research groups have maintained long term tests based on the stability of quantum networks. The most notable of these projects include DARPA, TokyoQKD, SECOQC, SwissQuantum and the QuantumCity and QuantumStadium projects. The latter two were carried out by the Centre for Quantum Technology at the University of KwaZulu-Natal.

The DARPA network was the first metropolitan quantum network to be put into operation [36]. This implementation began in 2004 and included six nodes. The project grew to incorporate ten nodes with both fibre and free space channels. This system was able to generate a secure key generation rate of approximately 1 kbit/s, while maintaining a QBER below 3%. The SECOQC network, established in 2008, consisted of 5 nodes and included both fibre and free space channels [37]. The sifted key generation rate of this network was also 1 kbit/s. The TokyoQKD network linked five nodes with all-fibre channels [38]. Due to the usage of aerial fibre, the channel contributed to the high losses experienced in the system. This resulted in a relatively low secure key generation rate of between 0.25 and 304 kbit/s. The SwissQuantum network consisted of three nodes and was implemented to test the long term stability of a quantum network using encryption modules produced by idQuantique [39].

The Quantum City project was developed in 2008 as a test bed for a quantum network in the eThekwini municipality [40]. The network consisted of three peripheral nodes linked to a central node via the fibre infrastructure of Pinetown and Westville. The QuantumStadium project, implemented at the Moses Mabhida Stadium in Durban, became the first global event to utilise a QKD system to encrypt security data transmitted from the stadium's Venue Operations Centre to a Joint Operations Centre outside of the stadium [41]. This project was carried out during the 2010 FIFA World Cup™. Both the QuantumCity and the QuantumStadium projects used encryption modules produced by idQuantique.

3. The Use of Fibre and Free Space as QKD Channels

The first experimental demonstration of QKD was realised via a 30 cm free space laboratory setup by Charles Bennett *et al* in 1991 [42]. Since then, many groups have successfully implemented QKD cryptosystems either in laboratory sites or in practical applications. In order to practically realise quantum cryptography, the QKD protocols mentioned in chapter 2.2.1 must be implemented over a quantum channel. The two most common telecommunication channels are free space and fibre optic networks, therefore, QKD research has been focussed on developing cryptosystems that can utilise these networks. This will allow for QKD to be used as an encryption technique for mainstream telecommunications. The advantages and limitations of each of these channels will be discussed in this chapter.

3.1 Fibre Optic Channel

A fibre optic cable is manufactured from glass and is usually doped with germanium or aluminium in order to create differences in the refractive index within the fibre [43]. Single mode fibre consists of a core of a diameter between 6-10 μm and multimode fibre has a core diameter usually larger than 50 μm. The core is surrounded by cladding which has a diameter of 125 μm. The core and cladding are then protected by a coating which has a typical diameter of 250 μm, as shown in Figure 3.1.

The core is doped in order to have a higher refractive index than the cladding. The difference in refractive index between the core and the cladding is described by

$$n_1 - n_2 < 0.05 . \tag{3.1}$$

This difference in refractive index at the boundary between the core and the cladding causes total internal reflection of light, as long as the angle of incidence of the light is larger than the critical angle of the fibre, as shown in Figure 3.2. Therefore, the fibre acts as a waveguide as light is propagated through it, shown in Figure 3.3 [43]. Fibre exhibits optimal transmission at specific wavelengths, therefore, using these wavelength ‘windows’ can greatly increase the transmission distance of the fibre optic channel [44]. There are three main wavelength bands used for fibre optic communication and these are shown in Figure 3.4.

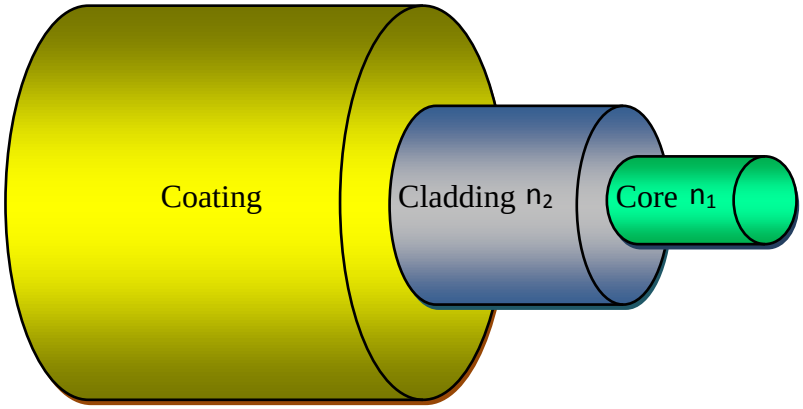


Figure 3.1: A schematic diagram of the structure of a fibre optic cable. The refractive index of the core, n_1, is larger than the refractive index of the cladding, n_2.

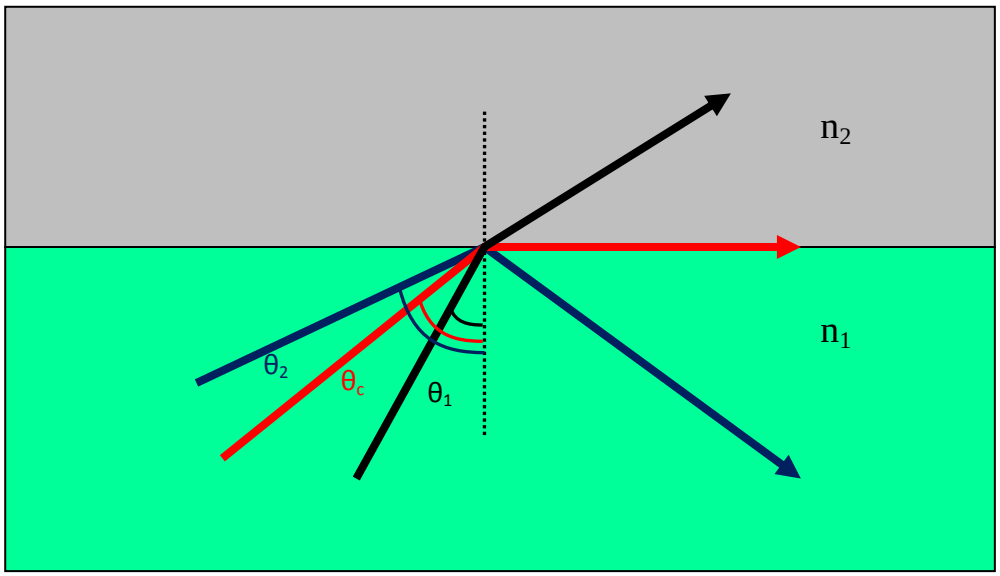


Figure 3.2: A diagram showing the condition for total internal reflection. The refractive index n_1 is larger than n_2, causing refraction of the transmitted light. The angle θ_1 is smaller than the critical angle, θ_c, allowing the light to escape the core of the fibre. The angle θ_2 however, is larger than θ_c, which causes the beam to be reflected back into the fibre.

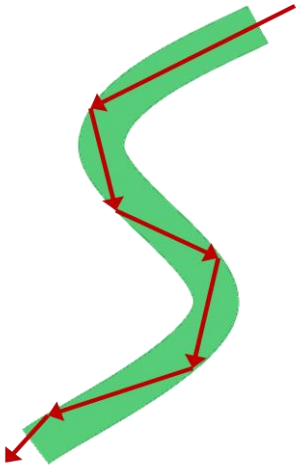


Figure 3.3: A diagram showing the propagation of light through fibre. The light is trapped in the core due to the process of total internal reflection. The fibre therefore acts as a waveguide, propagating the trapped light to the output of the fibre, regardless of the path that the fibre takes.

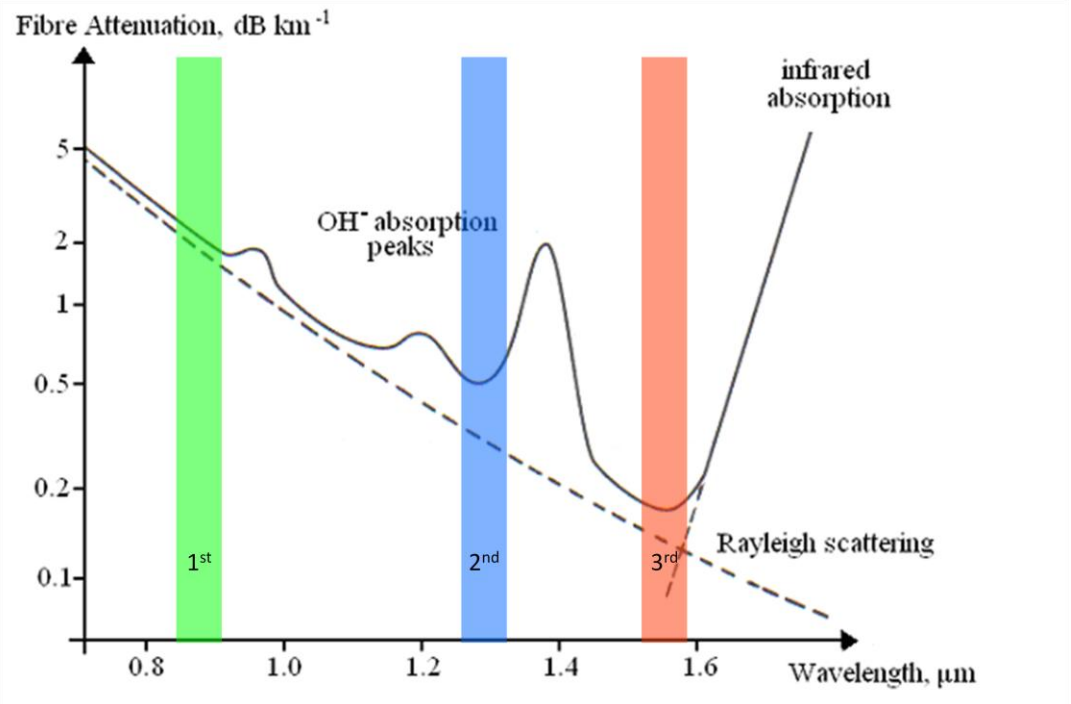


Figure 3.4: The wavelength dependent attenuation peaks in fibre optic cables. The minimum values correspond to the transmission peaks of fibre and the three most common transmission wavelengths are highlighted: 890 nm which still has a high attenuation level and is therefore best suited to shorter distances, 1310 nm which has a very low level of dispersion and 1550 nm which has the lowest level of attenuation and is therefore suited to long distance communication. This image is sourced from [44].

A fibre optic link is suitable for shorter distances of approximately 100 km, such as a metropolitan network [45, 46]. It has the advantage of being independent of a line of sight connection between the transmitter and receiver and can link multiple end users to one central node. It is therefore best suited for metropolitan areas with existing laid fibre networks. With the use of Wavelength Division Multiplexing, quantum signals can be transmitted over live fibre, thus removing the need for dark fibre for the key distribution process [47]. Such an implementation would create redundancy in the quantum network, which would minimise public network downtime due to QKD transmissions. This allows for QKD to be accessed by any user connected to the public network, integrating QKD as an encryption method for commercial telecommunications.

Fibre optic quantum links offer higher bit rates during key transmission. The fibre is protected by cladding, which provides low levels of noise in the fibre optic cable, hence there are fewer errors to discard during the key distillation process. Unlike a free space quantum channel, laid fibre is not affected by local atmospheric conditions. This makes the fibre optic channel more stable against changes in temperature and weather. Laid fibre is also protected from vibrations which can cause a disturbance in the quantum signal [48].

Transmitting over large distances is a challenge for a fibre channel because impurities in the fibre absorb photons and the qubits become too weak to measure after a length of 100-200 km [10]. Due to impurities and manufacturing errors, fibre optic cables have a minimum loss of 0.2 dBm per km and the longest recorded fibre quantum channel was 250 km [49]. Increasing the transmission distance of a fibre channel would require a quantum amplifier or quantum repeater, but these devices have not yet been developed [50].

Photons also lose power if a fibre is bent too sharply and some of the light is able to leave the core of the fibre [48]. Fibre optic cables are highly dispersive mediums and such an effect will reduce the signal quality of a quantum channel. Modal dispersion creates a broadening of the laser pulse due to modes travelling at different velocities [48]. This would require the single photon detectors to have a longer gating width. However, this would increase the dark count rate of the detectors, resulting in a higher quantum bit error rate. To rectify this problem, only single mode fibre can be used for QKD. Since only one mode can be propagated through the fibre, there is no interference between different modes and no broadening effect due to varying mode velocities.

Another significant disadvantage is that a fibre optic cable cannot maintain the polarisation of the light transmitted through it. This is due to the birefringence caused by stresses on the fibre which leads to an increase in the bit error rate. Therefore, compensation techniques must be implemented for a fibre link to be feasible. This will be discussed further in Chapter 7.

Birefringence also causes polarisation mode dispersion which is a broadening of the laser pulse due to the decoupling of the components of polarisation. This will put a constraint on

the clock rate of the laser [51]. The timing scale of polarisation mode dispersion can be in the order of tenths of picoseconds per 1 km for standard fibre [52]. The timing resolution of single photon detectors is in the order of hundreds of picoseconds, therefore these effects can be neglected for the short distances that are allowed by the fibre optic channel [53]. Polarisation mode dispersion becomes a challenge when bit rates exceed 10 Gb/s. This problem has been addressed in [54].

3.2 Free Space Channel

A free space channel provides a line of sight connection between Alice and Bob. The quantum signal is transmitted through the atmosphere between ground-ground, ground-satellite, satellite-satellite or satellite-ground stations [55]. This is shown in Figure 3.5. An advantage of free space QKD technology is the capability of transmitting a cryptographic key to a lesser developed area which may not have a fibre optic network. QKD transmission over rough terrain to remote locations can then be achieved. The atmosphere is a non-birefringent material and can therefore, maintain the polarisation of light. For this reason, QKD over a free space channel usually utilises states of polarisation to encoded qubits [42].

As with fibre, the atmosphere also exhibits optimal transmission efficiency for particular wavelength windows. This allows a greater transmission length for single photons of particular wavelengths [56, 57]. Figure 3.6 shows these wavelength-dependent windows of optimal transmission in the atmosphere. A wavelength of 780 nm is usually chosen for communications as this corresponds to an efficiency peak of silicon avalanche photo-diode detectors.

A free space link can allow for longer transmission distances compared to a fibre optic channel. The attenuation of a free space channel varies with respect to atmospheric conditions. Factors that contribute to atmospheric attenuation include low clouds, rain, snow or dust [57]. These impurities in the atmosphere can cause absorption of photons, scattering and scintillation of the beam. Atmospheric attenuation can be reduced to two main parameters: the visibility of the atmosphere and the distance travelled by each photon [57]. The visibility is defined as the distance travelled by the photon for its power to decrease by 2%. Attenuation due to the apparatus can be linearly added to this value. Approximations for the error rate experienced in a free space link have shown that for good visibility (greater than 6 km) the error rate can be kept below 3% [57].

Figure 3.5: An example of a free space channel linking two terrestrial locations via a satellite connection. This image is sourced from [58].

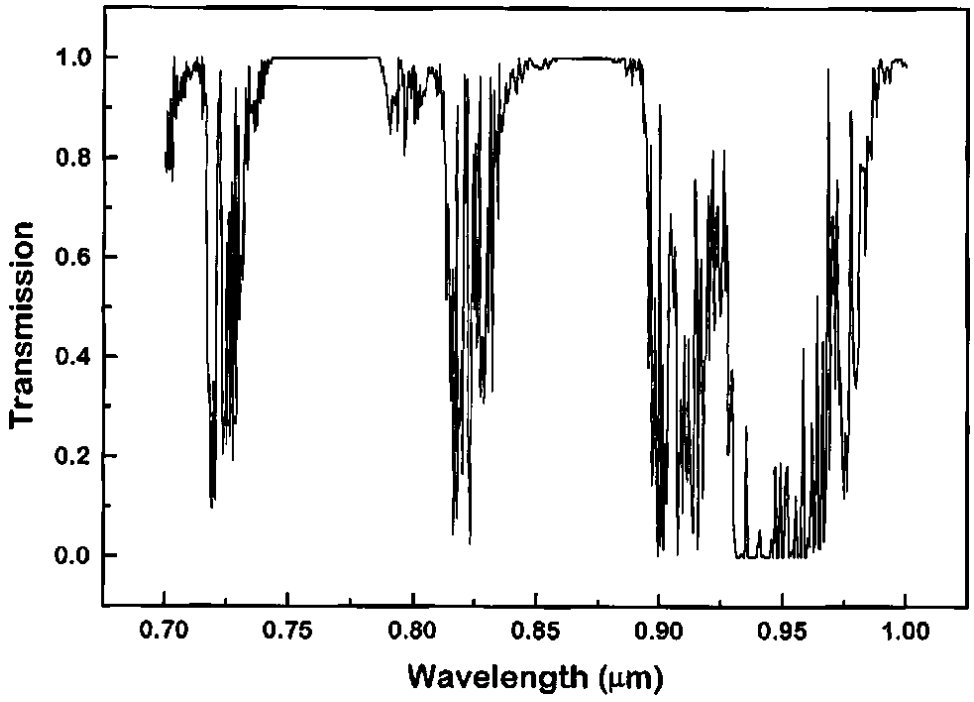


Figure 3.6: A graph showing windows of optimal transmission of different wavelengths in the atmosphere. This image is sourced from [10].

A free space link does however, have a few disadvantages with regards to implementation. Turbulent conditions can cause inhomogeneities in the refractive index of the atmosphere. This can cause a spreading of the laser beam between Alice and Bob [55]. The atmosphere is a medium which introduces a lot of background noise when transmitting a single photon. This can provide a better environment for an eavesdropper since disturbances caused by an eavesdropper can be mistaken for natural errors. The varying properties of the atmosphere, such as radiance from the sun or the moon, variable weather and cloud cover make single photon transmission difficult but these problems are addressed by implementing filtering techniques [57, 59]. Filtering can improve on the efficiency of a free space link such that it becomes a feasible method for QKD. There are 3 main categories of filtering techniques used for a free space channel:

-Spatial filtering: The solid angle visible by the receiver is reduced so that the detector is correlated only to the single photon source of the transmitter. This reduces atmospheric noise incident on the detector.

- Spectral filtering: A spectral filter only allows the specific wavelength produced by the single photon source to be measured by the detector. This prevents other wavelengths being detected and thus reducing noise in the quantum channel. Spectral filtering is especially important for daylight QKD as sunlight can overpower the faint signal of a single photon. By measuring only a specific wavelength, the photons become more distinguishable against background noise.

-Temporal filtering: The single photon source and the detector are synchronized so that the detector will only make a measurement when the source emits a photon. This reduces the measurement of noisy signals. Synchronising the transmitter and receiver will also prevent valid qubits from entering the detector during the detector dead time and this will increase the detection efficiency of the receiver. An additional time delay must be considered for instances when a turbulent atmosphere introduces a time jitter to the transmission [55].

By taking these filtering techniques into consideration, the efficiency of a free space QKD channel can be greatly improved.

3.3 Integrating QKD Channels Towards a Global QKD Network

Due to the upper bound on transmission distance, a fibre optic link is not feasible for long distance or global communication. However, the main advantage of a free space channel is that it can support transmission over longer distances [60]. This creates the possibility of QKD via satellite which opens the door for a global QKD network. Creating a link between a fibre channel and a free space channel, will allow for fibre-based metropolitan networks to connect to a local free space node. The free space nodes can transmit to a satellite network and thereby connect to another metropolitan network at another location as shown in Figure 3.7.

Such a methodology will bring together the advantages of a fibre network, such as a higher signal-to-noise ratio, and the larger transmission distance of a free space network. In order for such a global network to be successful, there must be an untrusted interface between the fibre network and the free space link. Coupling a fibre channel to a free space channel would allow for greater transmission distances since free space has a lower attenuation and a weaker dispersion property compared to fibre. It would also allow for various mediums of communication to be used in one meshed network. A relay device that can convert the quantum systems between various encoding schemes without actually measuring the systems would require the development of quantum repeaters and quantum memories. This would allow for a transition between a phase encoded fibre system and a polarisation encoded free space system. However, these devices are still being researched [50]. It is therefore necessary to create a passive interface between the fibre channel and the free space channel.

In order to achieve this, only one type of encoding can be used throughout the entire network. Therefore, it is necessary to develop either a phase encoded QKD system which operates over free space or a polarisation encoded QKD system which can operate via a fibre channel. Both these technologies pose implementational challenges but developing at least one of these is essential for a meshed network. Research is currently being done to allow for phase encoded QKD to be implemented over free space using Laguerre-Gauss modes. These modes carry Orbital Angular Momentum (OAM) which is used as the bit encoding for QKD [61]. Using OAM states provides the advantage of an infinite level system which can increase the bit rate of the key distribution process. However, coupling such a system to a fibre network would pose a problem since OAM states would require multimode fibre. Due to the negative effects of modal dispersion, only single mode fibre is used for QKD purposes.

Alternatively, polarisation encoding can be used over both channels. It is easier to implement polarisation encoding over a free space channel since the atmosphere is not birefringent, therefore, polarisation encoding must also be implemented through fibre. This poses a problem since a standard single mode fibre optic cable is not able to maintain the SOP of light that is transmitted through it due to birefringence. Therefore, the first challenge that must be overcome is a fibre optic cable's inability to maintain the state of polarisation of light that is transmitted through it. By overcoming this challenge, an untrusted interface can be developed between a fibre channel and a free space channel.

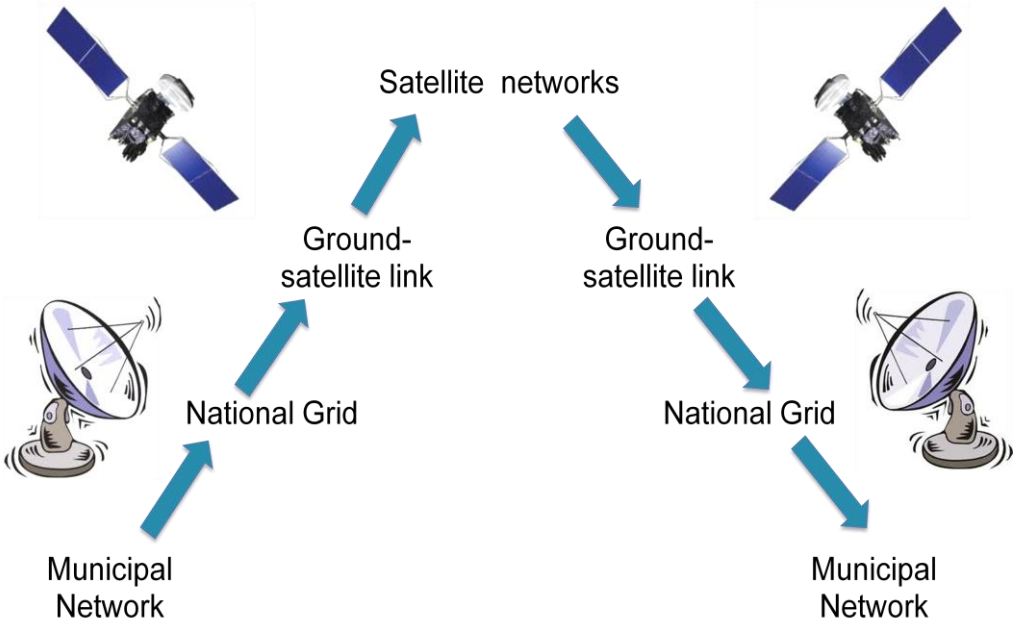


Figure 3.7: A schematic of the potential setup for a global QKD network.

4. Theory of Polarisation and Birefringence

4.1. Polarisation

Polarisation can be considered as the orientation of the electric field of an electromagnetic wave. The electric field oscillates transversely to the direction of propagation and can be in the form of a plane wave (linearly polarised light) or a spiral wave (circularly or elliptically polarised light) [62]. In the case of linearly polarised light, the orientation of the electric field is constant and can be represented as two orthogonal components of amplitudes E_{0x} and E_{0y}, both as a function of the propagation direction, z, and time, t,

$$\vec{E}_x(z,t) = \hat{\imath}\, E_{0x}\, \cos\,(kz - \omega t) \tag{4.1}$$

$$\vec{E}_y(z,t) = \hat{\jmath}\, E_{0y}\, \cos\,(kz - \omega t + \varepsilon). \tag{4.2}$$

The propagation vector of the wave is given by k and the frequency is described by ω. The term ε is the relative phase difference between the two components. If ε is described by

$$\varepsilon = m\pi\,,\ m \in \mathbb{Z}\,, \tag{4.3}$$

The resultant electromagnetic wave will also be linearly polarised, but it oscillates in a tilted line. If the relative phase between the orthogonal components of the state of polarisation is described by

$$\varepsilon = -\frac{\pi}{2} + 2m\pi\,,\ m \in \mathbb{Z}\,, \tag{4.4}$$

the electric field then becomes

$$\vec{E}_x(z,t) = \hat{\imath}\, E_0\, \cos\,(kz - \omega t) \tag{4.5}$$

$$\vec{E}_y(z,t) = \hat{\jmath}\, E_0\, \cos\,(kz - \omega t)\,. \tag{4.6}$$

In this case, the direction of the electric field varies with time and is not restricted to one plane. Thus, the resultant is described as circularly polarised light. If the electric field vector rotates in a clockwise direction, the wave is referred to as right-circularly polarised. If the electric field vector rotates in an anti-clockwise direction, the wave is referred to as left-circularly polarised.

Both linear and circular SOP's can be considered as special cases of elliptical polarisation, which includes all possible SOP's. Elliptical polarisation states are formed when the orthogonal components of the electric field differ in phase by $\pi/2$ but the amplitudes of the components are not equal. In the special case of the components having equal amplitudes, circular polarisation is obtained.

For a polarisation encoded implementation of the BB84 protocol, the states of polarisation that are traditionally used are vertical, horizontal, right diagonal and left diagonal, which are all linear states. However, since any two non-orthogonal bases can be used, it is also feasible to use circularly polarised light as one of the bases.

4.2. Optical components

The two optical components that are most commonly used to manipulate states of polarisation are half wave plates and quarter wave plates. When light is transmitted through a half wave plate, orthogonal components of the SOP are transmitted at different velocities [62]. This is because each of the components is aligned with the ordinary axis and the extraordinary axis of the wave plate respectively. The component aligned with the extraordinary axis will be transmitted faster through the medium than the other. Figure 4.1 shows an example of this. In this figure, the vertical component is aligned with the extraordinary axis and therefore, travels faster through the medium than the horizontal component. At the output of the medium, the vertical component has shifted half a wavelength relative to the horizontal component, thus resulting in a reflection of the state of polarisation about the optical axis of the wave plate. The half wave plate can similarly reflect an elliptical state of polarisation and invert the handedness of circularly polarised light[62]. Using this principle any SOP can be rotated by adjusting the optical axis of the half wave plate.

A quarter wave plate works with a similar principle to the half wave plate. In this case, however, the phase difference between the orthogonal components of the SOP is equal to a quarter of the wavelength of the light. This phase shift results in linear states of polarisation being transformed to elliptical states. In the special case of linear polarisation at an angle of 45°, the quarter wave plate produces circularly polarised light, as shown in Figure 4.2. Similarly, if elliptical or circular light is incident on the quarter wave plate, linearly polarised light will be produced.

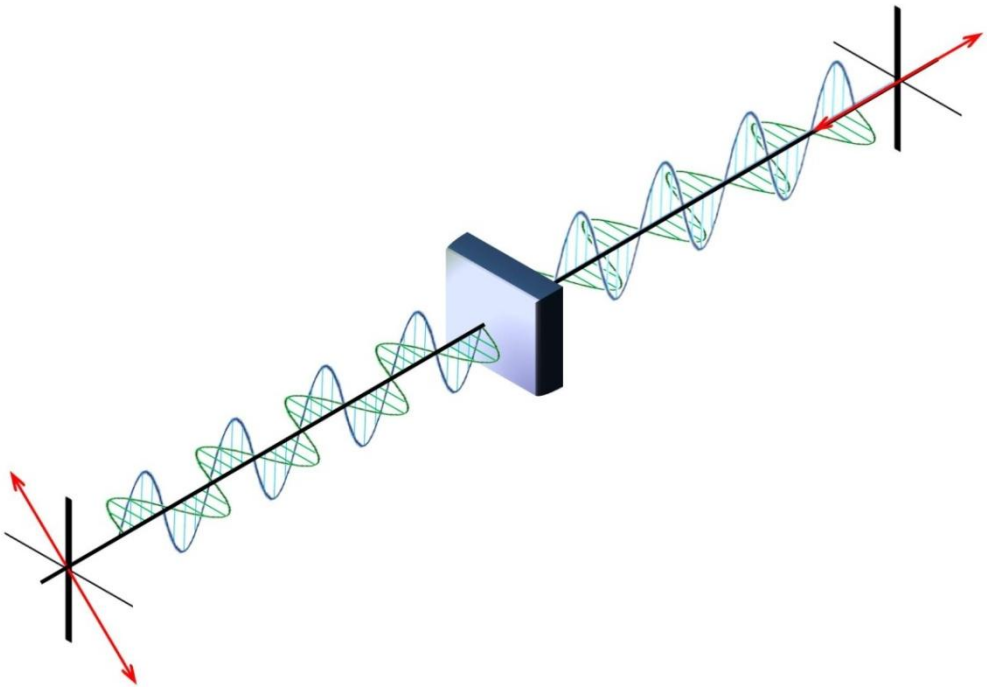


Figure 4.1: A diagram showing the effects of a half wave plate on linearly polarised light. The vertical component is transmitted faster than the horizontal component, thus resulting in a rotation of the state of polarisation.

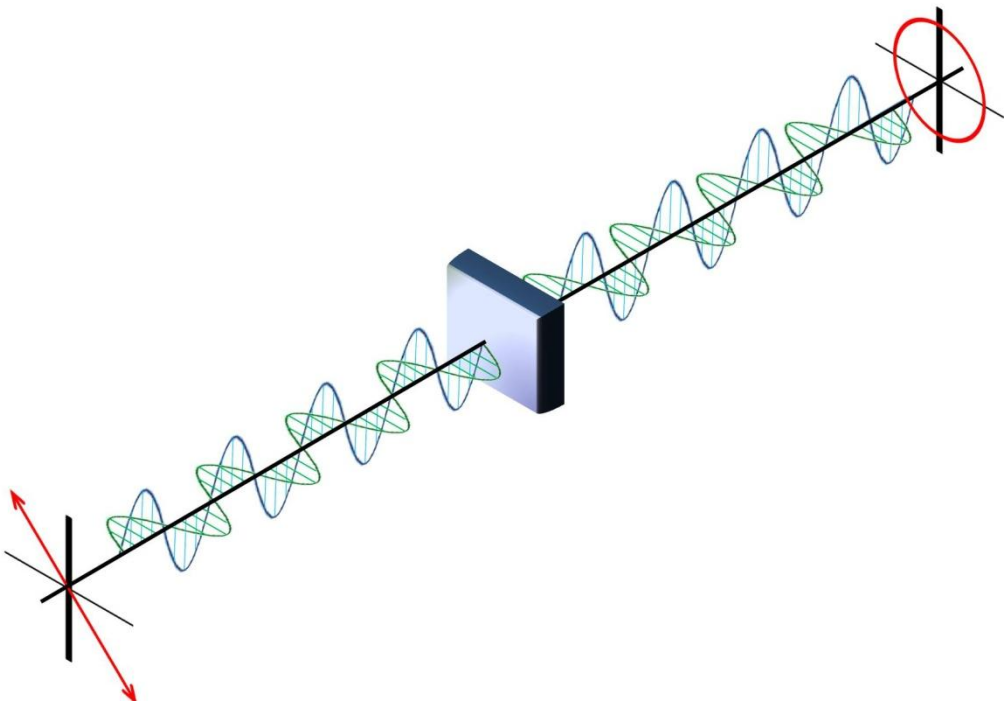


Figure 4.2: A diagram showing the effects of a quarter wave plate on linear, diagonally polarised light. The phase shift induced by the wave plate transforms the diagonal state of polarisation to a circular state of polarisation.

4.3. Jones matrix notation

A state of polarisation can be represented as a column vector, called a Jones vector. The components of the vector represent the *x*- and *y*-components of the electric field vector [62]. The Jones vectors for the six states of polarisation that are most commonly used for the purpose of QKD are shown in Table 4.1. Any optical device that causes a transformation of a SOP can be represented as a 2x2 matrix, called a Jones matrix. Table 4.2 shows a list of common optical devices and their respective Jones matrices. The evolution of a SOP when it encounters an optical device can be represented by

$$E_t = A\,E_i\,. \tag{4.7}$$

Ei is the Jones vector of the input SOP and *A* is the Jones matrix representing the optical device. The resulting SOP is given by E_t. Each of the optical components in an experimental setup is represented by its own Jones matrix. The total effect of all these components on a state of polarisation is the matrix product of all the individual component matrices applied in reverse order [62].

Since a quarter wave plate results in a phase difference between the two orthogonal polarisation components of a quarter of a wavelength, the effect of a half wave plate can be equated to the effect of two quarter wave plates in succession. Therefore, the Jones matrix of a half wave plate is actually the matrix product of two matrices representing quarter wave plates.

4.4. Birefringence

Birefringence refers to the double refraction of light when transmitted through an anisotropic medium [62]. Orthogonal components of the state of polarisation of light are transmitted through the medium at different speeds. This is called the differential group delay [48]. The component that is perpendicular to the optical axis of the medium is the ordinary ray and the component that is parallel to the optical axis of the medium is the extraordinary ray. The refractive differences between the ordinary ray and the extraordinary ray causes a decoupling of the components and the result of such a decoupling effect is the rotation of the state of polarisation as the light is transmitted through the material. Figure 4.3 shows how a SOP is rotated as it is transmitted through a birefringent material such as a fibre optic cable.

Table 4.1: The Jones vectors representing the six most commonly used SOP's. Sourced from [62].

State of polarisation	Jones vector
Horizontal	$\begin{bmatrix}1\\0\end{bmatrix}$
Vertical	$\begin{bmatrix}0\\1\end{bmatrix}$
Diagonal (+45)	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$
Diagonal (-45)	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$
Right Circularly Polarised	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$
Left Circularly Polarised	$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}$

Table 4.2: The Jones matrices representing the most commonly used phase retarders.

Phase Retarder	Jones matrix
Quarter Wave Plate (fast axis vertical)	$e^{i\pi/4}\begin{bmatrix}1 & 0\\0 & -i\end{bmatrix}$
Quarter Wave Plate (fast axis horizontal)	$e^{i\pi/4}\begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$
Half Wave Plate	$\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$

4.5. Birefringence in a Fibre Optic Cable

Birefringence occurs due to asymmetries in the fibre optic cable. This can be due to impurities in the fibre or manufacturing errors [63]. Figure 4.4 illustrates potential manufacturing errors which may cause irregularities in the fibre. These irregularities cause a fixed rotation of any state of polarisation that is transmitted through the fibre. This rotation can be corrected with the use of a passive polarisation controller. If the rotational effect of the fibre optic cable is represented by Jones matrix *A*, then the Jones matrix of the polarisation controller is the inverse of *A* such that

$$E_i = A\, A^{-1} E_i \ . \tag{4.8}$$

The polarisation controller therefore applies the inverse of the rotation caused by the birefringence effects, returning the SOP to its original form.

If the fibre is bent or subject to environmental stresses, such as heating or vibrations, the birefringent effects will vary randomly with time [64]. Therefore, an active polarisation controller must be used to correct for the changes in the state of polarisation of photons in real time. The effects of the fibre's birefringence must be regularly tested and the polarisation controller must be adjusted each time in order to compensate these changes. The SOP of each qubit must be accurately transmitted between Alice and Bob in order for them to obtain a cryptographic key, therefore, without this active polarisation control, implementing polarisation encoded QKD protocols over a fibre channel will not be achievable.

It is not feasible to use polarisation maintaining fibre for the QKD transmission. Polarisation maintaining fibre induces a forced and fixed birefringence on any transmitted light [64]. This prevents the SOP from rotating due to any natural effects such as bends and temperature gradients. In order for an SOP to be maintained, it must be aligned with either the fast or slow axis of the polarisation maintaining fibre. Therefore, non-orthogonal SOP's will not be simultaneously maintained during transmission [10]. Therefore, in order to utilise polarisation encoded QKD in a public network, a polarisation compensator must be developed.

If just one SOP was being transmitted from Alice to Bob, then the effects of birefringence can easily be corrected by a *polarisation locker*. Since QKD requires the transmission of randomly chosen non-orthogonal states, correcting each of these independent states becomes more complex. Therefore, compensation for birefringence effects must be done in real time for all SOP's. This requires an active compensation system which will be able to test the changes in the SOP and correct all states.

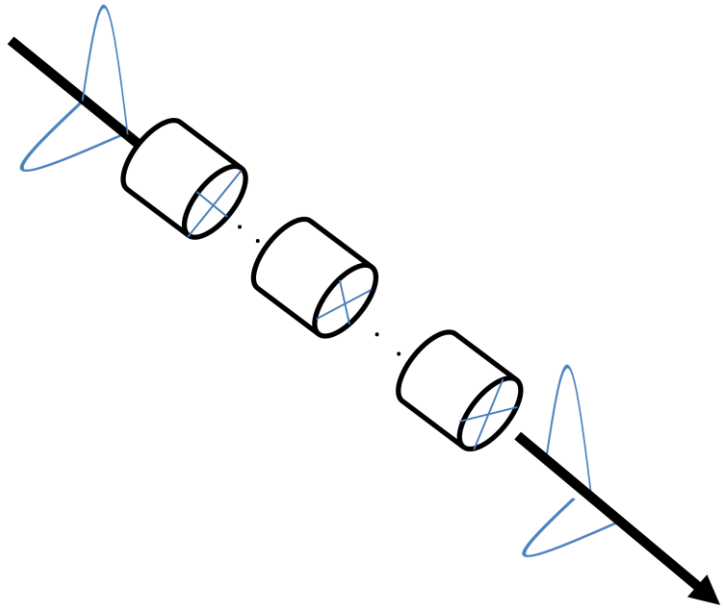


Figure 4.3: Diagram depicting how a state of polarisation is rotated as it is transmitted through a fibre optic cable. The cross sections of the fibre show that the orthogonal components of the SOP are rotated during transmission due to their differing speeds.

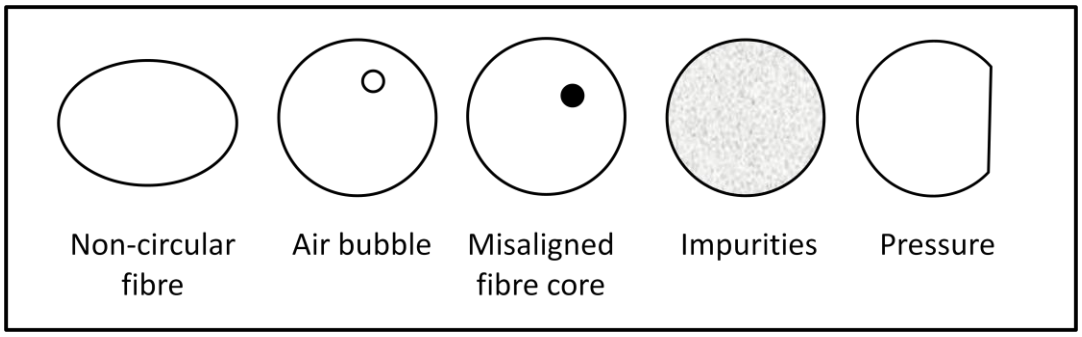


Figure 4.4: Various irregularities which may cause asymmetry in a fibre optic cable.

5. *Fibre-based Implementations of Polarisation Encoded QKD*

In 1994, Breguet, *et al*, demonstrated a polarisation compensation system in a fibre channel of 1100 m [65]. Two quarter wave plates were used to correct for the birefringence effects in the fibre channel. This minimised any ellipticity of the state of polarisation caused by the fibre channel. The orientation axis of the polarisation beam splitter was then adjusted in order to correct for any linear rotations. The error rate of the compensation system was maintained below 0.54%. Recent developments in autocompensating the effects of birefringence in fibre are discussed in this chapter.

Chen, *et al*, used Time Division Multiplexing (TDM) to separate the single photon signal from the reference pulses used for feedback [66]. The experiment was initially attempted with Wavelength Division Multiplexing (WDM), but due to the shortcomings of this method, WDM was discarded. The smallest difference between the wavelength of the single photons and the wavelength of the reference pulses was 0.8 nm, due to the channel bandwidth of the Dense Wavelength Division Multiplexer. This difference in wavelength meant that the changes in SOP were not identical for both the quantum and the classical channels due to the property of wavelength-dependent fibre birefringence. Furthermore, the changes in SOP for both channels deviated more from each other as the length of the channel increased.

A Time Division Multiplexed system used a single photon signal at a repetition rate of 1 MHz and reference pulses for real time polarisation feedback control, both at a wavelength of 1550 nm. An asymmetric Mach-Zehnder interferometer was used to introduce a 50 ns time delay between the single photons and the reference pulses. A 50/50 coupler was used to separate the two signals to different detectors. The single photon detectors were also set with appropriate gate delays in order to distinguish between the single photons and the reference pulses that may have arrived at the wrong detector. The measurements from the reference signal detectors were processed by a computer and two analogue signals were generated to control the squeezers of the Electronic Polarisation Controller in order to reverse the birefringent effects of the fibre channel.

The quantum channel was reported to be 50 km long and it was noted that the propagation distance could have been limited by the Rayleigh scattering of the reference signal. The

raw key generation rate was approximately 500 bit/s and the quantum bit error rate was approximately 5.27% for this system.

The same research group also devised another TDM-based system for polarisation compensation using the 'interruption' method [67]. In this case, the quantum signal is periodically stopped in order to allow for the transmission of the bright reference pulses. Due to the difficulties in compensating both non-orthogonal bases used for the BB84 protocol with one polarisation controller, this scheme was designed with two polarisation controllers, one for each basis. The single photons were separated into two compensation settings by a 50/50 beam splitter. This process acted as a means for Bob to randomly choose a measurement basis. The photon would then be compensated with respect to that basis. If the basis chosen for the SOP by Alice and the compensation basis matched, this would result in a correct measurement. If the basis for the SOP did not match the compensation basis, the SOP would not be returned to its original state and this would result in an error. However, since the photon is being measured in an incompatible basis, the post processing rules of the BB84 protocol dictate that this qubit must be discarded. Therefore, the incorrect compensation does not affect the Quantum Bit Error Rate of the system. The system was tested for quantum channels of lengths 50 km, 75 km and 100 km. The quantum bit error rates for these channels were kept below the security threshold. The maximum quantum bit error rate was 6.6%, obtained for the 100 km channel.

Liu, *et al*, of The National Institute of Standards and Technology (NIST) designed a polarisation compensation scheme for fibre QKD [68]. The objective of this design was to create a simple and user-friendly system in order to make polarisation encoded QKD in fibre more practical. The system used time division multiplexing to deploy a test signal in order to calculate the changes in the state of polarisation of the photons. These changes were calculated using the intensity of the signal incident on the single photon detectors. A polarisation controller was then used to correct the changes. For a proof of principle, the system was demonstrated on a 4 m quantum channel and a sifted key rate of 12 kbits/s was achieved. The system was then used for a 2 km quantum channel and the sifted key rate obtained was 2 kbits/s. The quantum bit error rate was tested over a period of 3 hours and fluctuated below 10%. Future work will focus on automating the system.

The above mentioned research group from NIST have carried out many qkd experiments. A pair of data handling circuit boards were designed to manage the bit stream, generate random numbers and carry out the post processing algorithms of the key generation process [51]. Using an initial clock rate of 1.25 Gbs, a mean photon number of 0.1 and a channel length of 1 km, the system produces a sifted key rate of 1.1 Mbs with a quantum bit error rate lower than 1.3%

Two Polarisation Recovery and Auto-Compensation (PRAC) subsystems were developed and integrated into the above mentioned system [69]. The first of these subsystems is based on liquid crystal retarders (LCR). A pair of LCR's were used as one polarisation controller and their axes were prealigned with the polarisation beam splitter placed before the

detectors. The retardance of the LCR's was controlled by a computer via an applied voltage. That allowed the SOP of incoming light to be rotated to any arbitrary value in order to execute the BB84 or B92 protocols. The response time of this system was approximately 100 ms.

The second subsystem was based on 3-axis piezo polarisation controllers. Each controller consisted of three piezo-driving phase retarders and the retardances of each were fixed at $\pi/4$, $\pi/2$ and $\pi/4$ respectively. Each retarder was independently controlled by a driver and any arbitrary SOP transformation could be achieved. This subsystem was easier to implement in comparison to the LCR subsystem since the piezo controllers did not have to be aligned with the polarisation beam splitter. Since the piezo system is fibre-based, the insertion loss was minimal. The response time of this system is approximately 30 microseconds but the communication speed of the RS232 connection between the piezo system and the computer greatly slows down the response time to approximately 150 ms.

This system used Time Division Multiplexing to compensate for the change in SOP. The transmission between Alice and Bob was stopped every 15 minutes and predetermined test pulses were transmitted over the channel and measured using predetermined bases. If the extinction ratio was too low, the recovery process was initiated. Different voltages were applied to the polarisation controllers and the extinction ratio was measured for each setting until the optimal setting was found. At first, a coarse-step search was used to find the optimal area and this was followed by a fine-step search to locate the correct setting. The number of steps can be as large as 2500 and total recovery time can be as high as 6 minutes for the LCR system and 8 minutes for the piezo system. Since the change in SOP varies over time, the recovery time is not fixed. The system was tested in a laboratory for a period of 24 hours and on average, the operation time for the LCR system was 15 seconds and for the piezo system, 36 seconds. Future improvements on the systems will focus on reducing the operation time while still maintaining precision.

In 2006, Tang, *et al*, of NIST reported on some of the challenges in producing a sifted key rate over Mbit/s [70]. The main drawback of high-speed key production is the dead time property of the single photon detectors. Once a detector has detected a photon, the gate closes and the detector temporarily shuts down in order for the electrons in the Avalanche Photo Diode to dissipate. This reduces the number of dark counts but increases the time taken for the detector to make two consecutive measurements. This effect makes it more likely that another detector measures the next photon therefore, consecutive bits are more likely to have different values. This correlation between consecutive bits is seen as a security hazard as random nature of the key is being compromised. The data-dependent timing jitter caused an increase in the QBER for an initial clock rate of about 1 GHz and higher. It was reported that the QBER can be reduced with an improvement in circuitry and quantum channel hardware. The bit repetition rate was doubled, compared to the previous reported experiment. This caused the sifted key rate to increase to 2 Mbit/s. After the process of privacy amplification, a net key rate of approximately 1 Mbit/s was achieved. To illustrate the relevance of this net key rate, the group reported to have

securely transmitted a high-speed video over the internet using the key generated by this experiment.

Tang, *et al*, reported a key generation rate as high as 4 Mbit/s in 2006. This was achieved over a fiber channel of 1 km [71]. The system worked slower for a longer channel of 4 km. A later project in 2009 reported the development of a timing and data handling system which allowed QKD transmission at the maximum capacity of the single photon detectors [72].

In order to make a QKD system compatible with fibre-optic telecom networks, Xu, *et al*, also of NIST, developed an up-conversion subsystem to combine speed and reliability [73]. Telecom networks usually operate at 1550 nm or 1310 nm in order for the signal to reach a greater distance. However, higher detection efficiency is obtained for much shorter wavelengths for a silicon-based avalanche photo diode, around 700 nm. This system was able to generate a key at 500 kbit/s over a 10 km channel using the B92 protocol. The group also generated a key at 10 kbit/s over approximately 50 km. There are three prominent benefits for this system. First, a low dark count rate due to the detectors operating at 700 nm. Second, a single fibre is used for both the classical and the quantum channel and third, the chromatic dispersion is very low for a wavelength of 1310 nm.

Current research by NIST is aimed at making QKD systems more cost effective. In 2008, a Detection Time Bin Shift scheme was developed [74]. This scheme allows for the number of single photon detectors to be reduced since these devices are the most expensive components of a QKD system. By using time division multiplexing, one detector is able to measure in two different bases. This is achieved by introducing a coupler before Bob's detectors. Photons are lead through either a short line or a longer delay line . If a photon is transmitted through the short line , its SOP is unchanged and it is measured in the rectilinear basis. If the photon is transmitted through the longer line , its SOP is rotated by 45° and it is measured in the diagonal basis. This system provided a sifted key rate of approximately 1 Mbit/s with a QBER of 2%. The channel length was set at 1.1 km. Even though the sifted key rate is reduced, the benefit of this system is the decrease in security concerns due to the unbalanced characteristics of detectors and bit correlation caused by the dead time of the detectors.

Xavier, *et al*, have demonstrated a polarisation compensation system using Wavelength Division Multiplexing [53].The fibre channel was 8.5 km long and the single photon signal and reference signal were separated by 0.8 nm. The initial clock rate was set to 100 kHz and the quantum signal was made with 0.2 photons per pulse. The WDM introduced an insertion loss of 3.1 dB. The reference signal was launched from Bob to Alice. The counter propagation of the reference pulses reduced the noise caused by this classical signal to the effect of Rayleigh scattering. An additional filter kept this level of noise below the dark count rate of the single photon detectors. Two four-plate piezoelectric controllers, each aligned to a different axis of the Poincare sphere, were used to correct for the changes in SOP. Filters were used to reduce the noise created by Rayleigh scattered light. The

measurement of the SOP was done by placing a linear polariser in front of the polarisation controller and using the intensity measurements from the photon counter to gauge whether the light was aligned with the polariser. This system is similar to that used by NIST [69]. The change in SOP was corrected within a period of 10 ms for a worst case scenario. This shows that the system can be used to correct relatively fast changes in SOP. The precision of the system complied with the accepted QBER in quantum communications of approximately 1%. In order to test the effective isolation of the reference signal from the quantum signal, the power of the reference signal was raised to +5 dBm. Noise from the reference signal was still observed to be lower than the dark count rate of the single photon detectors.

This group collaborated with Gisin, *et al*, of The University of Geneva in 2009 in order to improve on the system [35, 75]. The piezoelectric controllers were replaced by a lithium niobate polarisation controller, thus allowing much faster compensation. A second lithium niobate controller was used by Bob to switch between measurement bases. In order to test the effectiveness of the lithium niobate controller, a polarisation scrambler was included in the quantum channel to introduce fast changes in SOP. The channel between Alice and Bob had a length of 16 km and losses of 4.3 dB. An average of 0.1 photons per pulse was produced by Alice. The QBER was measured at 1.6% without the use of the polarisation control system. With the control system active, the QBER actually increased by 1.1%. This was said to be due to fluctuations in the SOP caused by the stabilisation algorithm. The system was, however, successful in controlling fast fluctuations in SOP, thus enabling polarisation encoded QKD.

Goldenberg and Vaidman developed a protocol in 1995 (experimentally realised in 2010 by Avella et al in [76]) using just one pair of orthogonal states to encode the information transmitted between Alice and Bob [77]. Each state consisted was formed by the interference of two basis states that were launched through the quantum channel at separate times. The two basis states are transmitted through delay lines in order to separate them in time and they eventually interfere to form one of the qubits just before being measured by Bob. Alice and Bob can check the security of the key by checking for any timing delays in the transmission or an unusually high error rate in the signal. Since Alice and Bob only use one measurement basis, the key distillation procedure is unnecessary. The raw key is therefore used in the error correction and privacy amplification algorithms. Using only orthogonal states simplifies the polarisation compensation process, since just one state needs to be compensated. The orthogonal state will be automatically compensated, thus only one polarisation compensator is needed and a simple step search will yield the perfect setting for the compensator.

6. Testing the Changes in the State of Polarisation

As mentioned in Chapter 4.5, the birefringence effects in a fibre optic cable varies with time. This is due to any fluctuations in the environment around the cable. Any temperature gradients or vibrations will alter the birefringence over time. It is therefore necessary to develop an active compensation system that can monitor birefringence and correct for these effects in real time. Since each photon in the quantum signal has a unique SOP, the polarisation controller will have to adjust each one separately. This, however, poses two concerns. Firstly, the polarisation controller must be able to compensate each photon without prior knowledge of what each respective SOP is. This is necessary in order to maintain the security of the QKD protocol being utilised. Secondly, polarisation controllers must not measure the SOP of any photons, since this will destroy the encoded information before Bob can receive it. This means that the polarisation controller cannot measure the current SOP and then make adjustments to it accordingly. Instead, the setting for the polarisation controller must be independently determined prior to the QKD transmission and any adjustments made to the SOP's of photons must be done passively. In order to determine the correct polarisation controller setting, test pulses must be deployed into the system. The polarisation controller must be adjusted to compensate the test pulses and thereby passively compensate the quantum signal.

The first step towards building a polarisation compensation system is to first develop a method to test for the changes in the state of polarisation of the quantum signal. Either Time Division Multiplexing (TDM) or Wavelength Division Multiplexing (WDM) can be used to deploy test pulses into the system. The advantages and disadvantages of these methods will be discussed in this section.

6.1. Wavelength Division Multiplexing

WDM utilises a calibration signal with a wavelength close to that of the single photon signal. The test signal and the quantum signal are multiplexed and transmitted through the quantum channel together [53]. The signals are demultiplexed at Bob and the test signal is used for analysing the changes in the SOP acquired in the quantum channel. This can be done in real time and is more effective for generating higher key rates since the key generation process does not have to be interrupted [35, 53]. A disadvantage of WDM is the wavelength-dependence of birefringence effects [66]. Usually, the difference in wavelength between the test signal and the single photon signal is 0.8 nm. This small difference in wavelength can still result in significant differences in the change in SOP for

the two signals. The WDM method was tested in a laboratory set-up in order to check its feasibility in a QKD system.

Measurements were done to monitor the difference in the birefringent effects of fibre for different wavelengths. The experimental setup is shown in Figure 6.1. Two laser channels, each of a different wavelength, were first given an initial SOP using polarisation controllers, PC1 and PC2. The channels were multiplexed and transmitted through a fibre optic cable of 1.69 km. Both the channels were passed through PC3 so that the same effects could be applied to both wavelengths. The channels were then demultiplexed and measured on separate polarimeters, POL1 and POL2.

The wavelength of λ_1 was fixed at 1550.12 nm and the difference in wavelength between λ_1 and λ_2 was set to multiples of 0.4 nm. The settings of PC3 were gradually adjusted and ideally, both wavelengths should undergo the same changes. However, this small difference in wavelength can still result in significant differences in the change in SOP for the two signals. Figure 6.2 shows the difference in angles of inclination and azimuth of the SOP of both channels with regards to the Poincaré sphere. As seen in this Figure 6.2, the relative angles between the channels were not constant. Similar tests were carried out for various channel spacing and for a longer fibre length of 24.70 km. Similarly, the changes in SOP of the two channels were not the same.

In a polarisation compensation system, the WDM method would be used to correct the single photon signal, based on the errors measured in the test signal. This principle was tested using the manual polarisation controller, PC3. Both channels were set to the same SOP and the fibre optic cable between Alice and Bob was disturbed. PC3 was used to return channel 1 to its original state and it was found that the second channel was not always corrected simultaneously. This shows that when using WDM, compensating the test signal will not ensure that the single photon signal will also be compensated. This can result in a high quantum bit error rate which will compromise the security of the cryptosystem.

Non-linear effects can also have a negative impact on the quantum bit error rate of the system [78]. These effects occur due to a variation in the refractive index of the fibre dependent on the intensity of the transmitted light. The bright test pulse can, therefore, transform the polarisation state of the single photon signal if both are transmitted through the channel simultaneously. This will render any attempt at polarisation compensation obsolete since the single photons will be rotated by the compensation test pulse itself.

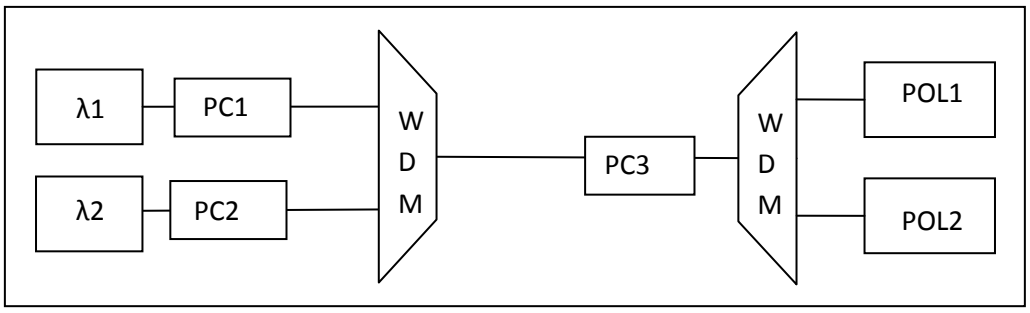


Figure 6.1: This experimental setup used to monitor the difference in the change in SOP for different wavelengths when subjected to the same conditions. The laser sources used for this experiment are represented as λ_1 and λ_2. The wavelength for λ_1 was fixed at 1550.12 nm and λ_2 was varied so that the difference between the two channels was set to multiples of 0.4 nm. Each of these signals was transmitted through a polarisation controller, PC1 and PC2 and were then combined with a wavelength division multiplexer, WDM. The signals were manipulated with polarisation controller PC3 and were demultiplexed. The separated signals were then measured with polarimeters, POL1 and POL2.

6.2. Time division multiplexing

For a system that uses TDM as a method to test the birefringence effects, the transmission of the single photon signal is stopped periodically and test pulses are then transmitted through the fibre [69]. This can be time consuming, and can decrease the key generation rate of the system. There is also a chance of the birefringent effects varying before the next test is done. However, if the time intervals between tests are optimised, the compensation of the single photon signal is more robust. Since the test signal and the single photon signal are of the same wavelength, the changes in the SOP of the single photons can be accurately measured by observing the test signals. Alternative to the interruption method, test pulses can be timed between single photon pulses to allow TDM in real time [66]. The signals are then separated at Bob and measured on separate detectors. This method does not have any negative effects on the key generation rate of the system but requires effective filtering so that the test pulses do not add noise to the quantum signal. The single photon detectors must be precisely synchronised so that the measurement gate only opens to allow a single photon pulse.

A SOP stability test was done under laboratory conditions by transmitting a polarised laser source through a length of fibre and measuring the SOP with a polarimeter for 16 hours. Changes in SOP measured during this test were due to environmental changes, such as a temperature gradient or vibrations caused by the equipment. The results are shown in Figure 6.3. These results were used to determine the period for a 1˚ change in the angles of azimuth and inclination in this environment. On average, these periods were 57.97 sec and 184.25 sec, respectively. Since orthogonal SOP's represent different bit values, a change of 90˚ can be considered as a total bit flip for the purpose of QKD. It is important to maintain

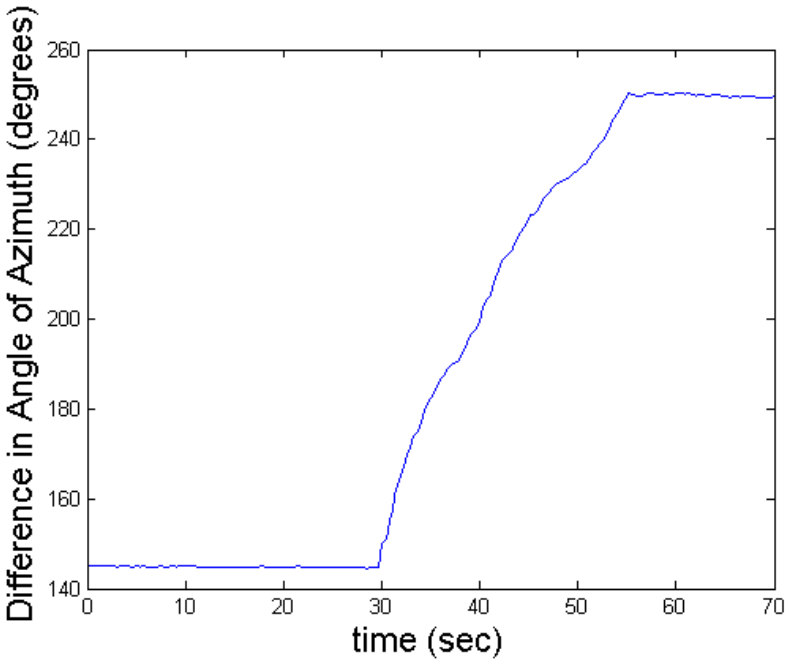
a low QBER so that errors caused by Eve are distinguishable from errors caused by the equipment and quantum channel. In order to achieve this, the SOP should not deviate too far from the intended state. A change in the angle of the SOP is proportional to the intensity of the measured SOP. This is shown using Malus' Law,

$$I = I_0 \cos^2\theta. \tag{6.1}$$

I_0 represents the initial intensity of the light. I is the intensity of the light after undergoing a rotation of angle θ and passing through a polariser with the original orientation [62]. The decrease in the intensity of the light with a change in θ and the subsequent increase of its orthogonal state are shown in Figure 6.4. Using this relationship, the QBER can be kept at an acceptable minimum by assigning an allowed angle of deviation. As an example, if an error rate of 1% is acceptable from the polarisation compensator, the angle of incident light may deviate by 5.74°.

The average period for the angle of azimuth on the Poincaré sphere to change by 5.74° was 332.75 sec and the corresponding period for the angle of inclination was 1057.59 sec. Therefore, when using TDM to test for the changes in SOP in this environment, the test signal must be deployed at least every 333 sec in order to ensure an acceptable quantum bit error rate. Of course, each environment is different and in order to effectively use the TDM method, a state of polarisation stability test must be done for each new environment that the system is set up in. Using the results from the stability test, the time interval for which the single photon signal can be transmitted without errors can be calculated. The duration of the test signal is dependent on the resolution of the compensator used for the system.

a)



b)

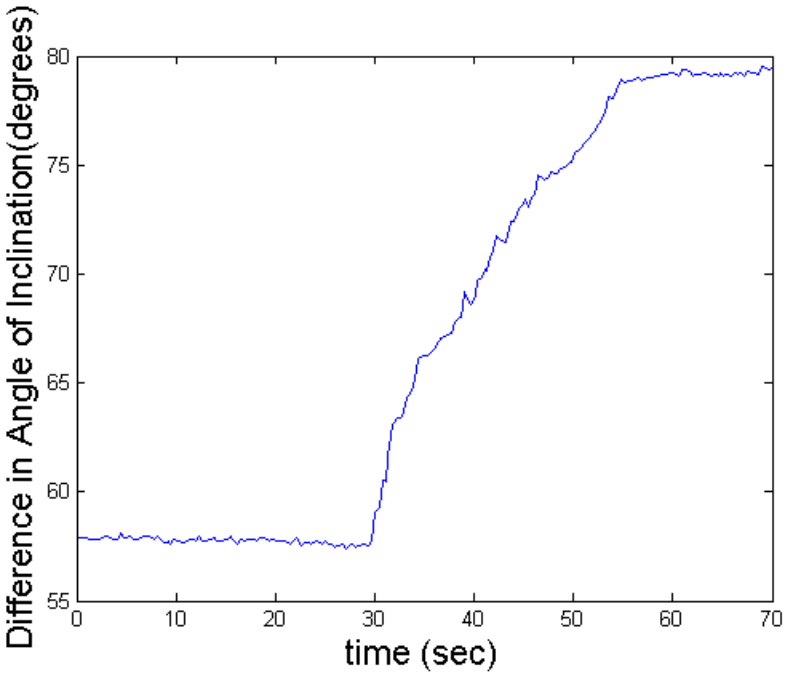


Figure 6.2: An illustration of the difference in the angle of a) azimuth and b) inclination between laser sources of different wavelengths. The wavelength spacing was 0.4 nm. The manual polarisation controller was gradually adjusted between the times of 30 sec and 55 sec. During this period, the difference of the angles of azimuth and inclination between the channels vary greatly.

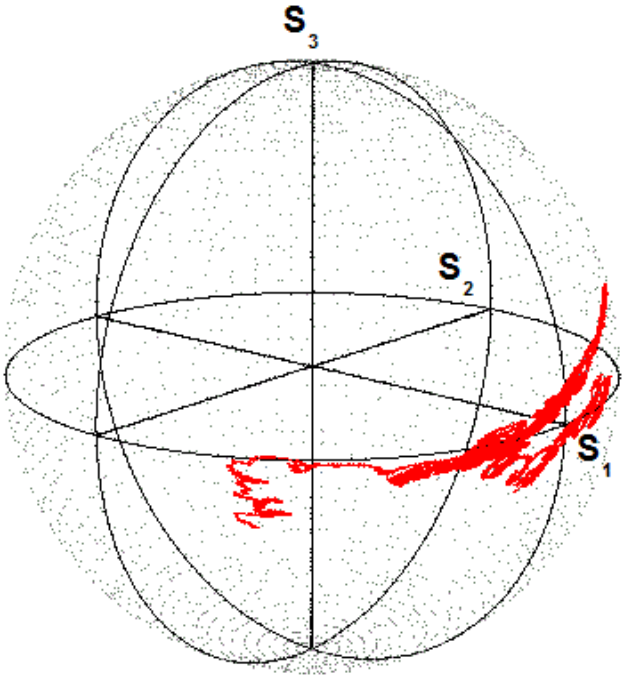


Figure 6.3: A plot of the SOP of a laser source over 16 hours. All changes in the SOP occur naturally with changes in the surrounding environment. The SOP of the laser source deviated from its initial state over this period, showing that polarisation compensation techniques must be used in order to carry out QKD over extended times.

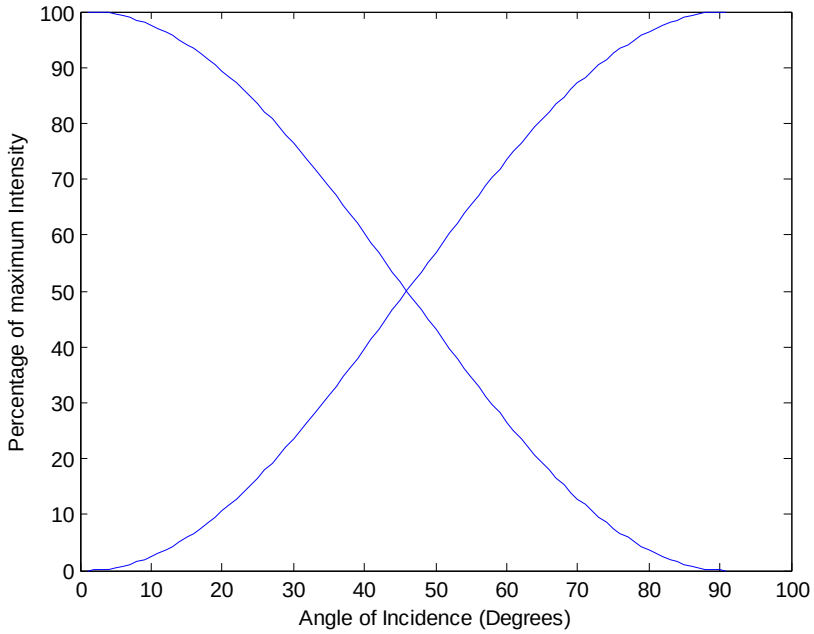


Figure 6.4: The change in the intensity of incident light with respect to the angle between the linear SOP and measurement basis. The consequent increase in the intensity of the orthogonal SOP is also shown.

7. Compensating for the Change in SOP

7.1. The Experimental Setup

The first step in developing the polarisation compensation system was to first set up a proof of principle experiment to show that the state of polarisation of a photon can be rotated back to its original state after undergoing changes in the quantum channel. The birefringence effect of the fibre channel is represented by a unitary transformation applied to the SOP of each photon [75]. The polarisation compensator must apply the inverse of the unitary transformation in order to return the state of polarisation back to its original state.

The experimental setup is shown in Figure 7.1. The components for Alice in this experiment consisted of a pseudo-single photon source and a polarisation state generator. The pseudo-single photon source was provided by a pulsed laser source with a wavelength of 1550 nm, attenuated to simulate the power of a single photon per pulse. The laser pulses were then randomly polarised by a polarisation state generator. The photons were then transmitted through a fixed 1000 m length of fibre which served as the quantum channel. The fibres used for the channel and the patchcords were single mode fibres with a core diameter of 6 μm, unless otherwise stated as polarisation maintaining fibre. The birefringence effects of the fibre on the SOP of the single photons was then corrected by a compensator. Different compensators were used for this application and the outcomes of each will be discussed in this chapter.

A half wave plate was installed after the length of fibre, before the photons were transmitted to a polarisation beam splitter. The half wave plate served as a means to change the measurement basis of the beam splitter. After the polarisation beam splitter, the photons were directed to one of two single photon detectors. The half wave plate, polarisation beam splitter and single photon detectors served as Bob in this experimental setup. Each of the components in the setup will be explained in further detail.

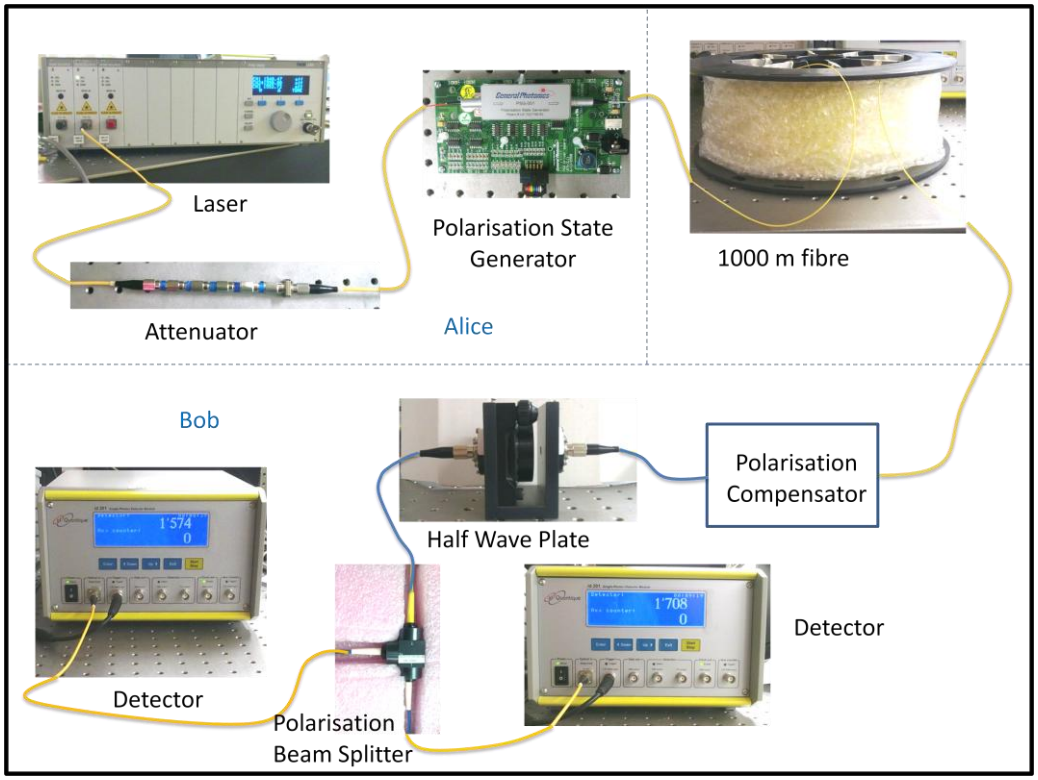


Figure 7.1: The experimental setup for a polarisation encoded quantum key distribution system. The laser source is pulsed and attenuated and then transmitted through a polarisation state generator. The polarised photons are then transmitted through the quantum channel. The state of polarisation of each photon is then corrected with a polarisation compensator. A half wave plate is used to randomly select the measurement basis of the detectors. A polarisation beam splitter then separates orthogonal polarisation states and the photons are measured using single photon detectors. The fibre between the output of the polarisation compensator and the polarisation beam splitter must be polarisation maintaining fibre. This is to make sure that the state of polarisation is not changed after the compensator makes the necessary corrections.

7.1.1. Laser and Attenuation

A laser of wavelength 1550 nm was chosen for this experiment. This wavelength experiences low absorption losses and is therefore suited to long distance fibre communication. This wavelength also corresponds to an efficiency peak of InGaAs avalanche photodiode detectors. The laser pulses were triggered by an external trigger provided by the single photon detectors. Each of the laser pulses initially contain a large number of photons which can be adjusted on the laser source. These pulses must be attenuated in order to simulate a single photon source. The number of photons in a laser pulse follows a Poissonian distribution [79].

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \quad . \tag{7.1}$$

In equation 7.1, $|\alpha|^2$ refers to the mean photon number per laser pulse. The probability of obtaining two photons in a pulse is given by

$$|\langle \alpha \mid 2 \rangle|^2 . \tag{7.2}$$

By first calculating $\langle \alpha \mid 2 \rangle$,

$$\langle \alpha \mid 2 \rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^{*n}}{\sqrt{n!}} \langle n|2\rangle \tag{7.3}$$

$$= e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^{*n}}{\sqrt{n!}} \delta_{2,n} \tag{7.4}$$

$$= e^{-|\alpha|^2/2} \frac{\alpha^{*2}}{\sqrt{2!}} , \tag{7.5}$$

the probability of obtaining two photons in a pulse is simplified to

$$|\langle \alpha \mid 2 \rangle|^2 = \left| e^{-|\alpha|^2/2} \frac{\alpha^{*2}}{\sqrt{2!}} \right|^2 \tag{7.6}$$

$$= e^{-|\alpha|^2} \frac{|\alpha|^4}{2} . \tag{7.7}$$

The mean photon number can now be substituted for $|\alpha|^2$. By setting the mean photon number to one, the probability of obtaining two photons in a pulse is given by

$$|\langle \alpha \mid 2 \rangle|^2 = e^{-1} \frac{1}{2} = 0.184 . \tag{7.8}$$

Similarly, the probability of obtaining three photons in a pulse is 6.1 x 10^{-2}.

The case of there being more than one photon per pulse will enable Eve to implement the Photon Number Splitting Attack [28]. As mentioned in chapter 2.2.3, Eve is able to separate the photons in a pulse using a beam splitter. She can then intercept one of the photons without disturbing the other. The remaining photon can be sent to Bob without any evidence that Eve has tampered with the signal.

To reduce the probability of there being more than one photon per pulse, the laser pulses must be attenuated to a value smaller than one. For this experiment, the laser pulses were attenuated to a value of 0.1 of the power of a single photon. By recalculating equation 7.8, now with a mean photon number of 0.1, the probability of obtaining two photons per pulse becomes

$$|\langle \alpha \mid 2 \rangle|^2 = e^{-0.1}\frac{0.01}{2} = 4.5 \times 10^{-3}, \quad (7.9)$$

and the probability of the pulse containing three photons decreases to 1.5 x 10^{-4}. These values are negligibly small and the information that Eve may gain from intercepting multi-photon pulses is not enough for her to gain the cryptographic key. Lowering the mean photon number of Alice's source will lower the key generation rate of the system, since in this case, only one out of every ten pulses actually contain a single photon. However, the advantage of this method is that the security of the cryptographic key is fortified against the photon number splitting attack.

The required power of each laser pulse in order to obtain the equivalent power of a single photon per pulse is calculated as

$$P_{\text{Watts}} = \frac{hcf}{\lambda}. \quad (7.10)$$

This value is dependent on the clock rate, *f*, of the pulses. The power per pulse required for a mean photon number of 0.1, converted to units of dBm, is given by

$$P_{dBm} = 10 \log \frac{0.1 \times P_{Watts}}{1mW}. \quad (7.11)$$

For this experiment, the pulse frequency was set to 100 kHz and the wavelength of the laser source was 1550 nm. Substituting these values into equation (7.10), and converting this power to dBm, the power of each laser pulse was required to be -119 dBm.

To achieve this, in-line optical attenuators were installed to bring the power of each laser pulse sufficiently low. In-line optical attenuators are manufactured from doped fibre which result in a fixed attenuation to any light that is transmitted through it [80]. Bearing in mind that other components of the experimental setup also contribute to the attenuation of the beam, the total attenuation of the in-line attenuators and the equipment must result in -119 dBm laser pulses leaving Alice.

7.1.2. Polarisation State Generator

The polarisation state generator (PSG-001 from General Photonics) uses 6 magneto-optic rotators to produce any SOP on the Poincaré sphere [81]. The incoming light is passed through an initial polariser which aligns the SOP with the optical axis of a quarter wave plate which is situated between the rotators. The magneto-optic rotators are subjected to either a positive or negative voltage which rotates the light by 22.5˚ and -22.5˚ respectively. The combined effect of the rotators result in the output SOP's. The PSG is used to generate the six SOP's that may be used for QKD: vertical, horizontal, +45˚ (right diagonal), -45˚ (left diagonal), right circularly polarised and left circularly polarised. Figure 7.2 displays each of these SOP's on the Poincare sphere. Table 7.1 shows the bit configuration required for each SOP, where 1 represents a positive voltage and 0 represents a negative voltage.

7.1.3. Polarisation Beam Splitter

The polarisation beam splitter separates two orthogonal states of polarisation by allowing one to be transmitted through the crystal, while the other is reflected [62]. In this experimental setup, the horizontally polarised photons were transmitted through the beam splitter and the vertically polarised photons were reflected. Figure 7.3 depicts this property. The vertically and horizontally polarised photons could therefore be measured with separate detectors. An additional half wave plate was installed before the polarisation beam splitter so that the measurement basis could be changed. In order to separate diagonally polarised photons, the half wave plate first rotates the incoming photons back to the rectilinear basis so that they may be split by the beam splitter.

7.1.4. Single Photon Detectors

The single photon detector used for this experiment was the id201 InGaAs/InP avalanche photo diode detector [82]. The photo diode consists of a semi-conductor material. The absorption band of the semiconductor is influenced by a weak electric field so that electrons and holes drift according to their polarity. The multiplication band is influenced by a strong electric field so that charge carriers are accelerated in this region. An incident photon strikes the absorption band and produces an electron-hole pair. These drift to the multiplication band which already contains excited electrons in the strong electric field. Any additional energy causes collisions between the excited electrons and each collision excites more electrons. This results in an 'avalanche' of electrons being detected.

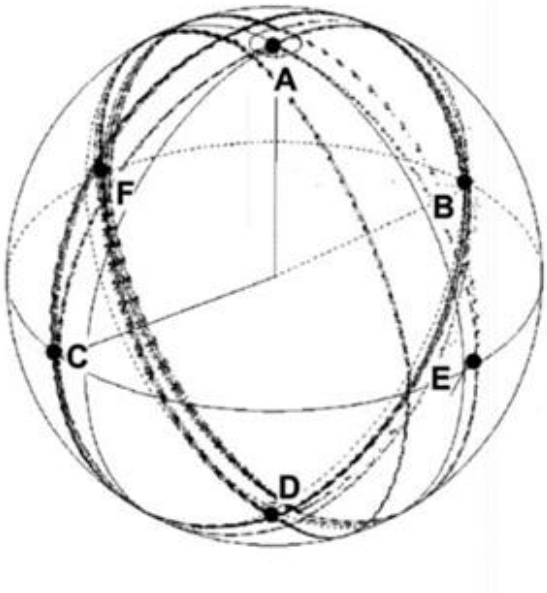


Figure 7.2: A diagram portraying the SOP's produced by the PSG on the Poincare sphere. The points A and D represent the circularly polarised SOP's. The points B, C, E and F represent the linear states usually used for QKD, i.e. vertical, horizontal, right diagonal and left diagonal. This diagram is sourced from [81].

Table 7.1: A list of the SOP's provided by the PSG and the corresponding combination of voltages applied to the magneto-optic rotators. Sourced from [83].

Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	SOP
0	**0**	**0**	**1**	**0**	**1**	**LCP**
1	**1**	**0**	**1**	**0**	**1**	**RCP**
1	**0**	**1**	**0**	**1**	**1**	**L -45**
1	**0**	**1**	**0**	**0**	**0**	**L +45**
1	**0**	**1**	**1**	**1**	**1**	**Horizontal**
1	**0**	**1**	**0**	**1**	**0**	**Vertical**

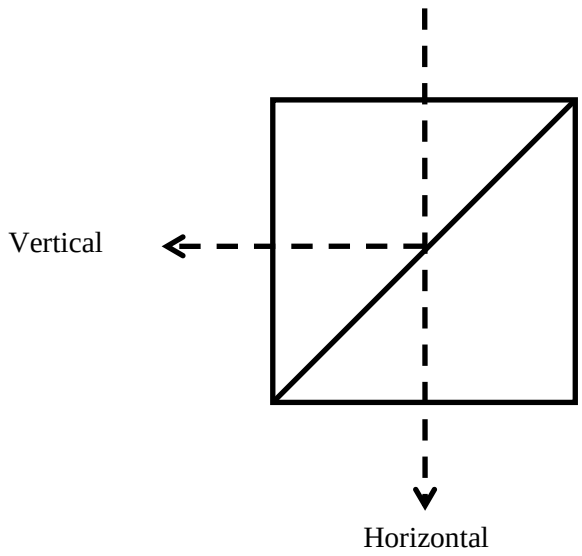


Figure 7.3: A diagram showing the effects of a polarisation beam splitter.

The avalanche must be quenched before the detector is ready to take the next measurement hence a *dead time* is introduced. This is the time taken for a detector to recover after a photon is counted so that it may register the next photon without interference from the avalanche of the previous measurement [84]. This can happen when electrons become trapped within the multiplication layer of the detector and are only released after the avalanche [85]. The spontaneous release of these delayed electrons can trigger an avalanche of excited electrons without the incident photon and will result in a false count (dark count) being measured. This interference is referred to as afterpulsing. The detector must therefore be switched off so that all excited electrons may dissipate before the detector accepts another photon. If not, the quantum bit error rate will increase due to dark counts. The detector will ignore any incident triggered signals for the duration of the dead time [86]. This means that the detector may miss some measurements, which decreases the efficiency of the detector. It is important to note that the quenching time will not affect the security of the key distribution process, but will just decrease the key generation rate.

The gate width is the time for which the detector allows the measurement to take place. A shorter gate width is beneficial as this will reduce the level of noise incident on the detector. This, however, requires that the transmitting and receiving systems be precisely synchronized. A longer gate width will allow for a discrepancy in the synchronisation between the source and the detector, but this will also allow for more false detections. For this experimental setup, the gate of the detector was triggered by the internal trigger of the detector. This was also used to trigger the laser. A delay was programmed into the detector so that the gate only opened when an incoming laser pulse was ready to be detected.

An increase in the temperature of the detector will result in higher thermal energy of the electrons in the detector. Higher energy leads to more spontaneous breakdown which will result in an avalanche of electrons. An increase in temperature will therefore lead to an increase in dark counts due to thermal noise [87]. A decrease in temperature will 'freeze' electrons thus electrons require a longer time to dissipate after the avalanche. This makes afterpulsing common at low temperatures. In order optimise the detector against these effects, the temperature of the detector was set to -50˚C.

The dark count rate of the single photon detectors proved problematic when measuring very faint pulses. A dark count occurs when a detector registers a count when no photons are present. These are caused by thermal and tunnelling effects [87]. This means that the detectors are unable to provide a `zero' measurement and it is difficult to differentiate between a dark count rate and a very weak laser pulse. Comparing two detectors also posed as a challenge since no two detectors are manufactured exactly alike. By altering the bias voltage of each detector, similar results could be acquired for both detectors measuring the same signal. The biasing voltage alters the potential across the semiconductor of the detector [88]. The device is reverse-biased, therefore, an increase in the bias voltage will increase the probability of an electron moving from the absorption band to the multiplication band, as shown in Figure 7.4. This will increase the probability of an avalanche, and therefore, a photon count. Similarly, a decrease in the bias voltage will decrease the probability of a photon being measured by the detector.

7.2. Testing of Compensators

7.2.1. Half wave plate

As a proof of principle demonstrating that the state of polarisation of a photon can be returned to its original state after being transmitted through a fibre optic cable, a half wave plate was installed as the polarisation compensator. By manually adjusting the axis of the half wave plate, the single photons were rotated so as to return them to their original polarisation state. Figure7.5 shows that for incoming vertically polarised light, the fibre caused the state of polarisation of incoming photons to be rotated by almost 90˚ and so initially, the horizontal detector had a higher signal than the vertical detector. This would cause a quantum bit error rate that is too high for a key distribution process. After compensation, the measurements represented the original state of polarisation transmitted by Alice. The vertical signal was at a maximum and the horizontal signal was at a minimum. Obtaining a measurement of zero for the horizontal signal would have been impossible due to the dark count rate of the detectors. Similar results were obtained for a different set of measurements using horizontally polarised light. Figure 7.6 shows that the birefringent effects of the fibre channel rotated the horizontal state of polarisation. The effects were not as strong as the previous measurement, but even this seemingly small difference in the SOP can cause a quantum bit error rate that is too high.

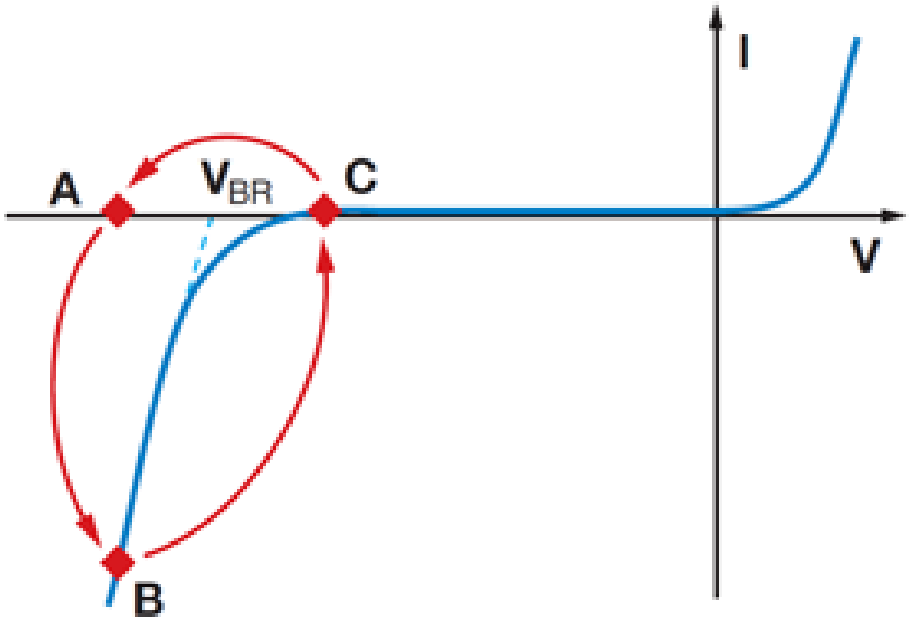


Figure 7.4: A graph showing the reverse bias characteristics of the avalanche photodiode in the single photon detector. The bias voltage of the detector is set at point C which is just below the break down voltage of the semiconductor, V_{BR}. Any increase in the reverse bias voltage will cause a sudden negative increase in the current within the diode of the detector. In this case, the voltage is at point A, bringing the current to point B. This will increase the probability of a detection of an incoming photon. Alternatively, a decrease in the reverse bias voltage will not allow a flow of current in the diode. In this case, the detector will not be able to measure any incoming photons. Image sourced from [88].

After compensation, the horizontal signal is at a maximum and the vertical signal is at a minimum. The half wave plate proved effective in compensating any linear changes in the state of polarisation. However, the fibre optic channel causes three dimensional changes to the SOP of the transmitted photons. Therefore, a half wave plate cannot effectively correct all the changes due to birefringence, as it cannot reverse any changes in the ellipticity of the SOP. This explains why the half wave plate was not able to bring the minimum signals down to the dark count rate. A quarter wave plate is needed in conjunction with the half wave plate in order to correct for changes in the state of polarisation in any direction.

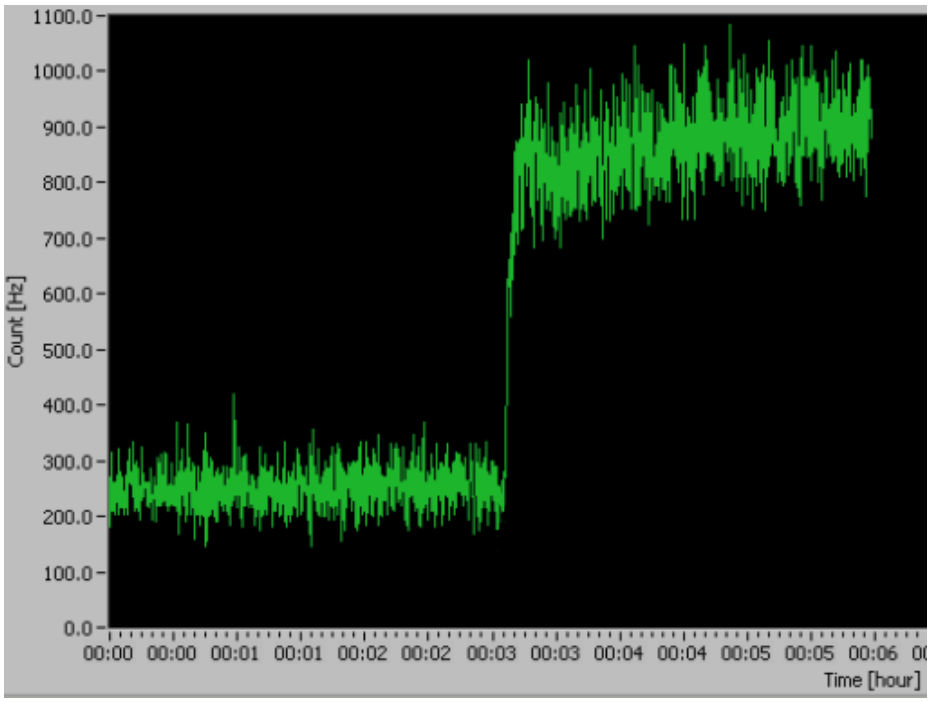
7.2.2. Three Paddle Polarisation Controller

A polarisation controller incorporates both quarter wave plates and half wave plates in order to transform a fixed state of polarisation to any arbitrary state [89]. For a free space system, the polarisation controller consists of a half wave plate between two quarter wave plates, as shown in Figure 7.7a. The first quarter wave plate is used to eliminate any elliptical components of the incoming state of polarisation. This will result in a linear state.

The half wave plate then rotates this linear state by the appropriate angle. The last quarter wave plate transforms this linear state to the required elliptical state. Using this free space polarisation controller will require the laser pulses to be coupled from a fibre channel into free space and back into fibre. This can cause losses in the channel which will affect the quantum bit error rate. The wave plates are also wavelength-sensitive and therefore cannot be used at all telecoms wavelengths. It would be more efficient to have a purely fibre-based polarisation controller. This would minimise losses due to coupling and back-reflection [89].

In order to incorporate this principle into the fibre-based experimental setup, a three paddle polarisation controller was installed as the compensator. The three paddle polarisation controller simulates the three wave plates of the free space controller in a fibre channel, shown in Figure 7.7b. The fibre optic cables are coiled in each of the paddles. The number of coils in each paddle and the diameter of the coils determine the type of wave plate that each paddle represents. Manually rotating each paddle causes stress on the fibre. The stress causes birefringence in the fibre, which rotates the state of polarisation. This device can therefore be used to produce birefringence effects inverse to those caused by the fibre channel. Figure 7.8 shows the results of using a 3 paddle polarisation controller as a compensator. A vertically polarised signal was used for this test. Initially, the vertical signal had been distorted by birefringence such that the horizontal SOP detector had a higher bit rate. After compensation, the vertical signal is returned to a maximum. The signal reaches a bit rate of about 1 kHz which is the expected bit rate at Bob. The measurements show that the bit rate is actually about 1100 Hz. This is due to the programming of the detector. The detector averages the single photons that it measures over a time of 0.2 seconds. Therefore, if the detector measure 1 photon in 0.2 seconds, it will display a bit rate of 5 Hz, regardless of whether it received more photons in that second or not. For this reason, the bit rate of the vertical SOP appears slightly higher than expected. The horizontal signal had been decreased almost to zero. Since the detectors have a non-zero dark count rate, the horizontal signal cannot be measured lower than this value.

a)



b)

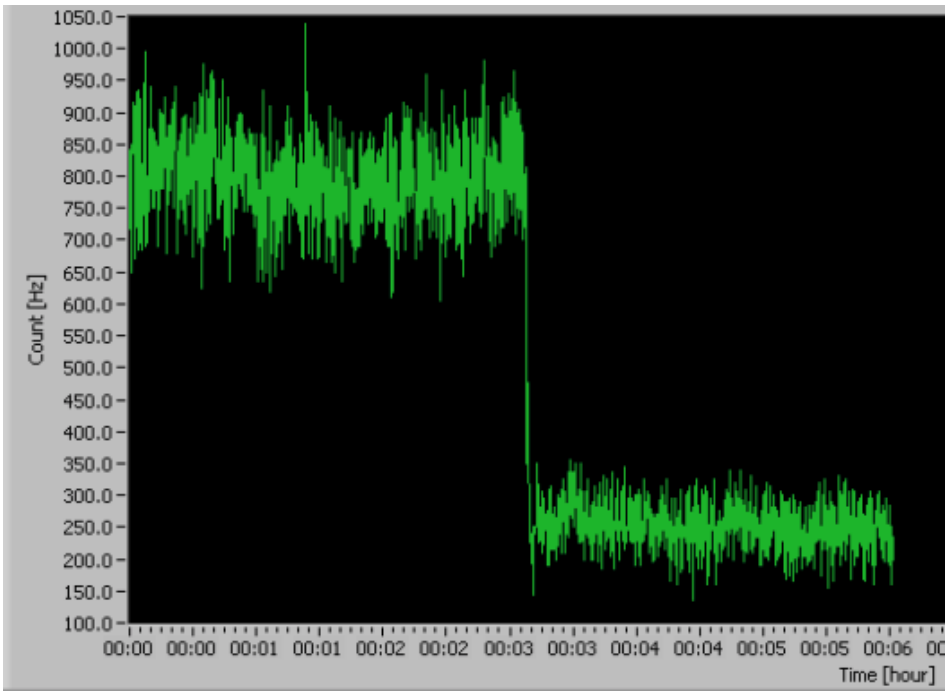
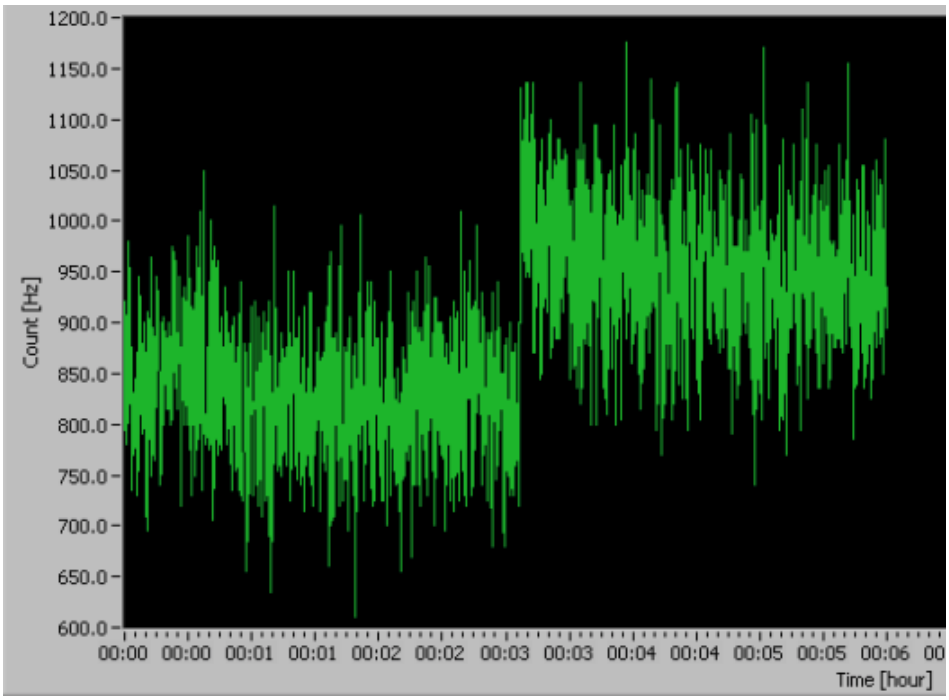


Figure 7.5: Results obtained for incoming vertically polarised photons measured at a) the vertical detector and b) the horizontal detector. This signal has been compensated by a half wave plate. The initial clock rate was set to 100 kHz, but since the mean photon number was set to 0.1 and the detector was operating at an efficiency of 10%, the expected maximum detection rate was 1 kHz. The detection rate occasionally exceeds this value due to the averaging of detection counts per 0.2 sec.

a)



b)

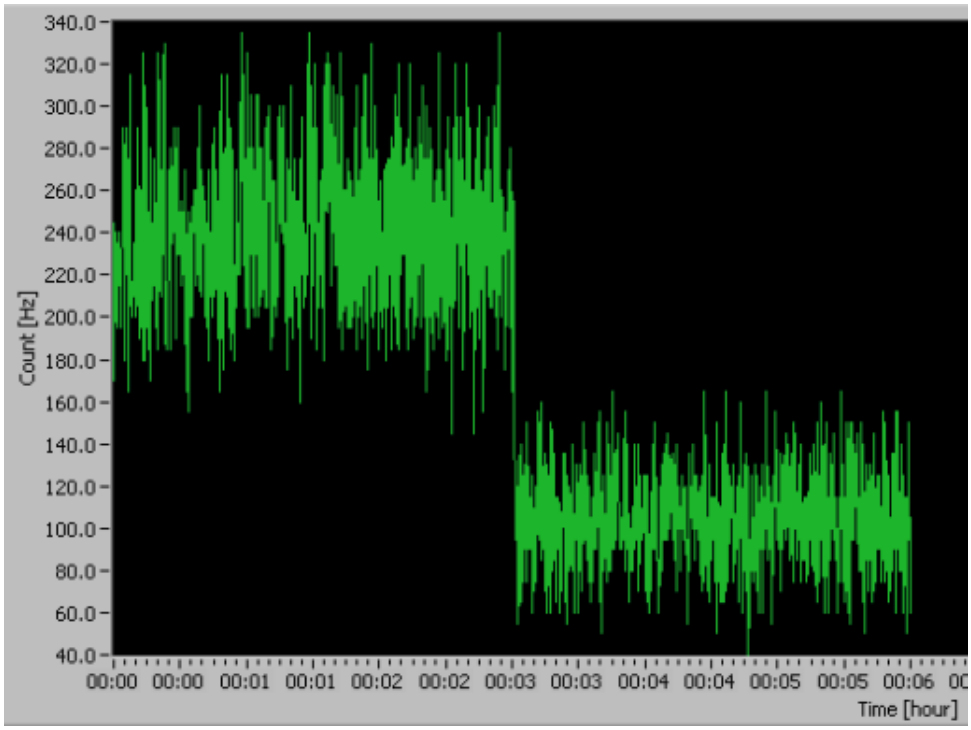


Figure 7.6: Results obtained for incoming horizontally polarised photons, compensated by a half wave plate and measured at a) the horizontal detector and b) the vertical detector.

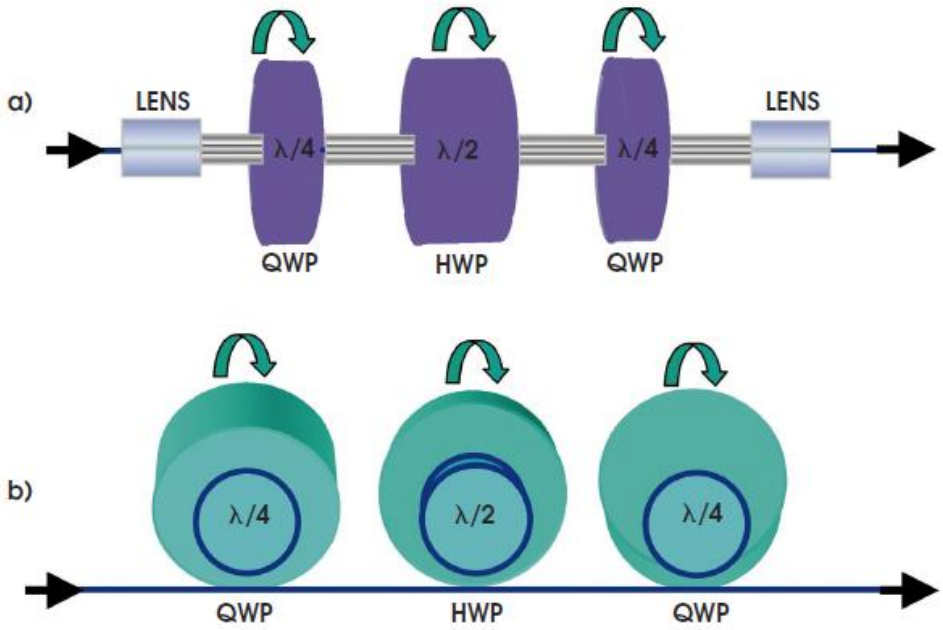


Figure 7.7: The free space polarisation controller is shown in a). It includes two quarter wave plates and a half wave plate in order to rotate an incoming state of polarisation to any desired output. Figure b) shows the fibre counterpart to this polarisation controller. The three paddle controller coils the fibre at specific radii in order to create a controlled birefringence effect on the incoming state of polarisation. Image sourced from [89].

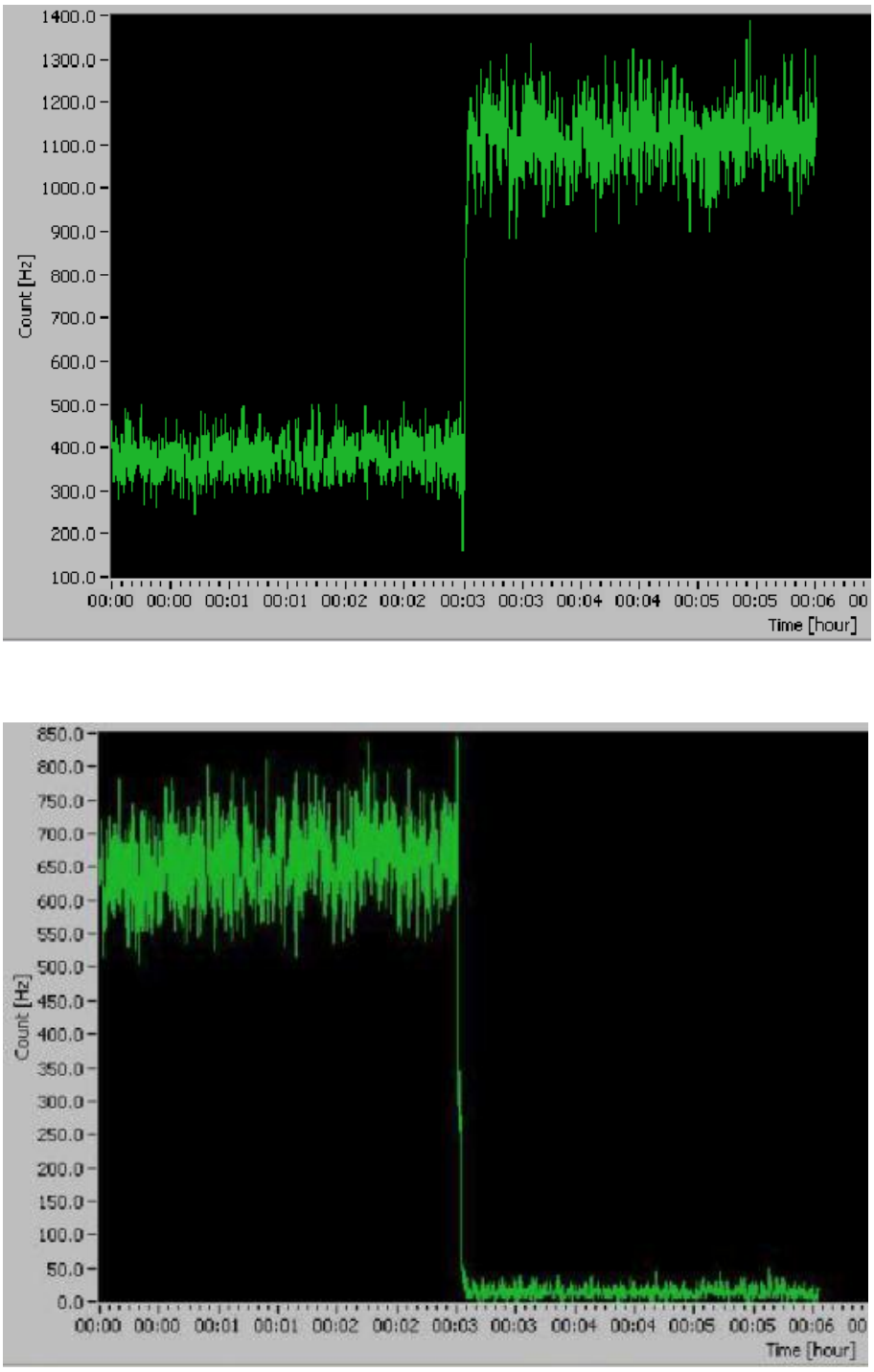


Figure 7.8: Single photon detection rates of a) the vertical SOP signal and b) the horizontal SOP signal. Rotating the initially vertically polarised signal back to its original state, with a three paddle polarisation controller, brings the vertical SOP signal to a maximum and reduces the horizontal SOP signal to a minimum.

7.2.3. The Polarisation Locker

The 3 paddle polarisation controller discussed in the previous section worked well as a manual demonstration for a polarisation compensator. In order to develop a compensator that can be integrated into a commercial QKD system, an automated polarisation controller must be used instead. A polarisation locker (PL100S from Thorlabs) was used as the automated polarisation controller. This device is a fibre-based controller but the technique used to manipulate a state of polarisation is different to that of a 3 paddle controller.

The polarisation locker includes many internal piezoelectric polarisation controllers which are controlled by varying voltages, shown in Figure 7.9. Piezoelectric controllers squeeze the fibre optic cables in order to induce a controlled birefringence. An in-line polarimeter and digital signal processor form an internal feedback loop which drives the piezoelectric controllers to produce deterministic SOP's, as shown in Figure 7.10 [90]. The locker can be pre-programmed so that all output SOP's can be fixed onto a state chose by the user. The internal polarimeter will measure the output SOPs and communicate the adjustments that need to be made to the polarisation controller via the feedback loop. Using this method, the polarisation locker is able to 'lock' onto a specified SOP. Alternatively, the user can manually increment the value of the SOP along a grid superimposed onto the Poincaré sphere to a specific state. Using these functions, the polarisation locker can be used as an automated compensator for the experimental setup.

7.3. Compensating Orthogonal SOP's

The fibre squeezers of the polarisation compensator simultaneously bend the fibre to induce a reverse rotation of the SOP of each photon. A good example of this implementation is found in [67]. It was previously mentioned that this setup used four SOPs however, two polarisation controllers were utilised to compensate these four states. This is because the compensation of one SOP will automatically correct its orthogonal state, since orthogonal SOP's remain orthogonal after a rotation [91]. This can be shown by applying a rotational matrix to the Jones vector of an SOP. As an example, the vertical SOP is used in this calculation, i.e,

$$\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\beta \\ \sin\beta \end{bmatrix}. \tag{7.12}$$

Now the same rotational matrix is applied to the Jones vector of the horizontal SOP

$$\begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -\sin\beta \\ \cos\beta \end{bmatrix}. \tag{7.13}$$

As expected, the rotated SOP's are orthogonal to each other. The above calculation can be adapted to the experiment by applying the Jones matrix of a quarter wave plate to the Jones vector of the vertical SOP

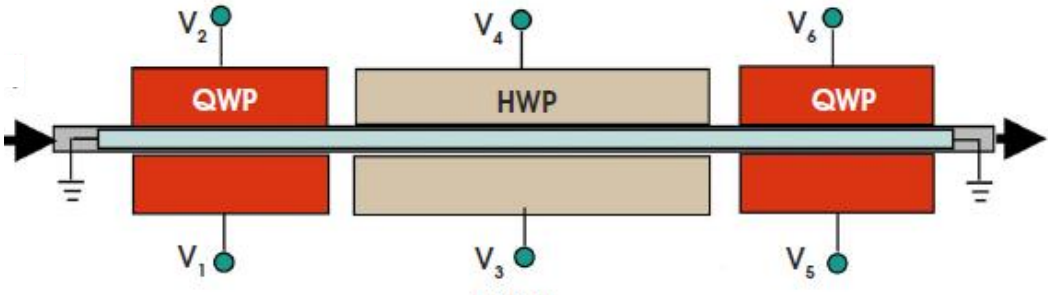


Figure 7.9: A schematic diagram of a piezo-electric polarisation controller. The fibre squeezers are driven by varying voltages in order to manipulate the state of polarisation that is transmitted through the fibre. Image sourced from [89].

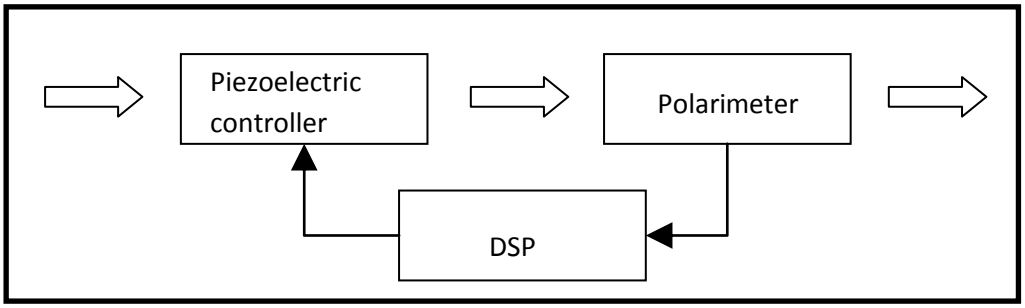


Figure 7.10: A diagram of the internal loop of an SOP locker. The piezoelectric controller is driven by the digital signal processor (DSP) which makes appropriate adjustments to the controller based on the measurements from the in-line polarimeter.

$$e^{i\frac{\pi}{4}}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = e^{i\frac{\pi}{4}}\begin{bmatrix}0\\ -i\end{bmatrix}. \tag{7.14}$$

The same calculation is done with a horizontal SOP

$$e^{i\frac{\pi}{4}}\begin{bmatrix}1 & 0\\ 0 & -i\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = e^{i\frac{\pi}{4}}\begin{bmatrix}1\\ 0\end{bmatrix}. \tag{7.15}$$

The rotated vectors are orthogonal and similar results can be obtained by using other sets of orthogonal SOPs. This shows that when two orthogonal SOPs undergo the same transformation using a phase retarder, the resulting vectors will also be orthogonal. Therefore, if a polarisation controller is set to correct for the vertical SOP, the horizontal SOP will undergo the same changes and will also be compensated. Therefore, only one

polarisation controller is required per basis. This was tested using the three paddle polarisation controller as well as the polarisation locker. Figure 7.11 shows the three paddle polarisation controller used to compensate a vertically polarised signal. The signal was then rotated using a half wave plate such that all linear SOP's were incident on the fibre channel. Figure 7.11 shows that both the vertical and horizontal states are conserved but all states that were nonorthogonal to the rectilinear basis were not compensated. Similar results were obtained for the diagonal basis. The polarisation locker recreated these results. Figure 7.12 shows the compensation of the diagonal basis using the polarisation locker.

7.4. Using One Polarisation Controller to Compensate for Both Bases

In the proposed scheme, shown in Figure 7.13, only one polarisation controller is required. In this case, the polarisation locker is used as the compensator. The locker is used to isolate one point on the Poincaré sphere and fix all incoming light to that SOP. In this setup, the locker is used in a TDM scheme and a test signal is used to achieve the settings for the locker. The quantum signal is periodically stopped to allow the test signal through the quantum channel. The test signal must have only one SOP e.g. vertical. The SOP locker is then used to return the SOP back to vertical after it undergoes changes in the quantum channel. This would compensate the horizontal SOP as well. Since only one SOP locker is used in this setup, the locker must also compensate the diagonal SOP's. This can only be done if the locker is used to isolate the plane on the Poincaré sphere that passes through all four SOP's being used in the QKD transmission. A step search must be used on the locker to correctly identify the plane on which all four SOPs exist. Usually, the locker fixes on one point on the Poincaré sphere, but this point can lie on any plane. If the plane is specified as the equatorial plane of the sphere, all four SOPs will be correctly compensated, thus allowing for polarisation compensation with just one polarisation controller. This method has been implemented manually and the results are shown in Figure 7.15.

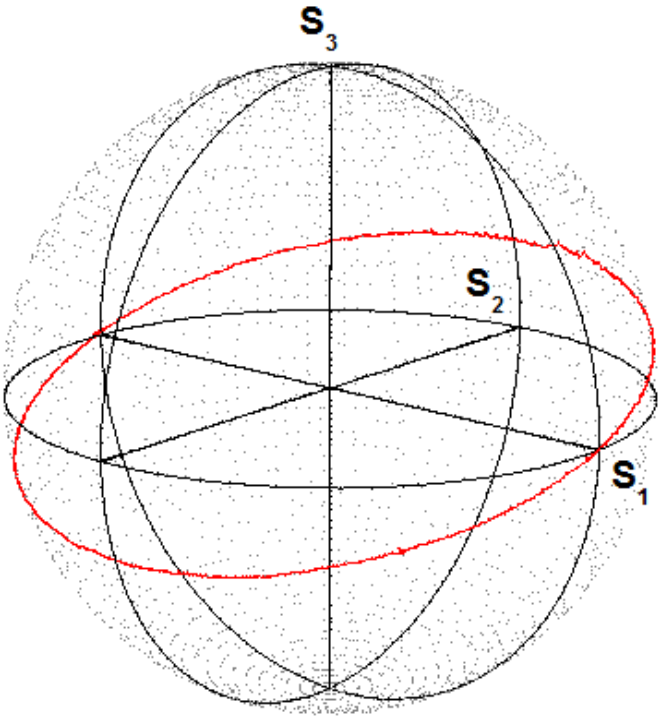


Figure 7.11: These results show that both the vertical and horizontal SOP's were returned to their original states, even though only the vertical SOP was compensated using the three paddle polarisation controller. Explain black and red lines

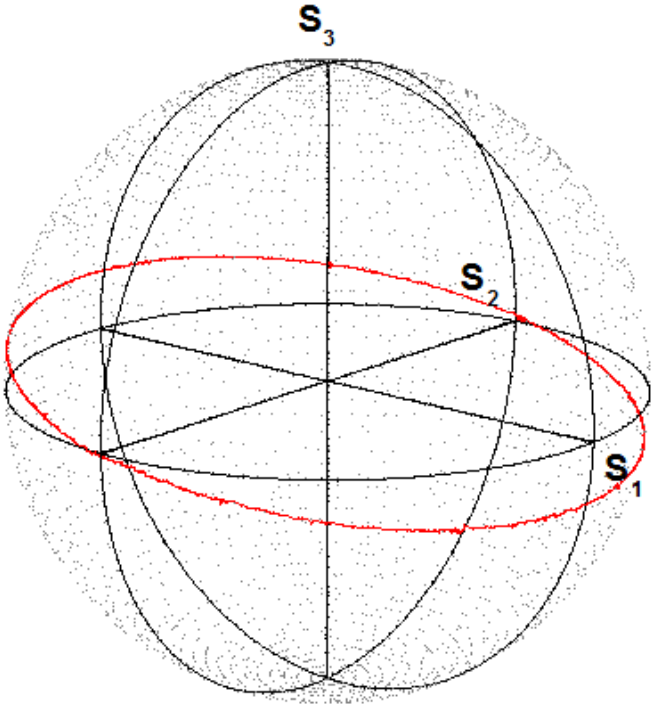


Figure 7.12: The polarisation locker was used to demonstrate the compensation of the diagonal SOP's.

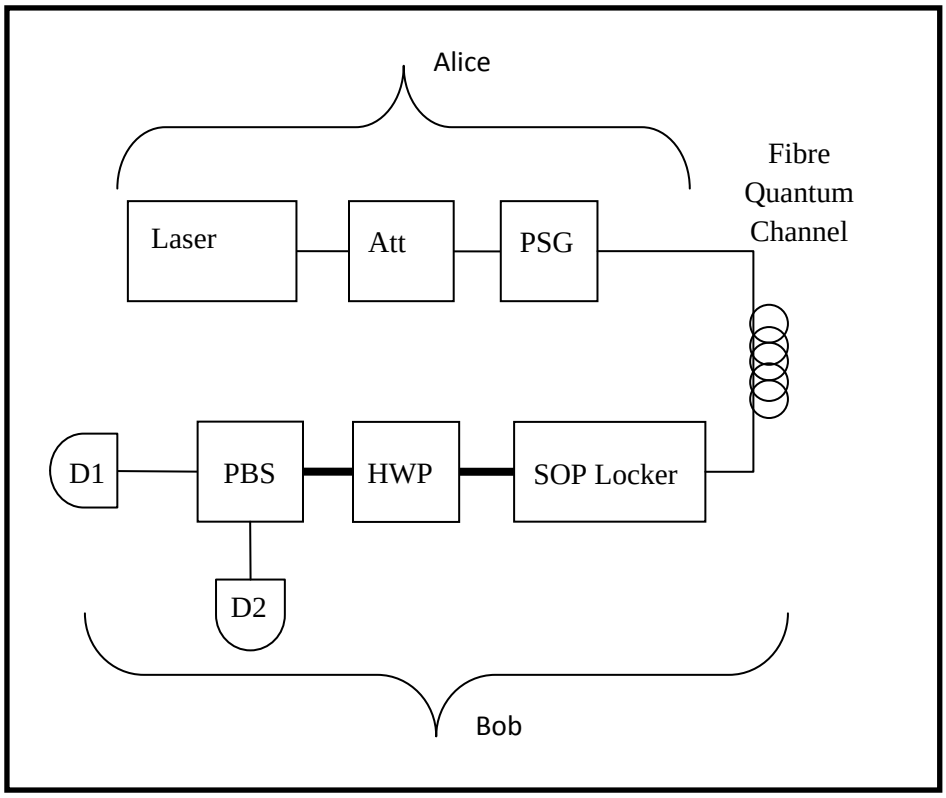
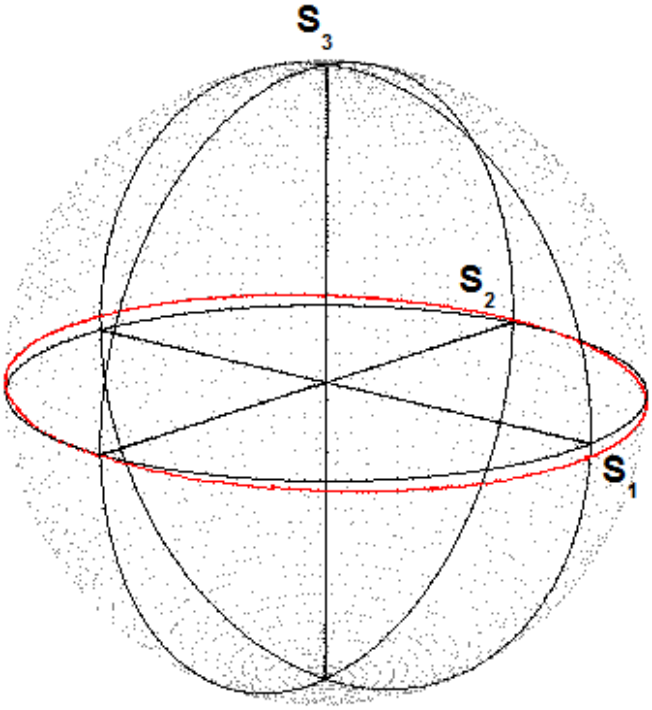


Figure 7.13: The proposed setup for a polarisation encoded QKD scheme. The laser pulses are first passed through an optical attenuator (Att) which creates pseudo-single photons. Each photon is then assigned an SOP with the polarisation state generator (PSG) and is transmitted through the quantum channel to the receiver. The receiver then uses the SOP locker to compensate for changes in polarisation. A half wave plate (HWP) is used to select the basis in which the receiver will measure each photon and finally, the photons are separated at a polarisation beam splitter (PBS) to be measured at one of two detectors. The bold lines in the diagram indicate polarisation maintaining fibre.

a)



b)

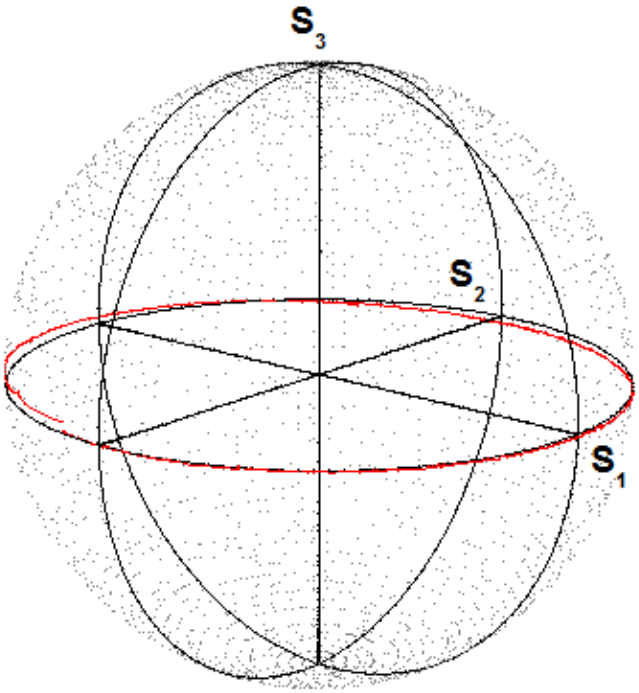


Figure 7.15: The equatorial plane of the Poincaré sphere was isolated using a) the three paddle polarisation controller and b) the polarisation locker.

7.5. Analysis

The polarisation locker proved effective in reversing the birefringence effects of the fibre channel. The measurements shown in Figure 7.15 indicate that the polarisation locker can easily be used to minimise the circular component of the SOP of any incoming light as well as rotate the SOP linearly so that it returns to its original state. The locker is therefore able to passively compensate all four SOP's simultaneously. Since the polarisation locker is able to lock onto any plane on the Poincaré sphere, the same method can be used to compensate the rectilinear and circular bases as well.

The range of the angle of inclination obtained from the above measurements ranges from -0.89° to 1.69°. Using Malus' Law, the error rate due to the polarisation locker was maintained below 0.1%. Ideally, the contribution of the apparatus to the QBER should be minimal, however, this is sometimes impractical. As previously mentioned, the angle of inclination may deviate by 5.74° if an error of 1% may be allowed. The maximum deviation of the ellipticity of the SOP may therefore be set according to the expected QBER of the entire system.

7.6. Future work

In order for the polarisation compensator to be integrated into a commercial QKD prototype, it must be a fully automated device. The polarisation locker can be programmed to search for the appropriate setting for compensation automatically. The correct setting can be obtained by employing a step search along a grid superimposed on the Poincaré sphere. The search algorithm must make a measurement of the rotation of all linear SOP's and make adjustments to the SOP locker in order to minimise the ellipticity of the incident SOP's. This will ensure that the equatorial plane of the Poincaré sphere has been isolated. The states must then be rotated linearly, using a half wave plate in order to return each SOP to it's original state.

Conclusion

The simple encoding and decoding methods of polarisation encoded QKD provides a feasible implementation for a QKD system. This is now achievable in fibre. Traditionally, polarisation encoding was only achievable for a free space channel but through active compensation techniques, it provides a promising approach for future systems.

By actively scanning and compensating the birefringence effects of the fibre channel, a simple, one-way QKD implementation can be achieved. This allows for the interchange of quantum signals between fibre and free space channels. This is imperative for the use of one common encoding in a meshed network. Creating an untrusted interface between fibre and free space communication channels, allows for the realisation of a global QKD network.

The active polarisation technique uses an automated polarisation controller to reverse any rotations caused by the fibre channel. Most compensation techniques rely on two compensators, each rectifying one of the non-orthogonal bases used for the key exchange process. This is done by compensating one of the SOP's of each basis, thereby simultaneously compensating its orthogonal SOP. The proposed system uses one compensator to isolate the plane on the Poincaré sphere that passes through all the states of polarisation that are required for the respective QKD protocol. Instead of identifying and translating a single point along the Poincaré sphere, this system identifies the randomised rotation of the plane of linear states and returns these states to the equatorial plane. The use of one polarisation controller allows for a more cost effective alternative to polarisation compensation.

The system presented in this dissertation requires further automation in order to be implemented in a polarisation encoded QKD system. The current, manual step search can be automated in order to streamline the isolation of the correct setting for the polarisation controller. The contribution towards the QBER by this compensation system can be quantified and hence, minimised by refining the precision of the step search. The birefringence effects can therefore be effectively controlled, thus allowing a realisation of polarisation encoded QKD in fibre.

References

1. Dupuy, P.J., Available online from: http://hiwaay.net/~paul/cryptology/history.html.
2. Stallings, W., Available online from: http://williamstallings.com/Extras/Security-Notes/lectures/classical.html.
3. Singh, S., *The Code Book: The secret history of codes and code breaking,* 2010: Fourth Estate. p. 17.
4. Ferguson, N. and Schneier, B., *Practical Cryptography* 2003: John Wiley & Sons Inc. p. 207-222.
5. Microsoft. *Cryptography Concepts*. Available online from: http://msdn.microsoft.com/en-us/library/aa380247(VS.85).
6. Schneier, B., *Applied Cryptography,* 2007: John Wiley & Sons. p. 1.
7. Mollin, R., *An Introduction to Cryptography*. Second edition, 2007, USA: Chapman & Hall CRC. p. 172-180.
8. Konheim, A., *Cryptography: A Primer* 1981: John Wiley & Sons Inc.
9. Shannon, C., *Communication Theory of Secrecy Systems.* Bell System Technical Journal, 1949. **28**: p. 656–715.
10. Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., *Quantum Cryptography.* Review of Modern Physics, 2002. **74**: p. 145-195.
11. Wiesner, S., *Conjugate Coding.* ACM SIGNAT News, 1983. **15**(1): p. 78-88.
12. Bennett, C.H. and Brassard, G.,*Quantum Cryptography: Public Key Distribution and Coin Tossing*. Proceedings of *IEEE International Conference on Computers, Systems and Signal Processing*. 1984. Bangalore, India.
13. Nielsen, M.A. and Chuang, I. L., *Quantum Information Processing and Communication,* 2002, United Kingdom: Cambridge University Press.
14. Wooters, W.K. and Zureck, W.H., *A Single Quantum Cannot Be Cloned.* Nature, 1982. **299**: p. 802 - 803.
15. Zettili, N., *Quantum mechanics: concepts and applications,* 2009: John Wiley & Sons Inc. p. 28.
16. Renner, R., *Security of Quantum Key Distribution.* International Journal of Quantum Information, 2008. **6**(01): p. 1-127.
17. SECOQC. *Quantum Cryptography: An Innovation in the Domain of Secure Information Transmission, White Paper*. Available online from: www.secoqc.net.
18. Bennett, C.H., *Quantum Cryptography using Any Two Nonorthogonal States.* Physical Review Letters, 1992. **68**(21): p. 3121-3124.
19. Scarani, V., *Quantum Physics: A First Encounter: Interference, Entanglement, and Reality,* 2006, Oxford UK: Oxford University Press. p. 67-80.
20. Ekert, A., *Quantum cryptography based on Bell's theorem.* Physical Review Letters, 1991. **67**(6): p. 661-663.
21. Mirza, A., *Towards Practical Quantum Cryptography*, MSc thesis in *Physics*2009, University of KwaZulu-Natal: Durban.

22. Scarani, V., Acin, A., Ribordy, G. and Gisin, N., *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations.* Physical Review Letters, 2004. **92**(5): 57901.
23. Hughes, R.J., Buttler, W. T., Kwiat, P.G., Lamoreaux, S. K., Morgan, G. L., Nordholt, J. E., and Peterson, C. G., *Free-space Quantum Key Distribution in Daylight.* Journal of Modern Optics, 2000. **47**(2/3): p. 549 - 562.
24. Jeong, Y., Kim, Y. and Kim, Y. *Weak-pulse Implementation of B92 Quantum Cryptography Protocol in Free-space*. Available online from: qopt.postech.ac.kr/publications/B92_ver3.pdf.
25. Lucamarini, M. and Mancini, S., *Secure Deterministic Communication Without Entanglement.* Physical Review Letters, 2005. **94**(14): 140501.
26. IdQuantique, *Winter School on Practical Quantum Cryptography.* 2011.
27. Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. and Sanpera, A., *Quantum privacy amplification and the security of quantum cryptography over noisy channels.* Physical Review Letters. **77**(13): p. 2818-2821.
28. Brassard, G., Lutkenhaus, N., Mor, T. and Sanders, B. C., *Limitations on Practical Quantum Cryptography.* Physical Review Letters, 2000. **85**(6): p. 1330-1333.
29. Curty, M. and Lutkenhaus, N., *Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses.* Physical Review A, 2005. **71**(6): 062301.
30. Hwang, W., *Quantum key distribution with high loss: Toward global secure communication.* Physical Review Letters, 2003. **91**(5): 57901.
31. Vakhitov, A., Makarov, V. and Hjelme, D. R., *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography.* Journal of Modern Optics, 2001. **48**(13): p. 2023-2038.
32. Wiechers, C., Lydersen, L., Wittmann, C., Elser, D., Skaar, J., Marquardt, Ch., Makarov, V. and Leuchs, G., *After-gate attack on a quantum cryptosystem.* New Journal of Physics, 2011. **13**(1): 013043.
33. Makarov, V., *Quantum cryptography and quantum cryptanalysis*, PhD thesis in *Department of Electronics and Telecommunications,* 2007, Norwegian University of Science and Technology: Trondheim.
34. Muller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H. and Gisin, N., *Plug and play systems for quantum cryptography.* Applied Physics Letters, 1996. **70**(7): p. 793-795.
35. Xavier, G.B., Walenta, N., Vilela de faria, G., Temporao, G. P., Gisin, N., Zbinden, H. and vin der Weid, J. P., *Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation.* New Journal of Physics. **11**(4): 045015.
36. Elliott, C., *The DARPA quantum network*. Quantum Communications and Cryptography, ed. A. Sergienko, 2005, Boca Raton London: CRC Press/Taylor and Francis. p. 83-102.
37. Poppe, A., M. Peev, and O. Maurhart, *Outline of the SECOQC quantum-key-distribution network in Vienna.* International Journal of Quantum Information, 2008. **6**(02): p. 209-218.
38. Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z. and Tanaka, A., *Field test of quantum key distribution in the Tokyo QKD Network.* Optics Express, 2011. **19**(11): p. 10387-10409.

39. Stucki, D., Legré, M., Buntschu, F. and B. Clausen, Felber, N., Gisin, N., Henzen, L., Junod, P., Litzistorf, G., Monbaron, P., *Long-term performance of the SwissQuantum quantum key distribution network in a field environment.* New Journal of Physics, 2011. **13**(12): 123001.
40. Mirza, A. and F. Petruccione, *Realizing long-term quantum cryptography.* JOSA B, 2010. **27**(6): p. A185-A188.
41. Mirza, A. and F. Petruccione. *Recent Findings from the Quantum Network in Durban*, in *QCMC 2010*. Editors: Ralph, T. and Lam, P. K., 2010. American Institute of Physics: Brisbane, Australia. p. 35-38.
42. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., *Experimental quantum cryptography.* Journal of Cryptography, 1992. **5**(1): p. 3-28.
43. Hecht, J. and Long, L., *Understanding Fibre Optics*. 4th edition. Vol. 3. 2002: Columbus: Prentice-Hall.
44. Kingfisher. *Application Notes*. Available online from: www.kingfisherfiber.com.
45. Hubel, H., Vanner, M. R., Lederer, T., Blauensteiner, B., Lorunser, T., Poppe, A. and Zeilinger, A., *High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fibre.* Optics Express, 2007. **15**(12): p. 7853-7862.
46. Hughes, R.J., Morgan, G. L. amd Peterson, C. G., *Quantum key distribution over a 48 km optical fibre network.* Journal of Modern Optics, 2000. **47**(2/3): p. 533-547.
47. Eraerds, P., Walenta, N., Legre, M., Gisin, N. and Zbinden, H., *Quantum key distribution and 1 Gbit/s data encryption over a single fibre.* New Journal of Physics, 2009. **12**(6): 063027.
48. Ramaswami, R. and K. Sivarajan, *Optical Networks: A Practical Perspective*. Second ed2002, San Francisco, CA, USA: Morgan Kaufmann Publishers.
49. Stucki, D., Walenta, N., Vannel, F., Thew, R. T., Gisin, N., Zbinden, H., Gray, S., Towery, C. R. and Ten, S., *High Rate, Long-distance Quantum Key Distribution over 250 km of Ultra Low Loss Fibres.* New Journal of Physics, 2009. **11:** 075003.
50. Beals, T.R., *Quantum communication and information processing*, 2008, PhD Thesis, University of California, Berkley.
51. Tang, X., Ma, L., Mink, A., Nakassis, A., Hershman, B., Bienfang, J., Boisvert, R. F., Clark, C. and Williams, C. *High Speed Fiber-based Quantum Key Distribution Using Polarization Encoding*. Proceedings of *SPIE 5893, Quantum Communications and Quantum Imaging III*. 2005.
52. Gisin, N., Passy, R., Perny, B., Galtarossa, C., Someda, F., Bergamin, M. and Matera, F., *Experimental comparison between two different methods for measuring polarisation mode dispersion in single mode fibres.* Electronics Letters, 1991. **27**(24): p. 2292-2294.
53. Xavier, G.B., Vilela de Faria, G., Temporao, G. P. and von der Weid, J. P., *Full polarization control for fiber optical quantum communication systems using polarization encoding.* Optics Express, 2008. **16**(3): p. 1867-1873.
54. Patel, K.A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V. and Shields, A. J., *Coexistence of high-bit-rate quantum key distribution and data on optical fiber.* Physical Review X, 2012. **2**(4): 041010.
55. Bonato, C., Tomaello, A., Da Deppo, V., Naletto, G., Villoresi, P., *Feasibility of satellite quantum key distribution.* New Journal of Physics, 2009. **11**(4): 045017.

56. Pfennigbauer, M., Leeb, W. R., Aspelmeyer, M., Jennewein, T and Zeilinger, A. *Free-Space Optical Quantum Key Distribution Using Intersatellite Links*. in *CNES - Intersatellite Link Workshop*. 2003.
57. Capraro, I., *Advanced Techniques in Free Space Quantum Communication*, 2008, Phd Thesis, University of Padua.
58. eoportal. Available online from: https://directory.eoportal.org/web/eoportal/satellite-missions/t/terrasar-x.
59. idQuantique. *Understanding Quantum Cryptography*. Available online from: http://www.idquantique.com/images/stories/PDF/clavis2-quantum-keydistribution/clavis2-whitepaper.pdf.
60. Schmitt-Manderbach, T., Weier, H., Furst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A. and Weinfurter, H., *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution Over 144 km.* Physical Review Letters, 2007. **98**(1): 10504.
61. Fickler, R., Lapkiewicz, R, Plick, W. N., Krenn, M., Schaeff, C., Ramelow, S. and Zeilinger, A., *Quantum Entanglement of High Angular Momenta.* Science, 2012. **338**(6107): p. 640-643.
62. Hecht, E., *Optics*2001, Reading MA: Addison-Wesley. p. 325-379.
63. EXFO. *Application Note - Polarization Mode Dispersion*. Available online from: documents.exfo.com/appnotes/anote047-ang.pdf.
64. OZ Optics. *Application Note - Polarization Measurements*. 1999; Available online from: www.ozoptics.com/ALLNEW_PDF/APN0005.pdf.
65. Breguet, J., Muller, A. and Gisin, N., *Quantum Cryptography with Polarized Photons in Optical Fibres.* Journal of Modern Optics, 1994. **41**(12): p. 2405-2412.
66. Chen, J., Wu, G., Xu, L., Gu, X., Wu, E. and Zeng, H., *Stable quantum key distribution with active polarisation control based on time-division multiplexing.* New Journal of Physics, 2009. **11**(6): 065004.
67. Wu, G., Chen, J., Li, Y. and Zeng, H. *Stable polarization-encoded quantum key distribution in fibre*. Available online from: arxiv.org/pdf/quant-ph/0606108.
68. Liu, W., Wu, W., Liang, L., Li, C. and Yuan, J., *Polarization Encoded Quantum Key Distribution over Special Optical Fibres.* Chinese Phys. Lett, 2006. **23**(2): 287.
69. Ma, L., Xu, H. and Tang, X., *Polarization recovery and auto-compensation in Quantum Key Distribution network.* National Inst of Standards and Technology Gaithersburg MD, 2006.
70. Tang, X., Ma, L., Mink, A., Nakassis, A., Xu, H., Hershman, B., Bienfang, J., Su, D., Boisvert, R. F., Clark, C., and Williams, C., *Experimental study of high speed polarization coding quantum key distribution with sifted-key rates over Mbit/s.* National Inst of Standards and Technology Gaithersburg MD, 2006.
71. Tang, X., Ma, L., Mink, A., Nakassis, A., Xu, H., Hershman, B., Bienfang, J., Su, D., Boisvert, R. F., Clark, C. and Williams, C. *Quantum Key Distribution system operating at sifted key-rate over Mbit/s*. Proceedings of *SPIE 6244, Defense and Security 06*. 2006.
72. Mink, A., Bienfang, J., Carpenter, R., Ma, L., Hershman, B., Restell, A. amd Tang, X, *Programmable instrumentation and gigahertz signalling fo single-photon quantum communication systems.* New Journal of Physics, 2009. **11**(4): 045016.
73. Xu, H., Ma, L., Mink, A., Hershman, B. and Tang, X., *1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm.* Optics Express, 2007. **15**(12): p. 7247-7260.

74. Ma, L., Chang, T., Mink, A., Slattery, O., Hershman, B. and Tang, X., *Experimental Demonstration of a Detection-Time-Bin-Shift Polarization Enconding Quantum Key Distribution System.* IEEE Communications Letters, 2008. **12**(6) p. 459-461.
75. Vilela de Faria, G., Xavier, G. B.,Temporo, G. P., Zbinden, H., Gisin, N. and von der Weid, J. P., *Practical Scheme for Fibre-optical QKD with Polarization Encoded Qubits using Real-time Polarization Control.*, Available online from: http://www.secoq.net/downloads/abstracts/SECOQC-vonderWeid.pdf.
76. Avella, A., Brida, G., Degiovanni, I. P., Genovese, M., Gramegna, M. and Traina, P., *Experimental quantum-cryptography scheme based on orthogonal states.* Physical Review A, 2010. **82**(6): 062309.
77. Goldenberg, L. and Vaidman, L., *Quantum Cryptography based on orthogonal states.* Physical Review Letters, 1995. **75**(7): p. 1239-1243.
78. Singh, S.P and Singh, N., *Nonlinear effects in optical fibers: Origin, management and applications.* PIER, 2007. **73**: p. 249-275.
79. Hu, Y., Peng, X., Li, T. and Guo, H., *On the Poissonian approximation to photon distribution for faint lasers.* Physics Letters A, 2007. **367**(3): p. 173-176.
80. Thorlabs. *Fixed optical attenuators*. Available online from: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=1385.
81. Yao, X.S., Yan, L. and Shi, Y., *Highly repeatable all-solid-state polarization-state generator.* Optics Letters, 2005. **30**(11): p. 1324-1326.
82. idQuantique. *id200 Series*. 2009; Available online from: www.idquantique.com/scientific-instrumentation/id201-ingaas-apd-single-photon-detector.html.
83. General Photonics, *Data Sheet - PSG-001.*
84. Castelletto, S.A., Degiovanni, I. P., Schettini, V. and Migdall, A. L., *Reduced Deadtime and Higher Rate Photon-Counting Detection using a Multiplexed Detector Array.* Journal of Modern Optics, 2007. **54**(2/3): p. 337-352.
85. Buller, G.S., Warburton, R. E., Pellegrini, S., Ng, J. S., David, J. P. R., Tan, L. J. J., Krysa, A. B. and Cova, S. *InGaAs/InP Single-Photon Avalanche Diode Detectors for Quantum Key Distribution*. 2008; Available online from: www.secoqc.net/downloads/abstracts/SECOQC-Buller.pdf.
86. idQuantique. *id400 Datasheet*. Available online from: http://www.idquantique.com/products/˜les/id400_specs.pdf.
87. Jiang, X., Itzler, M. A., Ben-Michael, R. and Slomkowski, K., *InGaAs/InP Single-Photon Avalanche Diode Detectors for Quantum Key Distribution.* IEEE Journal of Selected Topics in Quantum Electronics, 2007. **13**(4): p. 895-905.
88. Thorlabs. *Operating principle of Single Photon Counters*. Available online from: www.thorlabs.com/newgroupPage9.cfm?objectgroup_id=5255.
89. Yao, S., *Polarization in Fiber Systems: Squeezing out More Bandwidth*. The Photonics Handbook, 2003: Laurin Publishing.
90. Thorlabs. *Benchtop state of polarization locker*. Available online from: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=1769.
91. Wolfram Mathworld, *Rotation Matrix*. Available online from: mathworld.wolfram.com/RotationMatrix.html.