The Development of a Low-cost, Handheld Quantum Key Distribution Device

by

Sharmini Pillay

A thesis submitted in fulfilment of the academic
requirements for the degree of
Doctor of Philosophy
in the School of Chemistry and Physics,
College of Science, Engineering and Agriculture,
University of KwaZulu-Natal
Durban

Supervisor: Prof. Francesco Petruccione

Co-Supervisor: Dr. Marco Mariola

December 2017

ABSTRACT

Quantum Key Distribution (QKD) is an emerging field of information security. To date, this technology has been implemented for large scale financial and voting purposes, but QKD is a versatile solution which can also be utilised to secure personal transactions. The development of low cost, portable QKD devices can further promote the use of quantum encryption in commercial security systems. Research has been done to design hand-held QKD devices for personal use with ATMs. These devices use a short-range free space channel to produce a secret key using the polarisation of single photons as qubits. Free space applications of QKD usually utilise polarisation encoding of single photons since the polarisation states do not deteriorate in the turbulent atmosphere. Recent research also shows the feasibility of using quantum coherent states with continuous variable QKD in free space.

The proposed device uses the Coherent One Way (COW) protocol to exchange a secret key between the two authenticated parties. The COW protocol is a simple, practical protocol which uses the time of arrival of consecutive weak coherent pulses as the bit encoding. The security of this protocol lies in preserving the coherence between consecutive laser pulses. Should decoherence be observed in the monitoring line, the presence of an eavesdropper is inferred.

An advantage of using the COW protocol is the small size and low cost of the setup. This is ideal for a hand-held device used for short-range QKD. The COW protocol is not traditionally used for a free space channel due to the fragility of coherence in a turbulent medium. Since this is a short-range device which will not encounter any turbulence, the coherence of the laser beam is not compromised. It is therefore suitable to use the COW protocol under these conditions.

We present in this thesis, the design of the system, in particular, the conversion from a fibre channel to a free space channel. A low cost optical synchronisation system is presented for use in a laboratory environment and the system is characterised with respect to the efficiency of the source, synchronisation and detection components. The bit generation rate and quantum bit error rate of the system are measured and discussed.

Synchronisation techniques for long range free space implementation of the COW protocol, using radio transmission, are presented with a simulation. The simulation is used to demonstrate the compensation for Doppler effects required for communication between a Low Earth Orbit satellite and a ground station.

PREFACE

The experimental work described in this thesis was carried out at the University of KwaZulu-Natal, School of Chemistry and Physics, Westville, Durban, from May 2013 to December 2017, under the supervision of Professor Francesco Petruccione and co-supervision of Dr. Marco Mariola. 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.

Signed:_____Sharmini Pillay

On this 15th day of December 2017

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

Signed:_____ Prof Francesco Petruccione

On this 15th day of December 2017

Signed:_____ Dr. Marco Mariola

On this 15th day of December 2017

DECLARATION 1 - PLAGIARISM

I, Sharmini Pillay, declare that

1. The research reported in this thesis, except where otherwise indicated, is my original research.
2. This thesis has not been submitted for any degree or examination at any other university.
3. This thesis does not contain other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.
4. This thesis 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 thesis 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 PUBLICATION

Publication 1 - Published

Sharmini Pillay, Abdul R. Mirza, Timothy B. Gibbon and Francesco Petruccione, Compensating Birefringence Effects in Optical Fibre for Polarisation Encoded QKD. in Proceedings of SAIP2012, the 57th Annual Conference of the South African Institute of Physics. pp. 288 - 292. (Published in 2014)

Sharmini Pillay was the principal researcher, conducted the findings and authored the paper. Abdul Mirza, Timothy Gibbon and Francesco Petruccione supervised the research and edited the publication.

Publication 2 - Published

Sharmini Pillay, Abdul R. Mirza and Francesco Petruccione, Towards polarisation-encoded quantum key distribution in optical fibre networks. South African Journal of Science. 2015;111(7/8), Art. #2013-0380.

Sharmini Pillay was the principal researcher, conducted the findings and authored the paper. Abdul Mirza, and Francesco Petruccione supervised the research and edited the publication.

Publication 3- Published

Sharmini Pillay, Marco Mariola, Abdul R. Mirza, Francesco Petruccione, Handheld QKD Device Using the COW Protocol. in Proceedings of SAIP2015 (Addendum), the 60th Annual Conference of the South African Institute of Physics, pp 21-26. (Published in 2016)

Sharmini Pillay was the principal researcher, conducted the findings and authored the paper. Marco Mariola was the co-researcher and edited the publication. Abdul Mirza and Francesco Petruccione supervised the research and edited the publication.

Publication 4- Submitted

Sharmini Pillay, Marco Mariola, Francesco Petruccione, An Investigation of Synchronisation Techniques for a Handheld QKD Device. in Proceedings of SAIP2017, the 62nd Annual Conference of the South African Institute of Physics.

Sharmini Pillay was the principal researcher, conducted the findings and authored the paper. Marco Mariola and Francesco Petruccione supervised the research and edited the publication.

Presentations

The following is a list of conference/workshop presentations given during the period of my research:

Orals

Portable QKD Device using the COW Protocol, QIPCC 2014 conference, Alpine Heath Resort, Drakensberg, 3 – 7 November 2014.

Portable QKD Device Using the COW Protocol, SAIP Conference 2015, Boardwalk Convention Centre, Port Elizabeth, 28 June – 3 July 2015.

Posters

Polarisation Encoded QKD in Fibre, QIPC International Conference, Florence, 30 June – 5 July 2013.

Hybrid Two-way QKD in Free Space, SAIP Conference 2013, University of Zululand, 8 July – 12 July 2013.

Quantum Key Distribution in Free Space, South African Society for Atmospheric Sciences (Sasas) Conference, 26 – 27 September 2013, Salt Rock.

Hybrid Two-way QKD in Free Space, Postgraduate Research Day 2013, Hosted by the College of Agriculture, Engineering and Science, UKZN, 1 November 2013.

Portable QKD device using the COW protocol, QCrypt 2014 conference, Paris, 1 – 5 September 2014.

Portable QKD device using the COW protocol, Postgraduate Research Day 2014, Hosted by the College of Agriculture, Engineering and Science, UKZN, 27 October 2014.

Other Conferences Attended

QIPCC, 25 – 29 November 2013, Pumula Beach Hotel

Schools Attended

Entrepreneurship workshop hosted by IOP 20 – 24 May 2013

Media Publication

How quantum physics is opening new frontiers for data safety, The Conversation – Africa edition. Available online: https://theconversation.com/how-quantum-physics-is-opening-new-frontiers-for-data-safety-45550

Name: Sharmini Pillay

Signed: .....

Sri Gurubhyo Namaha

A salutation to all my teachers, past and present.

ACKNOWLEDGEMENT

I thank my supervisor, Prof. Francesco Petruccione, for his guidance, motivation and immense support throughout this project and his mentorship since the beginning of my postgraduate studies. I thank my co-supervisor Dr. Marco Mariola for allowing me to be part of the Africhino group. I have learnt so much from joining his lab and I am so grateful for the dedicated mentorship he has given me. I thank both my supervisors for the opportunities to learn and grow as a student.

I thank Dr. Abdul R. Mirza for his tireless assistance and mentorship at the commencement of this project and since the beginning of my postgraduate studies. I thank Dr. Yaseera Ismail for her assistance and guidance for this project and for editing this thesis. I thank Prof. Mark Tame for his guidance and helpful discussions about this project. I am grateful to all my teachers and lecturers at UKZN since my undergraduate studies. Without their guidance throughout my studies, I would not have discovered my passion for physics. I especially thank Prof. John Hey for inspiring my interest in experimental physics.

I thank my colleagues and friends at UKZN, Kreason Naidoo, Jason Francis, Stuti Joshi, Maria Schuld, Betony Adams and Sanele Dlamini for supporting me and being my go-to people. I appreciate each of them for all that they have done.

I am eternally grateful to my parents, Dixen and Salo Pillay, for their support and love, and to my sister, Priyoshni, for helping me stay grounded during stressful times. I thank my family and Sai family for their encouragement and belief in me. I will forever be thankful to Reginal Abdul. I could never measure the support that he has given me and I am grateful for everything that he does. I thank my best friend, Dr. Dunesha Naicker, for being so supportive and encouraging in all my endeavours.

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.

Contents

List of Figures

List of Tables

1 Introduction

Cryptography is an evolving field of study which has been developed since ancient times and is still relevent, more than ever, today. One of the earliest recorded uses of a cryptosystem was the scytale, which was developed by the Spartans as far back as the 5th century B.C [10]. Other notable cryptosystems include the Viganere cipher, the Beauford cipher and the Enigma Machine [11, 12]. As the processing power of technology increases, conventional cryptographic techniques that were once thought secure, become obsolete. With the increase in the importance of cyber communication in current society, reliable cryptography is now a necessity. Sensitive data such as military communication, classified government information and banking communication have been at the forefront of receiving the best cryptographic systems currently available. We currently also see a shift towards individual consumers using cryptography to protect their sensitive data online, especially when using online banking systems [13].

The use of public key cryptography and symmetric ciphers form the foundation of modern cryptography [14]. Decrypting these systems would require robust factorisation algorithms, which have not yet been developed, due to their mathematical complexity. It is important to note, however, that the development of strong factorisation algorithms are a mathematical advancement that may be realised in the future [15].

The development of quantum computers is an ongoing field of study and future experimental realisations of quantum computers may be able to decrypt our current cryptographic schemes and render them obsolete [16]. This is an open question but long term sensitive data requires a robust cryptographic scheme that is not vulnerable to future advancements in technology. Once current cryptographic schemes are broken, all current and past encrypted data become vulnerable. The only current encryption technique that has been proven to be secure is the One Time Pad (OTP) [17, 18, 19]. Only a brute force

attack, which would require the testing of every possible permutation of the key, would break the encryption, but this is time intensive. Advancements in quantum technology, used in tandem with techniques like the OTP, offers a solution for permanent security [20].

1.1 The Theory of Quantum Key Distribution

Quantum security was born of an idea to secure bank notes against forgery in the 1970's [21]. The concept of Quantum Key Distribution (QKD) was formalised by Bennett and Brassard in 1984 with their proposal of the first QKD protocol [22]. QKD relies on the theory of quantum mechanics to securely share a random, secret key between authenticated parties. The key can then be used to encrypt sensitive data for transmission or storage. The security of QKD lies in the physical properties of quantum mechanics, such as the "No Cloning" theorem and Heisenberg's Uncertainty relation, which will be explained in detail in the following section. The security of QKD is, therefore, independent of technological advancement in processing power, making QKD suitable for long-term encryption.

The qubits that constitute the key are transmitted between the transmitter (Alice) and receiver (Bob) in the form of quantum two-level systems [23]. Each quantum state $|\Psi\rangle$ can be expressed as a linear superposition of two eigenstates

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{1.1}$$

The probability of measuring the quantum state in each of its respective eigenstates is $|\alpha|^2$ and $|\beta|^2$ and the sum of these probabilities in unitary. The eigenstates are orthogonal and form a basis set. Many QKD protocols make use of a second basis set of orthogonal states, non-orthogonal to the first basis set. The second basis set can be expressed as

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle). \tag{1.2}$$

Using the principles of QKD, a quantum state cannot be measured with complete certainty without first knowing which basis the state should be measured in [22]. This property prevents an eavesdropper (Eve) from gaining complete knowledge about a quantum state without creating observable disturbances in the system. Attempting to clone the quantum state in order to make multiple measurements in different bases will also alert the transmitter and receiver to the presence of an eavesdropper [24].

Preliminaries of Quantum Mechanics

QKD exploits physical, quantum mechanical phenomena to secure data. Quantum bits (qubits) of information are encoded onto quantum particles such as the spin of single atoms or the polarisation state of photons of light [23]. While it is possible to use the spin of an atom or any other quantum property as a quantum binary system, this thesis will focus on the use of single photons as the information carriers, since they are easy to produce and transmit in practical applications. Quantum particles exhibit behaviour which can be described by the following principles:

Superposition

Superposition is the wave-like phenomena describing a quantum system that exists in all possible states, with an associated probability, until it is observed [25]. It then collapses into one observable state. Using the example of a polarisation state of a photon, the probability of measuring a diagonal state in the rectilinear basis, will depend on the angle of the diagonal state with respect to the measurement basis. The sum of the probabilities of each state is unitary. Since an eavesdropper will need to observe and recreate quantum states according to their observations, the presence of an eavesdropper will cause perturbations in the system which can be detected.

Uncertainty relation

Heisenberg's Uncertainty relation states that conjugate observables cannot be simultaneously measured with precision [26]. The measurement of one observable will create an intrinsic uncertainty in the measurement of its conjugate. Applying this principle to QKD, the measurement of a qubit in one basis creates an uncertainty when measuring the same qubit in another, non-orthogonal basis. Therefore, the same qubit cannot be precisely measured multiple times in different bases, preventing the collection of total information of one qubit.

No Cloning

The "No Cloning" theorem states that there is no quantum mechanical device that can create a perfect copy of an arbitrary pure quantum system without inducing changes in the original system [27]. This theorem prevents an eavesdropper from copying the information from a qubit multiple times and measuring conjugate observables of the clones in order to violate the Heisenberg Uncertainty relation.

Entanglement

Quantum entanglement describes the correlation between a pair of particles which interact and are then separated in space [28]. The pairs of particles are most commonly created by the process of parametric down conversion, resulting from pumping a non-linear crystal with a laser source [29]. The pair of particles are indistinguishable, thereby sharing identical information. The particles are in a state of superposition until one of them is measured. The measurement of one of the particles allows the observer to gain complete knowledge of its twin without actually observing the other particle. For the purpose of QKD, entangled pairs can alert the users to an eavesdropping attempt since the states of both particles will be perturbed if one is measured during eavesdropping. The quality of the entanglement between the pair of particles can be tested with the use of Bell's inequality [30].

1.2 Implementation of QKD

The implementation of QKD focuses on three aspects: the transmitter, the channel and the receiver. The Alice module consists of a single photon source and an encoding apparatus. A quantum random number generator must be linked to the encoding apparatus in order to ensure a truly random key. Qubits can be encoded onto photons using different techniques in order to create a 2-level system. The quantum channel is usually in the form of a free space, line of sight connection between Alice and Bob or a fibre optic link, independent of line of sight. The channel parameters contribute to the overall efficiency of the system, as well as the noise, Quantum Bit Error Rate (QBER) and secret key generation rate. The Bob module includes a method to randomly choose a measurement basis as well as the single photon detectors.

The first QKD experiment encoded binary information as polarisation states of a single photon [31]. The polarisation of light is described by the direction of oscillation of the electromagnetic wave, transverse to the direction of propagation, and can be linear, elliptical or circular [32]. This method is simple to implement and is still widely used today, especially in free space systems. Since commercial QKD systems operate in fibre optic networks, it is more efficient to implement phase encoded QKD [33], due to the intrinsic birefringence in fibre optic cables which alters the state of polarisation of a photon during transmission [34]. An unbalanced Mach-Zehnder interferometer is used to encode a phase difference for each pulse. The size of the interferometer is proportional to the phase shift required for the encoding. The pulses are transmitted through a second interferometer in the receiving apparatus which creates an additional phase difference, unknown to the

transmitter. The combined phase difference is measured and distilled to a binary value [35]. Practically, it is difficult to keep the relative path differences between the interferometers stable due to fluctuations in the environment. The interferometers must therefore be placed in temperature-stable housing [36].

The use of the orbital angular momentum (OAM) of a photon as an information carrier is an active area of research, especially for its application in free space communication [37]. The wavefront carrying OAM can be described as the twisting of the wave around its axis of propagation. The advantage of using an OAM state is the availability of an infinite dimension Hilbert space which can be applied to generating bits which are not restricted to binary states. Time bin encoding is a simple technique which uses the time of arrival of a photon as the information carrier [38]. The photons are transmitted through an unbalanced interferometer and the path of the photon determines whether a delay is introduced or not, creating a binary code.

There are a number of developing technologies that can increase the efficiency and transmission distance of QKD networks. Optical amplifiers can be used to boost a faint single photon signal so that it can be transmitted further [39]. Research is also being done to develop quantum repeaters, capable of recreating a quantum state via an entangled photon pair, without destroying the information in the original photon during interaction [40]. The information is shared with an entangled particle in order extend the channel length for quantum communication. Even though the sharing of information between particles does not destroy the original quantum state, a measurement made on any of the entangled particles will cause perturbations in the system and alert the authorised parties to the presence of an eavesdropper [40]. Reference-frame-independent QKD methods will also simplify the implementation of QKD systems, particularly in free-space communication [41]. These techniques, if implemented, can lead to the development of quantum networks as well the integration of different channel mediums into one, continuous network.

1.3 Security of QKD implementation

The theory that forms the foundation for QKD provides a secure data encryption method that is unconditionally secure [42]. This means that QKD is, in principle, secure regardless of the technological resources of an eavesdropper. The presence of an eavesdropper creates a perturbation in the system which can be quantified and Alice and Bob can formulate an upper bound on the information the eavesdropper may have acquired [43]. Alice and Bob estimate the expected errors in the system before the key distribution process and compare it to the errors measured afterwards using an error correction algorithm [44]. The

percentage of errors, the QBER, must be below the predetermined upper bound that was calculated in order to ensure the security of the key [24]. Privacy amplification algorithms can be used to reduce the length of the key, thereby reducing Eve's information to the point where she does not possess any usable information about the key [45].

QKD is considered to be unconditionally secure, but the implemented system must satisfy the following criteria in order to maintain unconditional security [43]. These requirements are applicable to all security protocols, including QKD:

- Alice and Bob must trust the integrity of their apparatus.
- The apparatus must be isolated from external probing.
- The classical channel between Alice and Bob must be authenticated.
- Any eavesdropper must also be limited by the laws of physics.

The vulnerability of QKD lies in the real world implementation, which often requires the use of imperfect devices. Known eavesdropping methods that are used to target QKD systems rely on implementational flaws, usually in the imperfect single photon source or the single photon detectors which have low quantum efficiency. Eavesdropping attacks can be separated into three classes [46, 47]:

• Individual attacks – In this category of attacks, each qubit is measured separately by Eve. Eve can either measure each photon in real time or store the photons in a quantum memory and measure them only after the public post-processing discussion by Alice and Bob. Since a quantum memory device has not been practically realised, this type of attack is not realistic.

• Collective attacks – Similarly to individual attacks, Eve also intercepts each qubit separately. In this scenario, she stores the information in a quantum memory and measures the ancillas several at a time, at a later instance.

• Coherent attacks – This is the most general category of attacks. Eve is able to carry out any form of attack and is only limited by laws of quantum physics.

Research on QKD eavesdropping techniques and their respective countermeasures is an ongoing task and commercial systems must continuously evolve in order to prevent newly found eavesdropping attacks. While it is possible to create individual fixes for each type of attack, a general solution for eavesdropping attacks remains elusive.

1.4 Contributions

The commercialisation of QKD as a robust encryption technology has expanded in the last decade. There has been a stronger focus on developing QKD systems for long range, fibre networks in municipal areas [48]. The development of long range, free space QKD systems is still an ongoing area of research with recent practical implementation. A newer application for QKD systems is the development of short range, handheld devices, appropriate for an individual consumer. In this thesis, we work towards building a laboratory prototype for a handheld QKD device using the Coherent One-Way (COW) protocol, due to its practical design. We focus on the synchronisation of the system using an optical and electronic subsystem. An emphasis is put on the detection line of the COW protocol, since the characterisation of the key distribution can be guaged from this portion of the system. The monitoring line will be discussed as future work for the project. The COW protocol is well suited for fibre communication, and for the first time, to our knowledge, this protocol has been implemented in a short range, free space channel.

We propose the application of this protocol to a long range free space channel between a ground station and a Low Earth Orbit (LEO) satellite. We discuss the synchronisation of the long range, free space system via a radio signal and present simulations of the synchronisation subsystem. The methods and results for the above will be presented in the following sections.

1.4.1 The experimental setup and optical synchronisation system

The COW protocol was first implemented in a fibre optic network and the literature shows that subsequent implementations have followed suit. The device presented in this thesis adapted the COW protocol for implementation in a free space channel. The components used for the implementation remained similar to the original design but added components were required for alignment. The synchronisation subsystem is important for any QKD device in order to optimise the efficiency of the system. An optical synchronisation system was designed and built for the handheld device. An optical synchronisation system was chosen for its low power consumption and off-the-shelf components. The optical synchronisation system was tested and implemented for the key distribution. This work is based on the Publication 3 and is presented in Chapter 3.

1.4.2 Characterisation of the quantum key distribution

The defining characteristics for a QKD system are the bit generation rate and the QBER. The bit generation rate gives an indication on how fast the system can generate and share a secret key. The QBER will determine if the key is appropriate for use. An interesting property of the COW protocol is that the security of the key is determined via measurements in the monitoring line. The work presented in this thesis does not focus on the monitoring line, but the relevence for a QBER measurement in the detection line is presented. The bit generation rate was predicted and each contributing factor was measured. The QBER was also predicted and the measurement of the QBER was equivalent to the theoretical prediction, proving the accuracy of the synchronisation system. This work is presented in Chapter 4.

1.4.3 Radio synchronisation for satellite QKD

Phase encoding for QKD has, so far, been limited to fibre optic networks. With recent developments, combining the techniques of continuous variable QKD with phase encoding, it has become a viable option to use phase encoding for long range, free space transmission between ground stations and satellites. This may allow for a long range, free space implementation of the COW protocol, since the coherence between pulses will not deteriorate. The synchronisation signal and classical communication can be implemented via a radio transmission which can be modulated using Binary Phase Shift Keying (BPSK). The demodulator requires a Costas Loop to receive the data from the public channel and extract the synchronisation signal. A simulation is presented, showing the advantage of using the Costas Loop during communication with a LEO satellite. The Doppler effect on the synchronisation is minimised, allowing the local oscillator of the receiver to match the frequency of the incoming synchronisation signal, thus increasing the duration of the transmission. This work is based on the Publication 4 and is presented in Chapter 5.

2 The COW protocol and portable QKD devices

A number QKD protocols have been devised since the first protocol in 1984 [22]. Three main classes of QKD schemes exist, namely, discrete variable QKD, continuous variable QKD and distributed phase reference QKD [43]. The following chapter will describe the three QKD classes as well as their associated protocols, focusing on the Coherent One-Way (COW) protocol which is part of the distributed phase reference category. This chapter also discusses the use of portable QKD devices in a quantum communication network and highlights some of the techniques used in implementing these devices.

2.1 Discrete, Continuous and Distributed Phase Reference QKD

2.1.1 Discrete Variable QKD

In a discrete variable protocol, a qubit is encoded onto a single quantum particle, such as a photon. The encoding can take many different forms, but the most commonly used quantum two-level systems in this class of protocols are polarisation and phase [43]. Discrete variable protocols are the most commonly used and widely researched protocols. In these schemes, each single photon is encoded with one qubit of information. The photons are transmitted from Alice to Bob in a sequence of pulses and each photon is individually measured by Bob.

BB84 Protocol

The BB84 protocol was designed by Bennett and Brassard in 1984 [22]. This was the first QKD protocol established and is still widely used in research labs and commercial

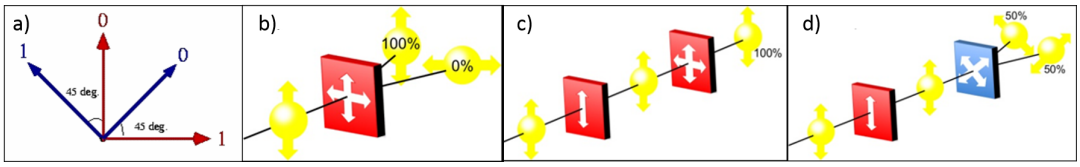

Figure 2.1: Figure a) shows an example of how polarisation states can be used to represent binary bit values for the BB84 protocol. Each non-orthogonal measurement basis (rectilinear and diagonal) has two states, each representing a bit value. Figure b) shows that when the correct measurement basis is used, the correct polarisation state will be measured with 100% certainty. As seen is c), if an eavesdropper intercepts the photon using the correct measurement basis, the polarisation state is unchanged and Bob will still receive the correct measurement. However, if an incorrect measurement basis is used, as shown in d), there is a 50% probability of either outcome of that basis. If Bob measures the resulting diagonal state with the rectilinear basis, there is again a 50% probability of either outcome of the rectilinear basis. The outcome could, therefore, be a horizontal polarisation state, which does not match the vertical state that Alice prepared. This image is sourced from [1].

systems today. The protocol has been applied to polarisation encoding as well as phase encoding. The following paragraph uses polarisation encoding to explain the processes of the protocol.

The four state protocol allows for each bit to be represented by two possible states, each in a different, non-orthogonal measurement basis, seen in Figure 2.1a). Therefore, upon measuring a state, an adversary cannot be certain of the bit value without additional information on whether the correct measurement basis was used, seen in Figure 2.1b), c) and d). Alice begins the protocol by randomly selecting one of four polarisation states. These states are transmitted to Bob sequentially and Bob randomly chooses a measurement basis for each single photon. After the measurements are complete, the quantum communication aspect of the protocol is also concluded. The remainder of the protocol is executed over a public, classical channel. Bob publicly announces the basis used to measure each photon and Alice confirms which of these match the basis she chose to encode them, hence resulting in a correct measurement. Since each basis contains both bit 1 and 0, announcing the basis used for each photon does not disclose any information about key. The instances of an incorrectly chosen basis are discarded since these measurements lead to ambiguous results. The remaining string of bits undergoes error correction and privacy amplification. If, during error correction, Alice and Bob notice an unusually high QBER, they can infer that an eavesdropper has intercepted their key. Typically, the BB84 protocol has a threshold of 11% for the QBER [49]. If the error rate exceeds this limit, the key is discarded, since all errors must be attributed to the eavesdropper. If the error rate is within the limit, Alice and Bob now both possess an identical string of bits which can be used as a quantum key.

Other Discrete Variable Protocols

Other commonly used discrete variable protocols include the B92 protocol [33] and the SARG04 protocol [50]. These protocols are similar to BB84 in terms of implementation and would require the same components to operate. They differ in the sifting procedure which is discussed publicly after the distribution of photons. Alternative protocols are designed to improve on the BB84 protocol by being robust against eavesdropping, specifically the Photon Number Splitting (PNS) attack [51]. The SARG04 protocol is especially robust against this type of attack since Eve would need to extract two photons from a pulse in order to gain full information from the bit, while leaving a third photon in the pulse for Bob to measure and remaining undetected. Resistance to PNS attacks makes QKD protocols simpler to implement with the use of a faint laser source instead of a costly single photon source.

Another method to prevent PNS attacks is to use decoy states [52] in conjunction with a discrete variable protocol. For this technique, Alice intentionally integrates multiphoton decoy pulses with her quantum signal. These pulses do not contribute to the quantum key and will be removed during the sifting process, but Eve cannot distinguish them from naturally occurring multiphoton pulses. If Alice and Bob notice that there are relatively more decoy pulses measured by Bob's detectors than the signal pulses, they can infer that an eavesdropper is intentionally trying to control which pulses reach Bob's apparatus. Alice and Bob can then stop the key distribution. The decoy state protocol has been widely implemented in QKD applications since it is a simple method to maintain the security of the key transmission over longer distances.

The Ekert91 protocol introduced the use of quantum entanglement for QKD [53]. The protocol is developed from the Einstein-Podolsky-Rosen gedanken experiment and uses spin half particles as the carriers of binary information. A pair of entangled particles is produced and Alice and Bob each receive one of the pair. They each randomly choose a basis of measurement and independently record their measurements for each particle. Alice and Bob announce the basis used for each measurement and only keep the bits for which they used the same basis. The remaining bits are not entirely discarded, like in the BB84 protocol. Instead, they are used to obtain a set of correlation coefficients which are used to verify the security of the key using the Clauser, Horne, Shimony and Holt (CHSH) inequality. Entanglement based QKD has provided an advantage in the development of QKD for real implementations. Since the photon pairs can be produced by a third party, Alice and Bob can increase the distance between them, effectively doubling the possible channel length of a one-way, prepare and measure scheme.

2.1.2 Continuous Variable QKD

While discrete variable QKD utilises one discrete quantum particle per qubit, continuous variable QKD uses continuously-modulated Gaussian states to create a key [54]. An example of this would be the use of field quadratures of multiphoton states of light. The quadratures are measured using homodyne or heterodyne detection. Continuous variable QKD can be implemented without the need for single photon souces or single photon detectors [55], making this category of protocols practical and efficient in noisy and lossy channels [56]. Continuous variable QKD require complex error correction algorithms, making it unsuitable for long-distance communication. However, research has been done to improve on the signal-to-noise ratio and stability of the quantum channel and generate larger data blocks which improve on the error correction bottlenecks. Due to these improvements, continuous variable QKD is now being implemented in fibre channels up to 80 km using standard telecoms components [57, 58]. The use of field quadratures has been shown to minimise the effects of turbulence in free space QKD [59]. Using this advantage, continuous variable QKD is being developed with phase encoding for satellite communication. This concept will be discussed further in Chapter 5.

2.1.3 Distributed Phase Reference QKD

This category of protocols does not encode one bit of information per photon pulse. Instead, the information is shared between two or more pulses. Distributed phase reference protocols are practical to implement, as they do not require single photon sources. The protocols are resistant to the PNS attack [60] and can therefore, be implemented with faint laser sources, making them cost effective and simpler to obtain components for. Two distributed phase reference protocols that have been researched and tested in recent years are the Differential Phase Shift (DPS) [61] and COW [2] protocols.

The DPS protocol was proposed by Inoue *et al.* in 2002 [61]. A photon is distributed between three sequential pulses, each separated by a phase difference determined by Alice's passive optical setup. The phase between two pulses is resolved by an unbalanced interferometer in Bob's apparatus and the recombined pulses are directed to one of two detectors, depending on whether the phase difference was 0 or π. Similar to the COW protocol, discussed below, the security of the key distribution is maintained by confirming that the coherence between consecutive pulses is unchanged.

2.2 The COW Protocol

2.2.1 Theory of the COW Protocol

The COW protocol was developed by Stucki *et al.* in 2005 [2]. This is a distributed phase reference protocol and therefore, the qubits are not represented in individual photon pulses. The protocol uses time bin encoding and the qubit values are encoded into two consecutive coherent pulses, one containing a single photon and the other, empty, as seen in Figure 2.2. The order of the pulses determines the bit value such that

$$|1k\rangle = |\sqrt{\mu}\rangle_{2k-1}\,|0\rangle_{2k}\,, \tag{2.1}$$

$$|0_k\rangle = |0\rangle_{2k-1}\,|\sqrt{\mu}\rangle_{2k}\,, \tag{2.2}$$

where k is the time bin index and μ is the mean photon number of that pulse. A portion of the pulse pairs both contain single photons and these consecutive, non-empty pulses are used as decoy states *f*. The decoy states can be described as:

$$|f_k\rangle = |\sqrt{\mu}\rangle_{2k-1}\,|\sqrt{\mu}\rangle_{2k}\,. \tag{2.3}$$

Alice begins the protocol by transmitting a sequence of coherent pulses, each randomly chosen to either contain a photon or be empty. The pulses are paired and the qubit values are recorded according to their time bin. The time bins for the decoy pulses are also noted. The apparatus required to implement the COW protocol is simple and includes off-the-shelf components. Alice uses a faint coherent laser source and an external optical modulator to create the string of qubits and transmits the string to Bob over the quantum channel. Bob's apparatus includes a primary detector D_B, in the data line, used to measure whether the incoming pulses contain photons or not. A portion of the pulses is diverted from the data line into a monitoring line using a beam splitter. Current implementations of the COW protocol usually use a 90/10 beamsplitter, therefore transmitting 10% of the pulses into the monitoring line. A Mach-Zehnder interferometer is used to create interference between two consecutive non-empty pulses (decoy states) and the outputs of the interferometer are measured on the monitoring line detectors, D_{M1} and D_{M2}.

For this protocol, Bob does not need to randomly choose his measurement basis, as in discrete variable protocols. Bob measures all pulses in the data line without the need for polarisation or phase discrimination, since it is just the presence of a photon and its time

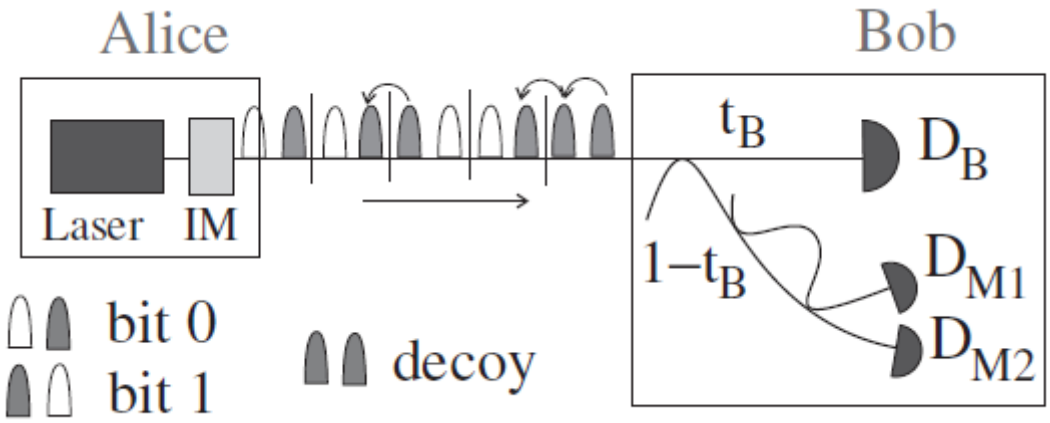

Figure 2.2: A diagram showing a simple schematic of the COW protocol setup. Alice's module consists of a laser and an intensity modulator (IM) which is used to create bit values by varying the mean photon number per pulse. A combination of one empty and one non-empty pulse contributes to the bit, their order determining the bit value. Two consecutive non-empty pulses are considered decoy pulses. Bob's apparatus consists of a detector D_B, which measures portion t_B of the incoming pulses in order to determine if they are empty or non-empty. The remaining portion of pulses are directed into the monitoring line, which measures the decoy pulses. The pulses are transmitted through an unbalanced interferometer and measured on detectors D_{M1} and D_{M2}. The arrows between pulses indicate the combination of bits which can be used to verify the pulse coherence in the monitoring line. The coherence can be measured within a pair of decoy pulses or across two bits with neighbouring non-empty pulses. Any pulses measured in the monitoring line are removed from the raw key. This image is sourced from [2].

bin that determines the bit value. The raw key is obtained from the detections of D_B and post processing is used to distil the key. Bob announces which bits were measured in the monitoring line, since these must be discarded from the key. Alice also announces which bits contained decoy states so that Bob can remove these measurements from the key as well.

The security of the key distribution is verified by monitoring the visibility of the Mach-Zehnder interferometer in the monitoring line [62]. The coherence of the pulses can be verified by Bob by superimposing two consecutive pulses using the Mach-Zehnder interferometer. Bob should observe constructive interference at one output of the interferometer and destructive interference at the other. Should this condition be compromised, the presence of an adversary is inferred. This can be used to estimate the information acquired by the eavesdropper. Alice and Bob apply error correction and privacy amplification algorithms on the sifted key in order to obtain the secret key which is then ready to be used for encryption.

2.2.2 Security of the COW Protocol

Security for Practical QKD Implementation

While QKD is an unconditionally secure method to transfer a cryptographic key, QKD protocols are implemented in real world applications using imperfect devices [63]. An eavesdropper may exploit the shortcomings of imperfect single photon sources or inefficient single photon detectors. There are well researched attacks that are subtle to the sender and receiver and cannot be detected unless special precautions are taken.

The PNS attack exploits the common implementation of faint laser sources in place of single photon sources [50]. When using an attenuated laser, for which the mean photon number follows a Poisson distribution, a percentage of the pulses will contain more than one photon [64]. An eavesdropper can divert the extra photons using a beamsplitter and gain full information from them when Alice and Bob publicly announce the basis used for each state. This can be especially high risk if the quantum channel causes high loss during transmission, since the loss that Eve introduces will be unnoticed.

Due to the low efficiency of single photon detectors, especially for fibre telecoms wavelengths, detectors can be exploited by an adversary and used to gain information about the cryptographic key. Eve can force detections by flooding the single photon detectors with excess light, thereby controlling Bob's measurements [65]. Eve can also exploit the timing resolution of the detectors and force a detection with bright light that will result in Bob obtaining the same set of bits that she has. The faked-states attack is an improvement on the intercept-resend attack [66]. The pulses that Eve resends to Bob have a very low optical power and are therefore, not measured should Bob use the incorrect basis so Alice and Bob do not notice an increased number of errors during post processing.

Trojan horse attacks exploit vulnerability in Alice's apparatus by interrogating the encoding components with bright light [67]. Any reflected light will carry information about Alice's encoding, which gives Eve full information about the key when combined with the post processing discussion. The same method can be applied to Bob's apparatus, whereby Eve can discern which basis Bob chooses for each measurement [68]. Counteracting implementational attacks can include the use of extra detectors to monitor bright light or filters to keep Eve's light out of the apparatus. Circulators can also be used to redirect any unwanted light.

While these countermeasures may be simple to implement, it is impossible to know exactly which attack Eve may use. So far, a general countermeasure for all categories of attacks is still to be developed [35]. An active area of research is the development of measurement-device independent QKD protocols which allow the use of untrusted appar-

atus in forming a secure key [69]. This will prevent the leak of information through side channels and decrease the risk posed by inefficient detectors and untrusted manufacturers.

Security proofs for the COW protocol

The security of the COW protocol has been a work in progress since its development [70]. Since the COW protocol is not a discrete variable protocol, it is difficult to estimate the upper bounds of the security. The COW protocol has been proven secure against intercept-resend attacks [3], general individual attacks and collective attacks so far [71]. A proof for security against most general attacks is still an active area of research since current QKD security proofs need to be adapted to the COW protocol.

The COW protocol has been proven secure against PNS attacks [3]. The COW protocol's robustness against PNS attacks allows the use of a higher mean photon number per pulse. Discrete variable protocols usually set a mean photon number of 0.1 photons per pulse. The COW protocol can be implemented with a higher mean photon number, still under 1 photon per pulse. This can lead to higher secure key generation rates and a longer quantum channel length, which is especially advantageous for fibre optic channels. Resistance to PNS attacks also means that the COW protocol is more suited for implementation with low cost, faint laser sources, without compromising on the security of the protocol.

The eavesdropper may attempt to attack coherently across two pulses in order to avoid detection. For example, if the eavesdropper attacks coherently across a decoy pair of pulses, the monitoring line will not measure the presence of the eavesdropper for those pulses. However, the coherence between non-empty pulses across the $|0\rangle\,|1\rangle$ bit separations will be destroyed and this can be observed in the monitoring line, as shown in Figure 2.3. It is important to note that, even though a small fraction of errors are measured in the monitoring line, a fast bit rate can ensure that the error rate for the transmission can be estimated in a reasonable time [3].

2.2.3 Implementations of the COW Protocol

The first experimental realisation of the COW protocol was done by Stucki *et al.* in 2005 [2]. The key distribution was achieved over a fibre optic channel and required simple components. A continuous wave laser at a wavelength of 1550 nm was coupled to an intensity modulator which selected the bit encoding. For a simple, proof-of-principle experiment, the pulses were encoded with a repeated sequence of decoy, 0, 1, 0. The pulses were generated at a frequency of 434 MHz and the delay between the successive repetitions of the sequence was set by a clock at 600 kHz. The laser pulses were attenuated

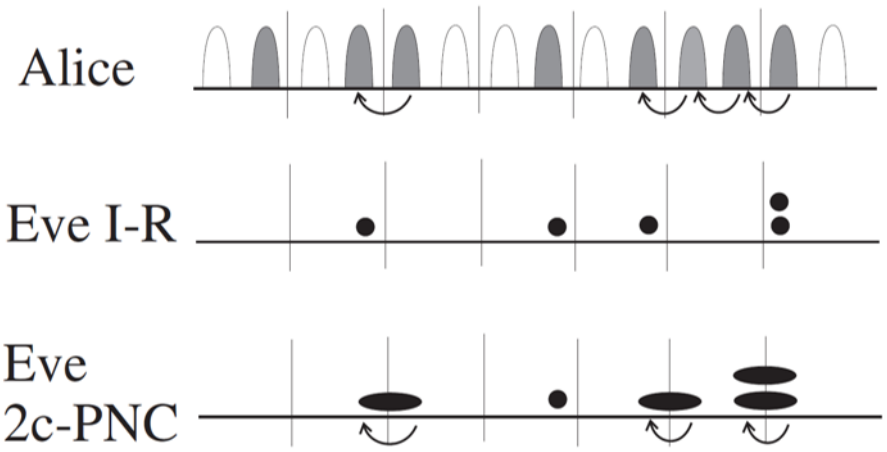

Figure 2.3: A diagram showing the effects of coherent attcaks by an eavesdropper (Eve) on Alice's transmission. The arrows between pulses indicate the coherence between them. If Eve implements the Intercept-Resend (I-R) attack on random pulses in Alice's transmission, the coherence between all the original pulses is broken. If Eve implements an attack that intercepts coherently across the bit separation, as shown in 2c-PNC, she leaves the coherence intact across the bit separations but the coherence between the decoy pulses is now destroyed. This can be measured in the monitoring line. This diagram is sourced from [3].

by a variable attenuator so that the mean photon number per pulse was set to $\mu = 0.5$. The loss in the quantum channel was 5dB. The detectors in Bob's apparatus, D_B and D_M were triggered by a time-to-digital converter and were controlled to open the detection gates for a duration of 25 ns. The quantum efficiency of the detectors was at 10% and the dark count rate was 2.5×10^{-5} counts per ns. The interferometer had a path length difference of 46 cm of fibre, corresponding to the pulse rate of 434 MHz. The interferometer was contained in a temperature controlled box so the phase could be controlled by varying the temperature. The raw detection rate was measured to be 17 kHz and was bound by the 10 µs dead time of the detectors. The QBER of the system was measured to be 5.2%. Of this, 4% was due to the noise in the detectors as well as afterpulses. The other 1% was due to imperfect pulse modulation.

A QKD prototype using the COW protocol to exchange a secret key was developed by Stucki *et al.* in 2009 [72]. The prototype was tested under laboratory conditions and was also implemented over the Swisscom fibre optic network. The prototype was designed as two rack-mountable modules, one each for Alice and Bob. The modules were linked by two fibre optic connections for quantum communication and classical communication, needed for synchronisation and post processing. The Alice module consisted of a Continuous Wave (CW) laser which was pulsed by a lithium-niobate intensity modulator. A portion of the beam was diverted into a detector, which monitored the power in each pulse, allowing the mean photon number to be set to 0.5 by a variable attenuator. The optical

pulses were produced by the Alice module at a rate of 625 MHz with a pulse width of 300 ps. A quantum random number generator was used to seed a pseudo-random number generator able to produce random numbers at a faster rate. This was linked to the intensity modulator, producing the bit encoding for the Alice module.

The Bob module consisted of a 90/10 beam splitter which allowed 90% of the incoming pulses to be measured by the primary detector D_B. The remaining 10% was diverted to the monitoring line and transmitted through a temperature stable Michelson interferometer before being measured by the detector D_M. The InGaAs/InP avalanche photodiode detectors both had a quantum efficiency of 10% and a dark count rate of 10^{-6} counts per ns. Both modules include electronics and an embedded computer to control the components and synchronise the system. The detector dead times were set to 30 μs in order to reduce the afterpulsing effects, however, this limited the detection rate to approximately 30 kHz.

The laboratory tests were carried out over 25 km of fibre with an additional attenuator placed between Alice and Bob, bringing the total attenuation to 21 dB, equivalent to 100 km of fibre. The system operated continuously for 10 hours and was able to automatically realign itself when the bit rates decreased below the pre-set threshold. A mean secret key generation rate of 2 kbits per second was achieved. The field tests were carried out over the Swisscom fibre network at a channel length of 150 km. Due to the high attenuation of this fibre link at 43 dB, the effective length corresponds to about 200 km of standard fibre. The InGaAs detectors were replaced by super conducting single photon detectors and an average secret key generation rate of 2.5 bits per second was measured over 3.5 hours. However, the visibility in the monitoring line became too low to be able to confirm the security of this transmission.

The COW protocol has also been implemented over a record fibre channel length of 307 km [73]. The experimental demonstration utilised an improved finite key security analysis and implementational improvements, such as semiconductor single photon detectors, which add very low levels of background noise to the transmission. Ultra low loss fibres were also used in order to lower the attenuation of the fibre channel, thus increasing the transmission distance. A chip-based QKD system was developed by Sibson *et al.* with application to fibre networks [62]. The system components were designed to implement phase encoding, allowing the BB84, DPS and COW protocols to be implemented on the same apparatus. The compact transmitter and receiver modules were connected via a variable optical attenuator which simulated the channel loss of 20 km of fibre. For the COW protocol implementation, the system was able to exchange a secret key at a rate of 311 kbps with a QBER of 1.37%.

2.3 Implementations of QKD over Long Range Channels

2.3.1 Current Implementations of QKD

The industrialisation of QKD technology created new opportunities to improve on existing key distribution methods and new protocols were rapidly developed. It also brought into focus the vulnerabilities of implementing quantum technology with imperfect devices [3]. As mentioned in Chapter 1, single photon detectors are not 100% efficient in measuring every photon and the quantum channel can deteriorate the photon signal significantly due to attenuation and dispersion. With the aim of making QKD a marketable technology, more research was conducted to exploit every vulnerability of the system and then compensate for these vulnerabilities, fortifying a commercial QKD system against all conceivable types of attacks.

The objectives that research and development of QKD systems has focused on achieving are [72]:

- The development of protocols resistant to the PNS attack, making faint laser pulses a more viable optical source for commercial use.
- The improvement of the components used to implement QKD in order to increase transmission distance and the bit generation rate.
- The standardisation and integration of QKD systems in existing networks.

Commercial QKD systems are available for purchase from IDQuantique, MagiQ Technologies, QuintessenceLabs and SeQureNet and many other companies are also developing QKD technologies for commercial purposes. Both IDQuantique and MagiQ Technologies use discrete variable QKD over a fibre optic channel, specifically the BB84 protocol. IDQuantique also implements the SARG04 and COW protocols. QuintessenceLabs and SeQureNet use continuous variable QKD for their commercial products, also over a fibre optic network.

QKD has already been implemented in long range fibre communication in both the public and private sector. Long term feasibility tests for QKD encryption systems have been conducted in public networks by many research groups in the past decade. The most notable of these long term QKD implementations include DARPA [74], TokyoQKD [75], SECOQC [76], Los Alamos National Laboratory [36], SwissQuantum [13] and QuantumCity [48]. The QuantumCity project was implemented in the eThekwini municipality by the Centre for Quantum Technology at the University of KwaZulu-Natal. This project led

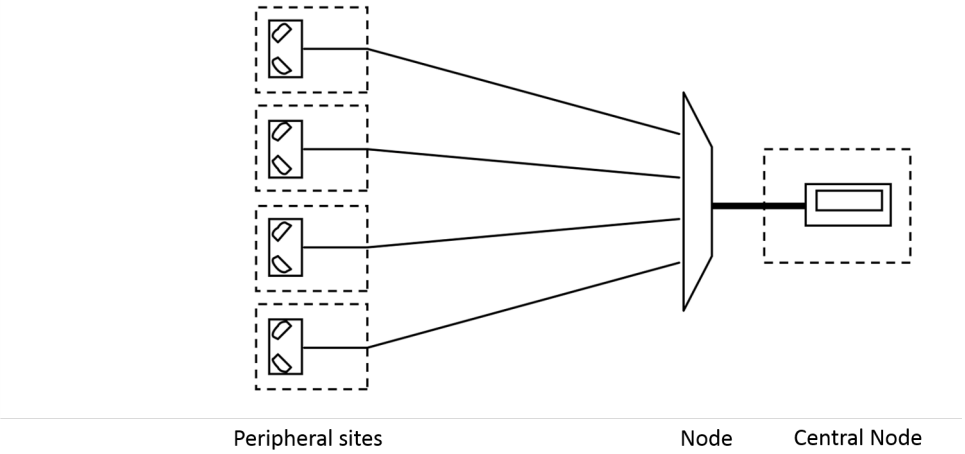

Figure 2.4: Diagram of a star topology network, connecting many peripheral sites to one, common central node.

to the QuantumStadium [77] project implemented during the 2010 FIFA World Cup^{TM} which encrypted all security communication throughout the event.

2.3.2 The use of the star topology network for a handheld QKD device

Commercial QKD systems are developed to encrypt a network between two points. This is typically an arrangement of fibre optic cables connecting a central node to one or more remote sites. The implementation of free space channels to form a network is a topic of current development. Depending on the requirements of the end users, networks can be arranged in different configurations. The star-topology network, shown in Figure 2.4, is most relevant for a QKD network as it allows for many periphal sites to communicate with, or be routed through, one central node [4]. This is especially useful for banks or businesses that need to communicate sensitive data to one central head office. This configuration requires just one Alice module, transmitting to many Bob modules or vice versa. Such an arrangement can be advantageous for costs as the cheaper module, between Alice and Bob, can be used for the peripheral sites while only one expensive module is needed for the node.

The device proposed in this thesis is designed to be used in a star-topology network, allowing several users to exchange a secret key with one node of the network. When implementing the COW protocol, the Alice module is simple and low cost, and is therefore assigned to be the portable peripheral module. The Bob module requires more components and a stable environment and will therefore be used as a node. Several nodes (Bob modules) at different locations then conduct a key distribution with a central node, thereby facilitating a key exchange between the users and the central node.

The key exchange between the user (Alice) and the node (Bob) is done over a short range, free space channel. The device presented in this thesis will focus on this short range aspect of the QKD network. The QKD between the node and the central node can be done via a long range fibre optic channel, which can be integrated with the telecommunications network of a municipality [78]. Since this technology is commercially available, it would be appropriate to use for the long range QKD channel. The alternative would be to use a long range free space channel, but this is a developing field of research with many implementational bottlenecks to overcome [79]. However, the use of a long range free space channel can be of great benefit in locations where accessing fibre optic infrastructure is difficult or unfeasible.

It is also interesting to note that a recent study by Ji *et al*. discussed the feasibility of QKD in seawater [80]. The experiment was carried out under lab conditions using a sample of seawater to transmit photons over a short distance of 3.3 m. While this was only demonstrated in a lab, the results showed that the seawater was able to transmit polarisation encoded entangled photons with a high fidelity. In a real world application, seawater transmission would need similar compensation techniques to a turbulent free space channel.

2.3.3 Short range free space channel for the QKD exchange between device and node

A free space channel was chosen for the short range portion of the key exchange. This allowed for devices to be easily portable and handheld without the need to connect fibre optic cables between the user's device and the node. Using fibre to connect a portable device can become difficult to maintain since the fibre connectors must always be thoroughly cleaned and the fibre can easily become damaged with excess connecting and disconnecting. It is therefore simpler to use a free space channel since the user will just need to align the device with the node and allow the apparatus to perform the key exchange. The alignment can be done by hand or the user can place the portable device in an adapter or docking station, which will automatically align the two systems.

Typically, free space quantum communication can be difficult to implement due to the detrimental effects of turbulence on laser beams, which will be discussed in the following sections. For short range communication implemented in a stable, controlled environment, turbulence effects are negligible and the system will not require compensation techniques. Short range communication over a free space link also allows for better visibility in the channel since fibre connectors can decrease some of the optical power during transmission [81].

2.3.4 Long range channel for the QKD exchange between node and central node

The choice of utilising a free space or fibre channel to carry out the long range aspect of the QKD transmission can have different effects on the quantum information and must, therefore, be carefully considered. Each channel provides different advantages and disadvantages for channel efficiency, as discussed below.

QKD in long range fibre networks

In order for QKD to gain commercial relevance, it is imperative to develop QKD into a reliable technology applicable to the channels used for modern telecommunications. The most commonly used telecoms channel for both short and long distance communication is fibre optic cables, used for applications ranging from local telephone networks and cross-continental data lines. Fibre is manufactured from doped glass which has a higher refractive index n_1, than the refractive index of its protective cladding n_2, as described by the following equation [82]:

$$n_1 - n_2 < 0.05. \tag{2.4}$$

Any light that encounters the boundary between the fibre and the cladding will be reflected due to total internal reflection, as long as the angle of incidence is larger than the critical angle of the fibre. Therefore, as long as there are no sharp bends in the fibre, it acts as a waveguide and the light is propagated through it. Due to wavelength dependent absorption and scattering, all wavelengths are not transmitted identically through the fibre. Fibre optic cables have 'windows' of optimum wavelength transmission [83]. The wavelength that experiences the least dispersion during propagation is 1310 nm [84], making it appropriate for high-speed transmission. The fibre attenuation is lowest for a wavelength of 1550 nm [85], allowing the longest propagation distance, hence the wide use of these wavelength bands for commercial telecommunications.

The average fibre optic cable creates a 0.2 dB loss per km for typical telecoms wavelengths of 1310 nm and 1550 nm [6]. This results in a maximum distance of about 100 km before the single photon signal is too low to distinguish from the detector dark counts [86]. The use of ultra low loss fibres and superconducting detectors have improved on the technology, increasing the transmission distance to up to 250 km [87, 88] but these special components are not easily integrated into an already existing fibre optic network. Even with this improvement, QKD in fibre optic cables is limited to applications in metro-

politan networks. With technological advances, transmission distances may be increased using trusted nodes or quantum amplifiers [89].

QKD systems typically operate with a clock rate in the order of Mbit/s [90]. Dispersive properties in fibre lead to a temporal broadening of the optical pulse during transmission. This may affect the measurement of the pulse in high speed systems since the time interval for the pulse may become longer than the gate width of the single photon detector. The detector will therefore only measure a portion of the pulse and may not receive the bit value of that pulse. Detector gating must therefore be adjusted to suit the characteristics of the incoming pulses [87]. High speed systems are also affected by dispersion. A high bit rate will produce narrow pulses with a narrow space between them. A broadening of the pulses will cause them to overlap and leak qubits into the incorrect time bins. This will lead to a high error rate in the system, resulting in the discarding of the key. Research done to compensate for dispersive effects resulted in the implementation of gigahertz clock rates over a channel of 101 km [91].

An advantage of using a fibre network is the dark channel provided by the fibre, greatly reducing any stray light in the quantum channel. By employing temporal filtering techniques, multiple communication channels, such as the quantum link and classical link, can be deployed in the same fibre [92]. Fibre networks are also laid underground, protecting the fibre from vibrational disturbances and sharp changes in temperature [93].

QKD in long range free space networks

QKD over a free space channel, particularly between ground and satellite stations, is an active area of research. One of the main aspects of the development of this technology is turbulence compensation. Turbulence effects, such as scintillation, divergence and beam wander, must be reduced in order to achieve communication over longer distances via a turbulent atmosphere [94]. Free space communication can also be applied to shorter links in urban areas [95] or remote locations with inadequate telecoms infrastructure.

Methods to compensate for turbulence effects include the use of adaptive optics which adjusts in real time in order to optimise the light measured by the receiving optics [96]. A more passive method of turbulence control would be to monitor the scintillation of the beam and only allow a single photon measurement to contribute to the key when high transmissivity is observed [79]. This selection process can be done during post-processing, after the transmissivity of the channel has been characterised.

Free space QKD requires additional spatial, spectral and temporal filtering components to assist with noise reduction in the channel, especially when executing a key distribution

in daylight [97]. The synchronisation between the Alice and Bob systems must also be finely tuned so that the detectors open precisely for the arrival of the qubits, thus reducing the stray light entering the detectors. A recent study by Liao *et al*. focused on reducing the noise effects of sunlight by using a transmission wavelength of 1550 nm, a wavelength typically used for fibre comminucation [98]. The study showed that 1550 nm light is an optimal wavelength to use for free space, due to the high transmittance co-efficient but single photon detectors at this wavelength have a low efficiency, resulting in a low signal to noise ratio for the transmission. The experiment used specialised equipment, such as narrow spatial filters and ultralow-noise upconversion detectors, to optimise the 1550 nm signal.

One of the advantages of using a free space channel is the potentially longer transmission distance compared to fibre optic cables [99]. Free space channels can span longer distances, especially when operated between two satellites, above the turbulent atmosphere. The implementational bottlenecks for satellite QKD are an active area of research. The ground to satellite communication link (uplink) in a free space QKD network may be difficult to implement due to the high divergence experienced by the beam. The large optical components required to measure a wide beam can become too bulky for a satellite. These challenges can be overcome by using the satellite for an entanglement source, transmitting via a downlink to two ground stations, or by using the satellite to reflect an incoming transmission from one ground station to another [100]. Alignment and synchronisation can also be challenging due to the relative movement between the satellite and the ground station. Alignment mismatches have been addressed in [101] and [102]. The synchronisation between stations will be addressed in Chapter 5.

2.4 Portable QKD devices

While most QKD research focuses on increasing transmission distances, either for a fibre or free space channel, recent research has also shown interest in short-range, handheld QKD devices. Personal, portable QKD devices can be used for authentication purposes or to exchange a One Time Pad (OTP) password between a consumer and a central service provider. The device can serve as a means to top-up a list of passwords or encryption keys which can be used to connect to a server from any location. An example of this application would be to use the device to securely exchange a list of OTP passwords between a bank and a customer. The customer would then be able to use the passwords from their home for services such as internet banking.

The key exchange can take place at a central node which acts as a trusted intermediary

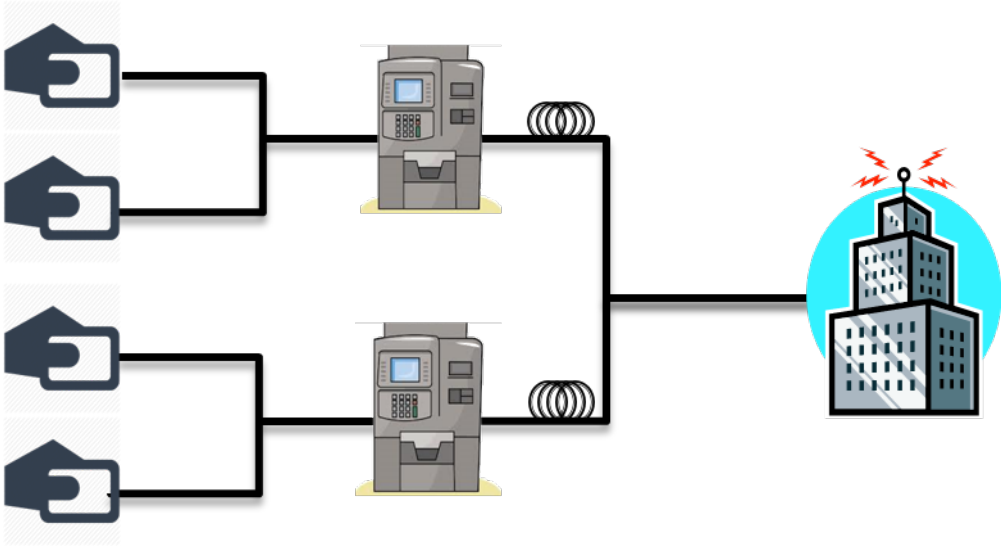

Figure 2.5: A diagram showing an example of a star topology network used to connect individual QKD devices to a central central node [4]. Multiple users are able to exchange a key with an intermediary station (node) such as an ATM. This station in turn, performs a QKD exchange with a central node such as the central office of the company. A secret key is established between the user and the vendor through the process of node hopping.

between the customer (Alice) and the bank (Bob). As per the example, the node can be in the form of an ATM, accessible to many customers, as seen in Figure 2.5. The ATM machines (nodes) would be linked to the central bank server in a star topology network. Through the process of node-hopping, a customer would be able to exchange a secure key with the bank.

A number of portable devices have been developed by research groups in the past decade. The devices developed in these studies use well established QKD techniques such as the BB84 protocol and polarisation encoding and apply them to a short range, free space application. Quantum technology is also being developed to be integrated into already existing technology. Research has been done to develop a quantum random number generator that can be retrofitted into a smartphone. Combining this technology with the design of a compact QKD device opens opportunities to enable QKD in smart phones and other easily accessible devices. These portable QKD devices and supporting technology will be discussed below.

Duligall *et al.* designed a portable and low cost QKD system using a short range free space channel [5]. The design includes both an Alice and Bob module and utilises polarisation encoding with the BB84 protocol to exchange the key. The intended use of the device is to house the Bob module in a fixed location, allowing portable Alice devices to exchange a secure key at a central location. The Alice module is intended to be compact so as to fit into cell phones etc. The Alice module consists of four red/orange LEDs that are

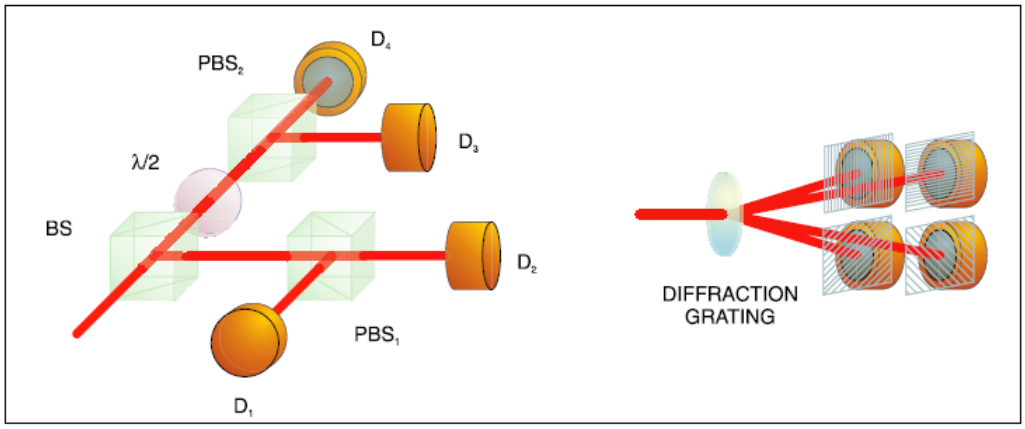

Figure 2.6: A diagram showing the schematic of the Bob module designed by Duligall *et al.* Instead of the traditional BB84 protocol setup, shown on the left, which uses beam splitters to choose a measurement basis and direct photons to the detectors, the setup uses a diffraction grating, as shown on the right. Incoming photons will be directed to one of four detectors. The detectors are each covered by a dichroic polariser, which selects the measurement basis for that detector. This image is sourced from [5].

controlled by a digital input/output card, triggered at a rate of 5 MHz. A quantum random number generator is used to generate a random key which determines which of the LED's are initiated. The LED's are arranged in a 2x2 matrix and are secured in a holder. Each LED has a dichroic sheet polariser in front of it, oriented in one of the four polarisation states used for the key distribution, i.e. 0^o, 45^o, 90^o, 135^o. The light emitted from the LED's was combined into one path using a diffraction grating. Additional spatial and spectral filters were included to reduce noise in the quantum channel.

The schematic of the Bob module differs from the traditional BB84 setup, as seen in Figure 2.6. In a standard BB84 scheme, the incoming photons would be diverted into two paths by a beam splitter. Each of these paths would correspond to the measurement of one of the non-orthogonal bases. The random basis selection gives the BB84 protocol a 50% efficiency at measuring incoming photons. Each path is further split into two by additional beam splitters, so that each state in a basis is measured at a separate detector. The Bob module proposed by Duligall *et al.* replaces the beam splitters with a diffraction grating. Incoming photons are transmitted through one of four possible paths in a 2x2 matrix. The four detectors each have a dichroic sheet polariser placed before the input. The polariser will only allow one of the four states to be correctly measured. The efficiency of Duligall's system is decreased to 25%. However, the compact size and low cost of the system justify this trade-off. The system was able to exchange a secret key of 4000 bits within an interaction time of 1 second. The system was able to operate in low light conditions but the developers intend to improve the system to be able to operate in daylight conditions.

Vest *et al.* designed a micro optic Alice module which could be integrated into compact, mobile devices, such as smartphones [103]. The module was designed using a single mode waveguide to transmit the pulses and had an intended dimension of 25 x 2 x 1 mm. The module consists of four Vertical Cavity Surface Emitting Lasers (VCSEL), triggered at a pulse rate of 100 MHz with a wavelength of 858 nm, each used for a different state of polarisation. These lasers were chosen due to the small cavity which produces a single longitudinal mode which therefore leads to a high coherence length. The lasers also had similar properties, producing pulses that are identical in terms of wavelength and spatial dimension. Using four LEDs would have been problematic in this application. The light would need to be coupled into single mode waveguides, which would be difficult due to the LEDs elliptical mode profile. The top emitting VCSEL sources were more suitable for coupling into the waveguide due their Laguerre-Gaussian intensity profile.

External wire-grid micropolarisers were used to passively set the polarisation state for each of the lasers. The waveguides were produced using a femtosecond laser writing technique which minimises birefringence effects on polarisation states. The four polarised sources were coupled into one output through the waveguide's directional couplers. The investigation into the suitability of these components showed that the waveguide exhibited low levels of birefringence but this will be compensated in future work by adjusting the distance between the arms of the directional couplers. The control of the birefringence effects could also allow the state of polarisation to be applied by propagation through the waveguide, instead of using external polarisers.

Nordholt *et al*. patented a design for a Quantum Cryptography (QC) smartcard which can exchange a secret key with a trusted authority when connected to a base, which acts as a network node [104]. The QC card can act as an authentication device, allowing the base to carry out the key distribution with the trusted authority over a fibre optic network. The QC card would be able to store the generated key after the key distribution. An alternative design of the QC card includes on-board optical and electronic components, allowing the key distribution to be carried out by the card itself, using the base as a network access point. The optical components would include polarisation components in order to carry out a 4-state BB84 protocol. It was also stated that the QC card could be powered by the base, removing the need for an on-board power supply. The compact QC card can be included in smart phones or other mobile devices.

A polarisation-based QKD system was also developed by Bunandar *et al.*, implementing QKD with semiconductor photonics [105]. Photonic integrated circuits provide a compact apparatus which will enable a more robust use of polarisation encoding in fibre networks. The dimensions of the polarisation modulator in the transmitter are in the order of millimeters, making it ideal for integration in mobile devices. The device was implemented

in a field test, first over a short 103 m fibre channel, and then over a longer 43 km fibre. The test on shorter 103 m fibre was able to generate a secret key at a rate of 950 kbps with a QBER of 2%. For the 43 km channel, the total channel loss was 16.4 dB and the secret key rate was 106 kpbs with a QBER of 2.8%. The results of this study showed that semiconductor photonics provide an improved method for high speed, polarisation encoded QKD in metropolitan networks.

Quantum Random Number Generator for phones

Apart from developing a full QKD system, research has been done to optimise specific components of a QKD setup and enable them to be integrated into existing compact systems. Sanguinetti *et al.* developed a Quantum Random Number Generator (QRNG) that can be operated on a mobile phone, using the phone's camera as a light sensor [106]. Since camera technology in mobile phones has developed to the point that cameras are now sensitive to a few photons, it was useful to exploit this feature in order to replace costly and bulky single photon detectors. Each green pixel of the camera was treated as a detector and was illuminated with a controlled light source. The number of photons measured by each pixel was converted to an equal number of electrons. This electron charge was amplified and converted into a digital signal which contributed to a binary sequence of random bits. The setup was able to generate 1.25 Gbits of random numbers from 48 frames using a computer to process the raw data. It was stated that if the raw data was processed using only the software of a mobile phone, random numbers can be generated at a rate of 1 Mbps.

2.5 Furthering the field of study

The common aspect between the systems presented in the above literature was the use of polarisation encoding for the bit generation. While the use of polarisation is a well established technology, especially for free space key exchange, it is not the simplest or the cheapest way to encode photons. Some systems used more than one light source, each connected to a different encoder, for selecting the quantum state. This increases the cost as well as the size of the device.

The use of the COW protocol presented in the following chapters improves on the currently available portable QKD systems. All polarisation related components such as polarisers, polarisation beam splitters and half wave plates are not necessary for the COW protocol, since it is only the presence of a photon that is required as the encoding. Bob's

apparatus only requires 3 single photon detectors (one for the key and two for the monitoring line) compared to the four detectors required for the BB84 protocol using a passive basis choice component, such as a beam splitter or diffraction grating. The single photon detectors are the most costly components of a QKD system.

Furthermore, Alice's device only requires beam modulation and attenuation, with electronic devices for synchronisation and post processing, making it compact and low cost. Following the development of a QRNG for mobile phones, it can be feasible to develop a low cost QKD device which can operate as a handheld device or be retrofitted into existing mobile devices. The use of the COW protocol may be ideal for this application.

3

The experimental setup and optical synchronisation

To date, the Coherent One-Way protocol has only been implemented in a fibre optic network [72]. It is not typically implemented in a free-space medium due to the turbulence effects experienced by the beam in long-range transmission. The coherence of the beam deteriorates due to the wave-front distortion caused by turbulence. The security of the key distribution process will therefore be compromised in a turbulent medium[107].

The device proposed in this thesis is designed to be used over a short-range, free space medium. The short transmission distance and enclosed environment will protect the beam from any turbulence effects and the coherence of the beam will remain uncompromised. This chapter will describe the design of the Alice and Bob modules and discuss their respective components in detail. The optical synchronisation system between Alice and Bob that was designed and built for this project will also be discussed.

3.1 Adapting the COW protocol for free space

The COW protocol scheme for fibre communication was adapted for use in free space. The optical elements remained similar to the original scheme, requiring extra components for alignment. The wavelength for the laser source and optical components was also changed to the near infrared range. Wavelengths in this range fall within an optical transmission band for free space, seen in Figure 3.1, and are therefore, best suited for atmospheric propagation. Some of the components in the Bob module retain the fibre connection in this experiment, due to the fibre coupled connection of the single photon detectors. However, a commercial system can use a channel operating only in the free space medium.

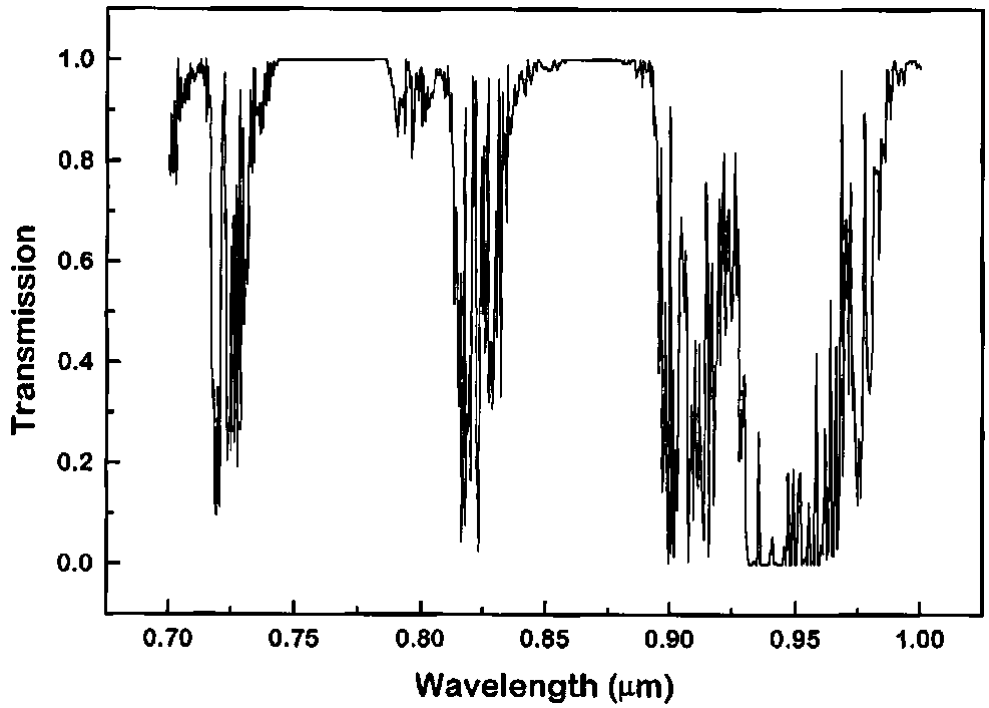

Figure 3.1: A graph showing windows of optimal transmission of different wavelengths in the atmosphere. This image is sourced from [6]

The apparatus, particularly for Alice, was designed to be compact and low cost. The COW protocol is well suited to these criteria as it is the most simple and straight forward QKD protocol to implement [3]. The apparatus will be described in two sections: The Alice module, which is the compact, consumer product and the Bob module which will be operated at a fixed site.

3.1.1 Alice Module

The Alice module is a handheld, portable device, so it is necessary to minimize the number of components included in this apparatus in order to control the size of the unit. Including fewer components also decreases the risk of Trojan horse attacks as well as malfunctions in the system [67]. Since the device will be mobile and expected to work in any environment, it is important that the components that are used are robust against temperature changes and vibrations. In order to implement the COW protocol, the following components are required for the module.

Coherent, faint laser source

A 7.26 mW laser with a wavelength of 808 nm was used for this device. As seen in Figure 3.1, the wavelength of 808 nm lies within an optical transmission band for free space and

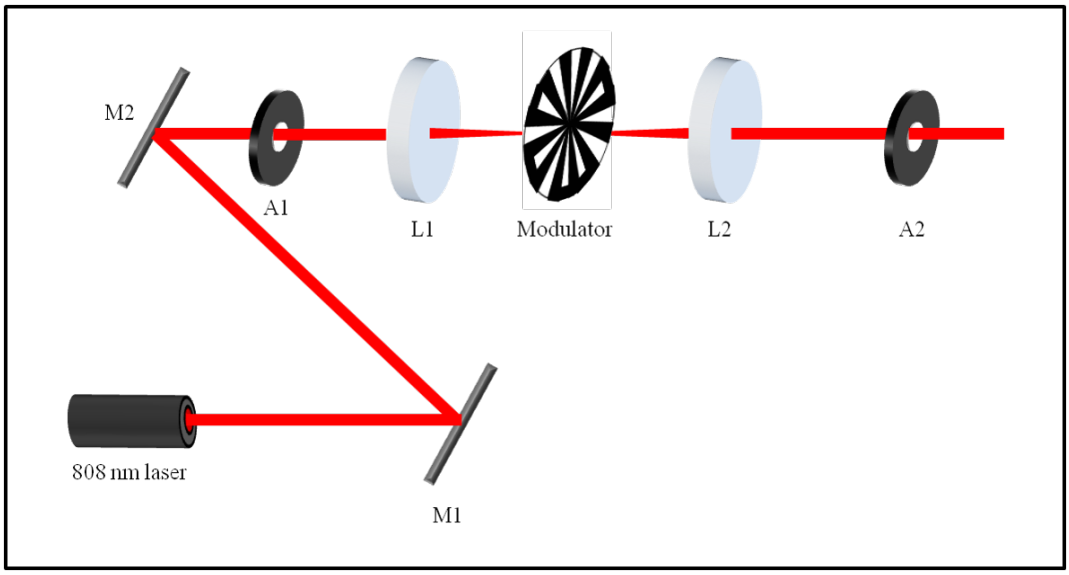

Figure 3.2: A diagram detailing the method used to align the laser. Mirror 1 (M1) and Mirror 2 (M2) were placed in the channel in order to align the laser with apertures A1 and A2. M1 was adjusted to align the beam with A1 in the near field. M2 was adjusted to align the beam with A2 in the far field. Once the beam was aligned, the apertures were removed and replaced by Alice's optics. Included in the optical setup was a lens system. L1 was used to focus the beam to a smaller diameter as it passed through the modulator in order to match the size of the modulator aperture. The modulator was placed at the focal length of L1. L2 was used to recollimate the beam at its original diameter.

ensures minimal loss of qubits during communication. A continuous wave laser with a beam divergence of 0.28 mrad was used. The distance of the free space portion of the channel from the laser source to the fibre couplers was 1.2 m so the beam divergence was negligibly small in this setup. The diameter of the beam was originally at 5 mm. The laser beam was focused to a diameter of 1 mm using a lens system so that the spot size was compatible with the modulator size. The beam was collimated after the modulator in order to minimize the divergence of the beam as it was transmitted through Bob's apparatus. The spot size was maintained throughout the optical channel since the beam did not experience any turbulence effects. The laser was aligned using two planar mirrors which were adjusted to align the beam for the near field and the far field, as shown in Figure 3.2.

Beam modulator and QRNG

The laser was directed through a mechanical modulator which determines the bit value for each pair of pulses by either blocking the beam's path or allowing transmission. An external modulator was used to pulse the laser beam instead of using an already pulsed laser source. This ensured that consecutive pulses remain coherent with each other. The

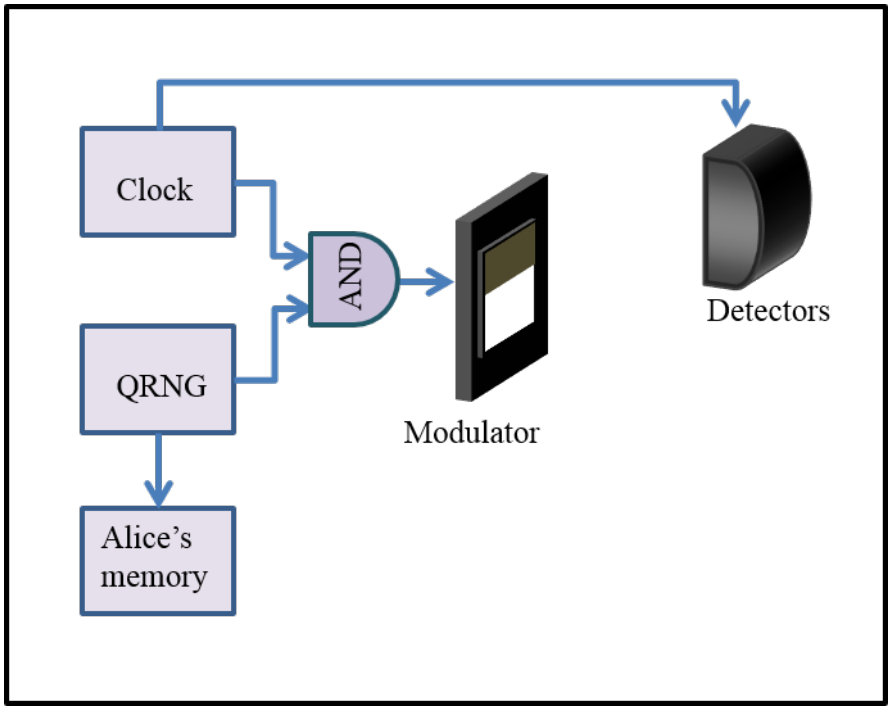

Figure 3.3: The clock rate in Alice's system must be combined with the bit string of the quantum random number generator with a logical AND gate in order to control the pulse modulator. The clock rate is also transmitted to Bob in order to synchronise the Bob's detector gate with the arrival time of a pulse. The bit string of the QRNG must be stored in Alice's memory for use during post processing.

modulator must be controlled by a quantum random number generator in order to ensure a completely random bit sequence. A liquid crystal beam modulator can be used for this application since it can operate at high speeds [108]. An opto-electronic shutter may also be used [109]. For simplicity, a QRNG was not used for this system. The modulation was done by an optical modulation wheel, discussed in Section 3.2.2.

The modulator should be controlled by a signal which is a combination of the internal clock and the QRNG. The signals should be combined with a logical AND gate so that the modulator only allows a pulse through when both the clock and the QRNG provide a bit value of 1. The QRNG signal should also be stored in Alice's memory since this will serve as her copy of the raw key. She will use this bit sequence after the key exchange for sifting and error correction. Only the clock trigger should be transmitted to Bob's apparatus in order to trigger the detector gates, forcing the detector gates to open every time there is a potential pulse entering the system. Bob's apparatus should not know what the bit value from the QRNG is, only the rate at which to expect incoming pulses and the duration for which to keep the detector gates open. This scheme is shown in Figure 3.3.

For the purpose of building a laboratory prototype, a random number generator was not used to produce the bit sequence. The modulator was designed to produce a fixed and

repetitive sequence of bits so as to recreate all bit possibilities and allow the anticipation of a bit sequence at Bob's device. This assisted with characterising the system's efficiency and visibility.

Attenuator and filters

Each pulse is attenuated by neutral density filters so that the mean photon number per pulse is one. The number of photons per laser pulse follows a Poissonian distribution [64]

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

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

$$|\langle\alpha|2\rangle|^2. \tag{3.1}$$

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

$$\langle\alpha|2\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \langle n|2\rangle, \tag{3.2}$$

$$= e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \delta_{2,n}, \tag{3.3}$$

$$= e^{-|\alpha|^2/2} \frac{\alpha^n}{\sqrt{2!}}, \tag{3.4}$$

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

$$|\langle\alpha|2\rangle|^2 = \left| e^{-|\alpha|^2/2} \frac{\alpha^n}{\sqrt{2!}} \right|, \tag{3.5}$$

$$= e^{-|\alpha|^2} \frac{|\alpha|^4}{2}. \tag{3.6}$$

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

$$|\langle\alpha|2\rangle|^2 = e^{-1} \frac{1}{2} = 0.184. \tag{3.7}$$

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

In order to maintain the security of the COW protocol, mentioned in chapter 2, the mean photon number was set to be no higher than 1. This allows for 24.4% of the pulses to contain multiple photons. Since the COW protocol is resistant to PNS attacks, the high rate of multiphoton pulses does not compromise the security of the transmission.

Additional apparatus for the Alice setup can include wavelength filters to prevent stray light from entering the channel. The filters also prevent Alice's apparatus from being interrogated by bright light by an eavesdropper who might try to gain information about the modulator [65].

3.1.2 Bob's module

Bob's module contains the receiving and measuring components for the QKD process. The components in Bob's apparatus, such as the detectors and interferometer, require an environment with a stable temperature. It is therefore necessary to house the device in a fixed location. This condition allows the apparatus to be larger than Alice's and it was, therefore, designed to hold the electronics required to synchronise Alice and Bob. Bob's module serves as an intermediary between the consumer and the vendor and will be located at a public service point, such as an ATM. The following components are required for Bob's module.

Beam splitter

The pulses received from Alice were first sorted by a beam splitter [110]. This component separated an incoming beam into two separate paths, one transmitted and the other reflected orthogonally at the surface between two joined prisms, as seen in Figure 3.4. In the first experimental realization of the COW protocol, a 90/10 beam splitter was used to siphon 10% of all incoming pulses and direct them to the monitoring line. The remaining 90% contributed to the key in the detection line. The device presented in this thesis used a 50/50 beam splitter as this was readily available for use. It also provided higher visibility in the monitoring line. The use of a 50/50 beam splitter lowered the bit generation rate of the system so it is preferable to use a 90/10 beam splitter for a commercial product.

Monitoring Line

The security of the key is determined by the measurements in the monitoring line. The monitoring line is necessary to check that the coherence of the laser beam remains intact

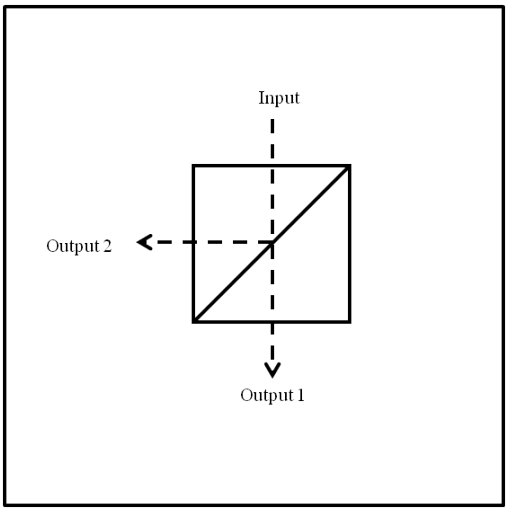

Figure 3.4: A beam splitter is able to separate incoming light into two paths. The first output is transmitted through the prisms and the second output is reflected orthogonally at the boundary between the two joined prisms.

after transmission. Once the bits from the detection and monitoring lines have been correlated to check for double clicks, the next step is to investigate whether any destructive interference was observed after the Mach-Zehnder interferometer. The dark counts of the detectors in the monitoring line has to be very thoroughly recorded. If the detector registers high readings, it must be taken for granted that it is only due to the interference of an eavesdropper and not due to any natural causes in the detector. It is therefore important that this detector is adequately cooled so that it does not get affected by thermal fluctuations resulting in high dark counts [111].

Unbalanced Mach-Zehnder Interferometer

A Mach-Zehnder interferometer is suited to measuring the phase difference between beams propagated through each of its arms [112]. In an unbalanced Mach-Zehnder interferometer, one path is longer in length than the other, causing a delay in the time of arrival of one of the beams. The delay can be adjusted to suit the experiment. For the COW protocol, the delay is set to be the precise time interval between incoming consecutive pulses, as shown in Figure 3.5.

The long path of the interferometer is set to delay a pulse, called pulse 1, by the time period between pulses so that it can interfere with the pulse behind it, called pulse 2. Pulse 1 and pulse 2 are a pair of decoy pulses, both containing a photon. Each of these pulses can randomly choose the long or short arm of the interferometer, but only one choice of configuration can lead to an interference pattern at the output of the interferometer. If pulse 1, in time bin t = 1, takes the longer path and pulse 2, in time bin t = 2, transmits

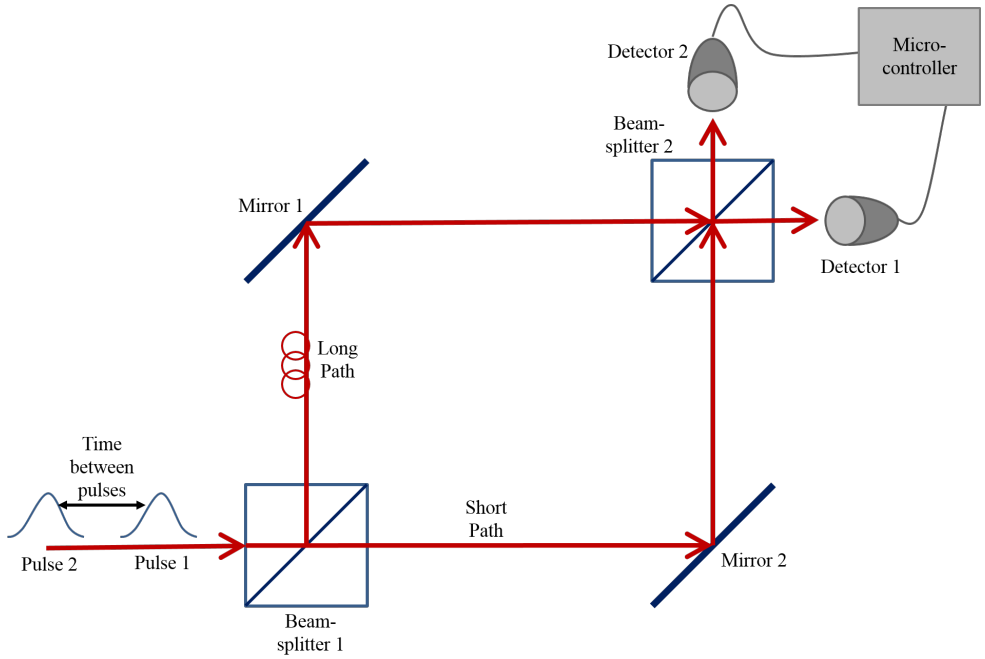

Figure 3.5: A diagram of a Mach-Zehnder interferometer which forms the monitoring line of Bob's module. The incoming pulses are randomly separated at Beam-splitter 1, choosing between the short or long path of the interferometer. Any pulses propagated through the long path will undergo a delay which will displace them by one time bin. The pulses are incident on Beam-splitter 2 and the photons are measured by Detector 1 or 2. Both detectors are triggered by the Microcontroller.

Pulse 1	Pulse 2	Result
Short Path	Short Path	Both pulses are detected separately in t1 and t2.
Short Path	Long Path	Both pulses are detected separately in t1 and t3.
Long Path	Short Path	Pulses are detected together in t2 at one detector.
Long Path	Long Path	Both pulses are detected separately in t2 and t3.

Table 3.1: Configurations of interferometer path choice for consecutive decoy pulses. The results show the detection times in time bins t1, t2 or t3.

through the shorter path, they will both reach the output of the interferometer at the same time, time bin t = 2. For coherent pulses, this will result in constructive interference at one output port of the beam splitter and destructive interference at the other. Other path choice configurations for the consecutive decoy pulses are shown in Table 3.1.

When building the interferometer, an important factor is the bit rate of the system. Since the long arm of the Mach-Zehnder interferometer needs to delay a pulse by one time bin, a slow bit rate will require a longer delay line in the interferometer. The simplest way to create a delay line was to add a length of fibre to the interferometer. Long lengths of fibre can be rolled into a compact size, as seen in the idQuantique Clavis systems [113]. At first, when building this system, a slower motor was used to rotate the optical modulation wheel, creating pulses 10 ms in width with an additional 10 ms in between pulses. The interferometer would then have to have a delay line corresponding to 20 ms. Using the speed of light in fibre as 2×10^8 m/s, the delay line would need to be 4000 km. This length of fibre is impractical, so the motor was replaced with a faster model. The faster motor produced a pulse rate of 100 μs, corresponding to a delay line of 20 km. This is a practical length for fibre QKD and the channel loss can be characterised and included when calculating the visibility of the system.

The wavelength of the single photon source used in this system was 808 nm. This wavelength, while optimal for free space communication, experiences high attenuation and dispersion in fibre [85]. The attenuation of 3 dB/km for 808 nm wavelength in fibre will set an upper bound for the length of the fibre used in the interferometer, and therefore, the lower bound for the speed of the optical modulator. The upper bound for the modulator speed will be dependent on the dispersion of the 808 nm light in fibre. Dispersion causes pulse broadening and a fast pulse rate will result in pulses broadening into other time bins [84]. The dead time of the single photon detectors also places an upper bound on modulation speed. The rate of incident pulses on the detector must be greater than the dead time of the detector. A faster modulation rate will cause incident photons during the dead time and these pulses will not be measured, resulting in a higher loss rate.

Single photon detectors

A single photon detector was placed at the end of the detection line in order to receive the bits for the key. The outputs of the interferometer in the monitoring line also require single photon detectors in order to measure the coherence of the beam [111]. The detectors are usually the most specialised and expensive component in the QKD module. Detection efficiency varies over the type of detector used and the operating wavelength of the transmission. An InGaAs SPD has a low quantum efficiency of approximately 10% for fibre telecoms wavelengths [114], whereas silicon detectors used for free space wavelengths have an efficiency of approximately 65% [111].

The SPCM-AQR-14 silicon Single Photon Avalanche Diode (SPAD) from Perkin Elmer was used to detect the single photons in this setup [9]. The SPAD uses a PN junction which is subject to high reverse voltages. Incident light excites electrons and causes them to move into the conduction band, forming electron-hole pairs. The electron-hole pairs generated in the neutral depletion region will drift to their respective electrodes. Electron-hole pairs with enough energy can create additional electron-hole pairs, creating an avalanche effect. The large charge build-up at the electrodes creates a current corresponding to the incoming light. The SPAD operates with a high reverse bias voltage, above the breakdown voltage, as shown in Figure 3.6a). With a high reverse bias, the electric field is high, so that a single charge carrier can trigger an avalanche [115]. Figure 3.6b) shows the scheme of a SPAD.

SPAD's are susceptible to afterpulsing effects [111]. Once an avalanche event occurs, the detector must be quenched so as to remove all electrons which could unduly trigger another event [116]. Each detector must be set with an appropriate dead time after a successful measurement to allow enough quenching time [117]. If the dead time is too short, it will cause an increase in erroneous measurements but a long dead time will decrease the overall key generation rate of the system since the detector will miss a large portion of incoming photons. The dead time must, therefore, be optimised for the channel length and trigger rate.

All single photon detectors have a dark count rate dependent on the operating temperature of the device [114]. Dark counts occur due to thermal tunnelling and will trigger an avalanche without the presence of a photon. The detectors must be kept in a temperature-controlled station in order to prevent excess dark counts due to thermal tunnelling. For the silicon detector used in this setup, operating temperature was between 5 ^{o}C and 40 ^{o}C [9]. The dark counts can therefore be kept to a minimum with standard air conditioning for the room.

The dark count rate of a detector must be measured before the detector is used in the system. This value must be subtracted from the overall count rate measured during the key sharing process as it contributes to the QBER. Since QBER is dependent on detector dark counts, a high signal-to-noise ratio must be maintained for the transmission. A high rate of dark counts will force a necessary decrease in the channel length in order to keep the transmission losses at a minimum [118].

In order to reduce external noise in the channel, the detector gate must be triggered to open precisely for the arrival of the pulses from Alice. If the gate is open for an extended time, it allows stray light to enter the detector, which is especially prevalent in a free space channel or a fibre supporting many communication channels. The electronics required to synchronise the arrival of the pulses with the detector gate were housed with Bob's apparatus and will be discussed in the following sections of this chapter.

The detectors used for this system were fibre coupled. The free space channel had to therefore be coupled into fibre before being measured by the detectors. The fibre couplers had to be very precisely aligned in order to receive all the incoming pulses. An error in alignment will cause a significant loss in measurements, especially when the mean photon per pulse is low. The beam was coupled into multimode fibre, since this type of fibre has a larger core diameter than single mode fibre. With a larger area to receive the light, multimode fibre was more efficient in collecting the incoming light. The coupling efficiency decreased optical power by approximately 56%. However, this was preferred to the single mode fibre which was difficult to align and only coupled a negligibly small amount of light.

Similar to Alice's setup, Bob needs additional spectral and spatial filtering to remove excess noise in the channel. An accurate gating control for the detector serves as the temporal filtering for the system. Spatial filtering can be in the form of an aperture placed at the entrance to Bob's device. This will prevent stray light from entering the system at oblique angles. A wavelength filter can be used to block any wavelengths apart from that of the single photon source from entering the apparatus. This will be of use if the apparatus is housed in a room that is illuminated with fluorescent lighting. The wavelength filters will prevent the room's light from entering the quantum channel.

Figure 3.7 shows a complete diagram of the Alice and Bob modules for a generic COW protocol implementation and how they are linked.

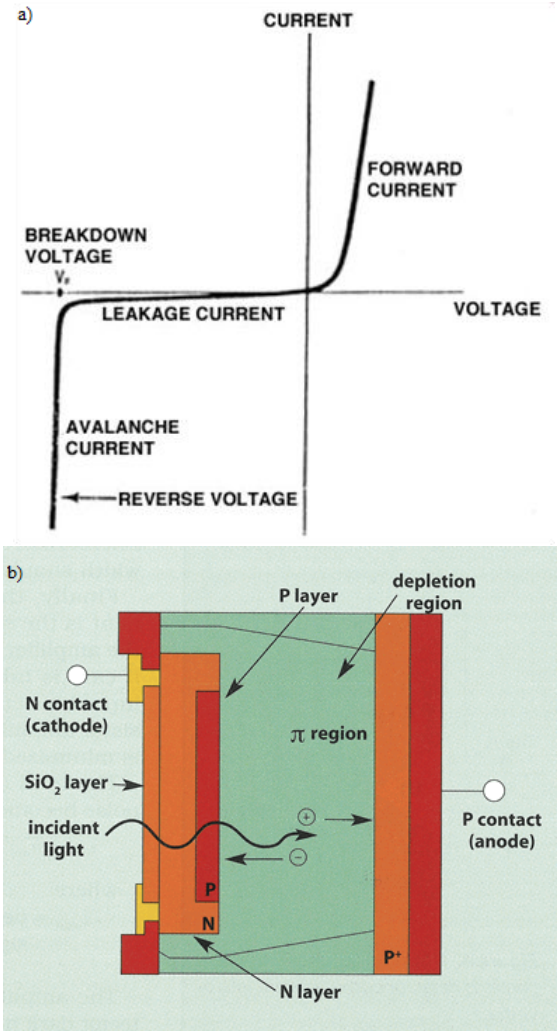

Figure 3.6: a) A graph showing the reverse bias properties of a SPAD. The detector operates above the breakdown voltage, so that electron-hole pairs accelerate in the strong electric field created by the high reverse voltage. The presence of a charge carrier will cause the current to rise rapidly, leading to a detection. The SPAD must then be quenched by lowering the voltage in order to minimise the current. The voltage is then raised above the breakdown voltage in order to accept the next photon. Image a) was sourced from [7]. b) A diagram showing the schematic of a silicon SPAD detector. Any light incident on the detector will excite electrons, causing electron-hole pairs in the depletion region. The electrons and holes each build up at their respective electrodes. The electron-hole pairs with enough energy can create additional electron-hole pairs, resulting in an avalanche. The intensity of the incoming light therefore corresponds to the current produced by the charge build up at the electrodes. Image b) was sourced from [8].

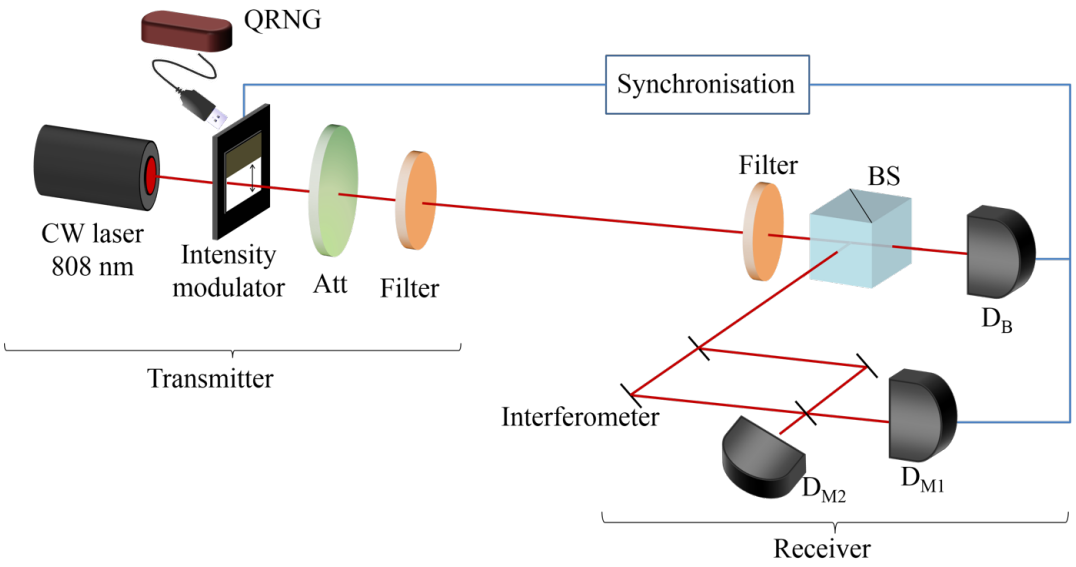

Figure 3.7: A diagram showing a generic scheme of the COW protocol adapted to free space. The transmitter (Alice) module consisted of a 808 nm laser for the single photons which was pulsed by an intensity modulator. The pulses were attenuated so that the mean photon number per pulse was one. The quantum random number generator supplied Alice's key to the modulator and the clock regulated the frequency of the system. The receiver's (Bob's) module consisted of a beam splitter which separated the detection line and the monitoring line. The detection line consisted of a single photon detector, D_B, and the monitoring line consisted of a Mach Zehnder interferometer. The outputs of the interferometer were measured on single photon detectors, with D_M indicating a break in the coherence of the beam. Both Alice and Bob have filters in the modules to reduce stray light entering the quantum channel. Alice's filters also have the added function of preventing an eavesdropper from interrogating the module with bright light in order to gain information about the modulator.

3.1.3 Post processing

Once Bob has received the stream of pulses from Alice, they must communicate via a classical, public channel in order to sift the raw key. The sifting consists of two steps [3]:

• Bob informs Alice when the detectors in the monitoring line have clicked so that both parties may discard these events from the key. The information being transferred will be in the form of time bin information of the relevant bits to discard.

• Alice must also inform Bob about the time bin information of the decoy states, so that these events may also be removed. The remaining bits are considered to have been measured in the detection line and will therefore contribute to the sifted key.

At this point, the sifted key must undergo error correction and privacy amplification in order to be secure for use as a cryptographic key.

Both the synchronisation and single photon transfer are done optically over a free space channel, which means that there is no physical connection between the Alice and Bob

modules. The post processing can also be done via a classical optical connection, e.g. the synchronisation light source and photodiode, since binary data can easily be transmitted through optical systems.

Bob will also need to communicate with Alice and will therefore, also need a light source and Alice will need a photodiode detector. Alice will need to translate the optical signals from the photodiode to binary information and will need to store and access information. It is therefore necessary for Alice to have an embedded system required to receive an optical signal, similar to Bob's synchronisation electronics. The sequence from the QRNG as well as the sifting communication from Bob must be stored in an on board memory during the key exchange process. This information will eventually be replaced by the final key after the exchange.

3.2 Synchronisation of the system

3.2.1 The synchronisation of the commercial product

An optical signal was used to synchronise the Alice and Bob modules before the key transfer could begin. The advantage of using an optical signal is that the Alice and Bob modules do not need to be joined by any cables or sockets. A light source separate to the single photon source should be used for the synchronisation since the single photon laser will be automatically aligned with the attenuator and will be directed to the single photon detectors. Since the efficiency of the quantum channel is lower than 100% it will be easier to measure the synchronisation source with another, classical photo diode, therefore making it appropriate to use bright light for the synchronisation process.

Synchronisation can be established before the QKD transmission begins or the synchronisation can be done in real time. Both of these methods were tested for the system. In order to establish the synchronisation before the quantum transmission, the modulator was set to pulse the synchronisation source according to Alice's clock rate. Bob passively measured the incoming signal and calculated the pulse width and frequency from the measurements. The synchronisation process could then be preprogrammed to last for a set length of time and immediately after, Alice switches to using the single photon source and Bob begins measuring with the single photon detectors which are gated with the frequency established during synchronisation.

This method was initially used for the proposed system. Due to electro-mechanical errors, such as slipping of the motor or inconsistent voltage applied to the motor, a phase shift of the synchronisation signal was observed. Any errors in the phase of the synchronisation

signal could result in the detector gate opening at the incorrect time, leading to losses in the key exchange process. An electronic modulator was better suited to this synchronisation method and may be implemented in the commercial version of the system. For the lab prototype, a real time synchronisation method was chosen.

For real time synchronisation, Bob received the signal from the synchronisation source before each potential single photon pulse. The synchronisation signal must only indicate the clock rate and must in no way give any information about the QRNG. This approach requires less programming in Bob's device since the detectors are passively gated from Alice's incoming signal.

Both the pre-synchronisation and real-time synchronisation techniques allow for Bob's device to be used at any frequency allowed by the components. Since the operating frequency is set by Alice, Bob's device can be used with different models of the Alice module, operating at different frequencies.

3.2.2 The modulator and synchronisation system used for the lab prototype

For the purpose of this thesis, we opted to use a simpler optical chopper wheel as the modulator, which provided a synchronisation signal in real time to the single photon detectors. This modulator was controlled by a motor and the rotation speed of the modulator could be varied with the voltage supplied to the motor. The modulator could not be controlled by a random number generator but was instead designed to repeat a set sequence of bits 1001110110 (which correlated to 1 0 decoy 0 1 in the COW protocol encoding). While this modulator may not be appropriate for a commercial system, it was adequate for use in the lab. For the purpose of a proof of principle setup, the wheel still allowed a complete evaluation of the quantum bit error rate, which is one of the key criteria of a QKD system. The repetitive bit sequence allowed the testing of all possible bit combinations (10 01 11). By anticipating the bit sequence arriving at Bob's detectors, it became simpler to characterise the system's efficiency. It was also unnecessary to have a bit storage device in Alice's apparatus since there was no need to compare the QRNG sequence to Bob's measurements.

A green LED with a wavelength of 532 nm was used as the synchronisation light source. This wavelength was chosen because it did not add noise to the near infrared quantum channel. The light from the green LED was spatially filtered through an aperture and also transmitted through a lens to focus the spot size so that the beam was of the same dimension as that of the 808 nm laser.

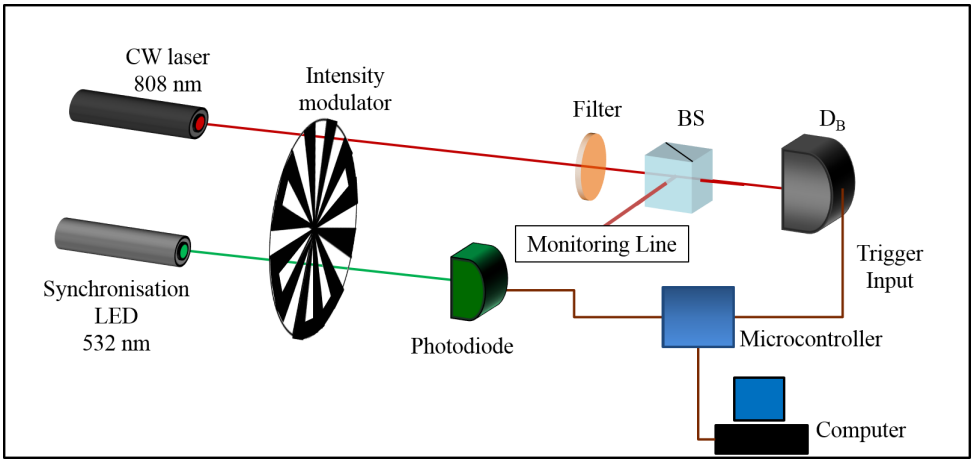

Figure 3.8: The 808 nm laser and green LED were both modulated by an optical chopper wheel. The laser was positioned at the outer edge of the wheel and was modulated by beam blockers on the wheel to form a fixed encoded sequence. The green LED was positioned near the center of the wheel and was not affected by the encoding. The green LED was measured by a photodiode and the signal was processed by a microcontroller which transmitted the resulting trigger signal to Bob's detectors. The microcontroller was connected to a computer which was used to update the microcontroller software and store incoming measurements.

The green LED was positioned so that the beam was modulated near the middle of the wheel and the 808 nm laser was positioned to be modulated at the outer edge of the wheel. This positioning creates similar pulse modulation in both beams while allowing the primary laser to undergo bit encoding independent of the green LED. Some of the wheel apertures were blocked at the outer edge to create a bit sequence to encode the 808 nm laser. By blocking the beam, the pulse allocated for that time bin was empty and by allowing the beam through, a pulse containing a photon is transmitted through the system. The green LED signal was unaffected by the bit encoding since it was positioned on another part of the wheel, and it continued to produce a steady pulse frequency. The green LED was measured by a photodiode and the signal was processed by a microcontroller. The microcontroller used for this experiment was a ATMEGA328P with 2 kb SDRAM, 32 kb flash memory and a 16 MHz clock [119]. The microcontroller used the measurement of the green LED to produce a trigger signal which gated the detector. This is shown in Figure 3.8.

The positions of the 808 nm laser and synchronisation LED were finely adjusted so that the LED was blocked as the 808 nm laser was transmitted through Bob's apparatus, reducing any stray light in the detectors. The synchronisation signal was, therefore, inverted in order to trigger the detectors' gates to receive the laser pulses. The alignment of the synchronisation source relative to the single photon source had to also be very precise. The sources had to be exactly anticorrelated so that the green LED was off when the red laser was on and vice versa, as shown in Figure 3.9. Once aligned, this configuration

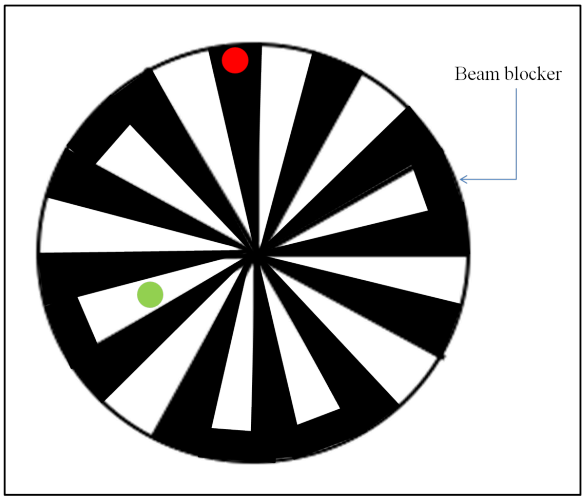

Figure 3.9: The relative positions of the red and green light sources were anticorrelated on the modulation wheel. When the 808 nm laser was blocked, the green LED was allowed through. This configuration prevented excess light from entering the quantum channel. The trigger was therefore switched on when the green LED was blocked. Additional beam blockers were also placed in the path of the 808 nm laser in order to provide a bit sequence. Since the green LED was aligned closer to the center of the wheel, it was unaffected by the beam blockers.

could not be adjusted as it would have compromised the synchronisation of the system.

In order to precisely set the relative positions of the laser and the green LED, a temporary photodiode was installed to measure the laser. Both photodiodes, for the laser and LED, were connected to the microcontroller so that they could be simultaneously monitored, as shown in Figure 3.10. Since the 808 nm laser was in a fixed position, aligned with the other components, the position of the green LED was adjusted until the voltage outputs associated with each photodiode were inversions of each other. The output voltages of both photodiodes were monitored on an oscilloscope, seen in Figure 3.11. The position of the green LED was finely adjusted so that it was measured by the microcontroller before the arrival of the 808 nm laser. This time delay allowed for the microcontroller to measure and invert the signal from the green LED and transmit the trigger signal to gate of the single photon detectors.

3.2.3 Description of the electronics and software used for the synchronisation

The photodiode used to detect the green synchronisation LED was connected to a circuit to receive and digitise the signal and transmit the digital output to the microcontroller. The circuit was also connected to its own power supply, which together formed a detector for the green LED, as shown in Figure 3.12.

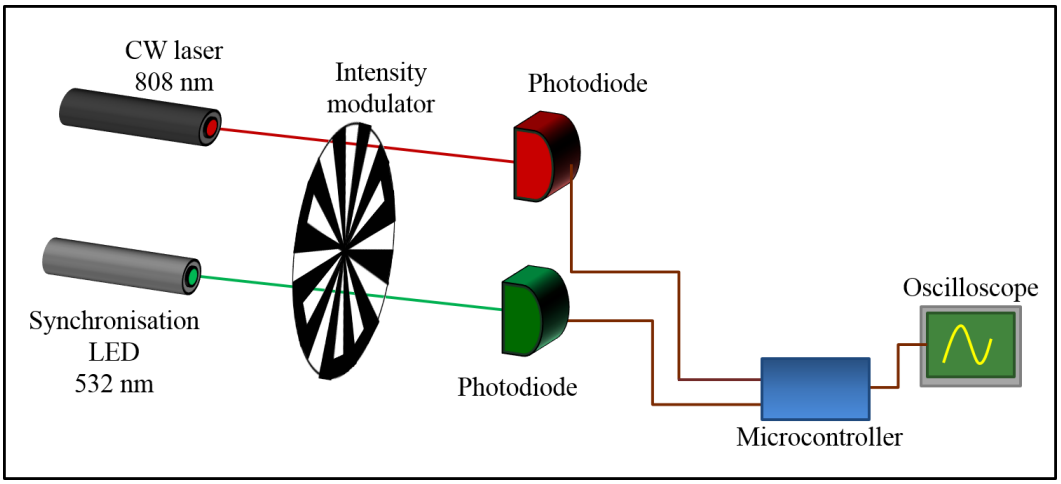

Figure 3.10: A temporary photodiode was added into the system to precisely align the relative positions of the 808 nm laser and the green LED. The signals from both photodiodes were measured by the microcontroller and displayed on an oscilloscope.

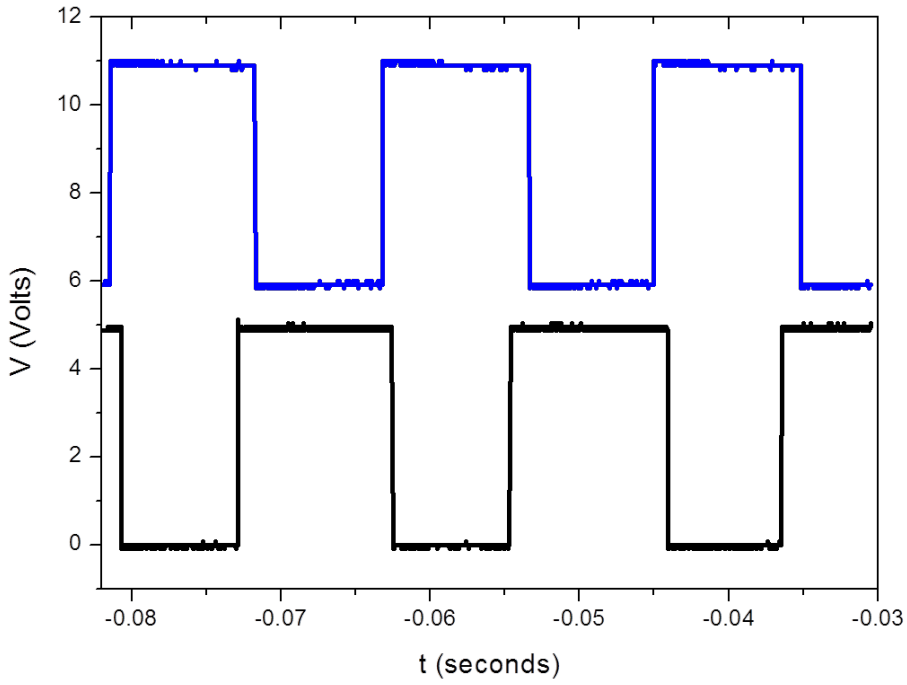

Figure 3.11: The blue and black lines represent the voltage output from the measurement of the 808 nm laser and the green LED respectively. The voltage signals were processed through an inverting comparator, hence, both are inverted in this figure. In this graph, the trigger signal and 808 nm laser are measured when the black line (green LED) is high and the blue line (808 nm laser) is low. The LED was positioned so that it was measured before the 808 nm laser. This compensated for the time delay between the measurement of the LED and the trigger pulse being received at the detector gate. Both sets of data had voltage measurements between 0 V and 5 V. For illustrative purposes, the 808 nm pulses are displayed above the LED pulses.

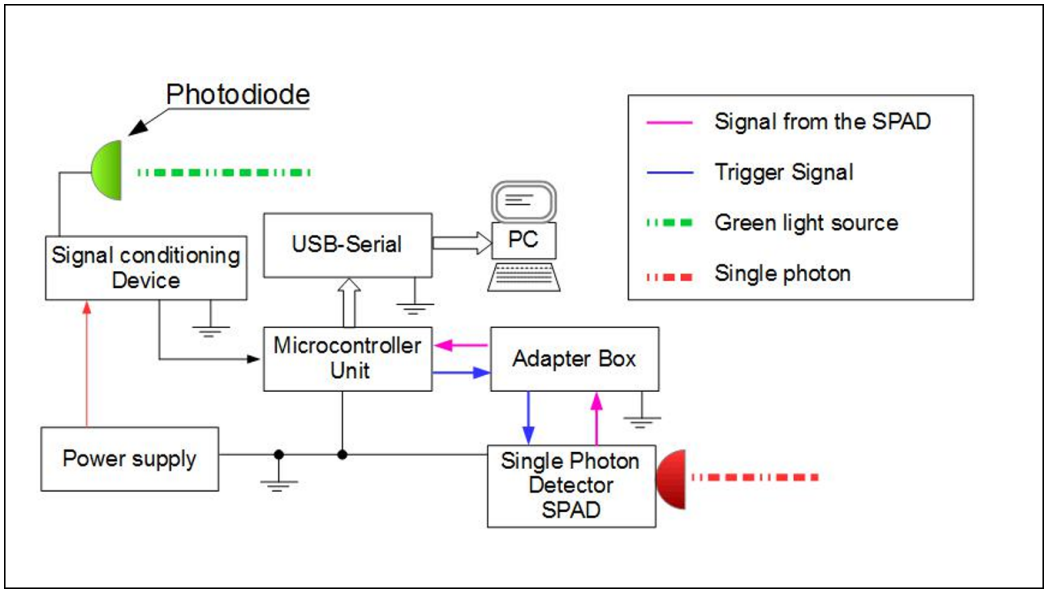

Figure 3.12: A block scheme of the electronic connections used to synchronise Alice's module with Bob's detectors. The components shown in this diagram were all housed in Bob's unit. The photodiode which measured the green LED transmitted its signal to the microcontroller which then triggered the detectors via the connection panel on the adapter box.

All connections made to the digital ports of the microcontroller were through a panel of coaxial connectors, shown in Figure 3.13. The connections on the panel included the incoming measurement of the green LED, the outgoing trigger signals for the single photon detectors and the incoming measurement signals from the single photon detectors. The microcontroller was connected to a computer via a usb port. An image of the full lab setup is shown in Figure 3.14, showing the optical setup and the synchronisation subsystem.

The programme that was operated from the microcontroller processed the signal from the synchronisation source and translated it into a trigger signal for the single photon detectors. The programme accepted a measurement from the synchronisation photodiode and if the value was a logical high, the program did nothing, keeping the detector gates closed. If the value was low, the detector must get ready to accept a pulse. The programme commanded the microcontroller to send a gating signal to the detector and immediately read the output measurement of the detector. After one measurement was recorded, the gate of the detector was forced to close so that the detector may dissipate and prepare for the next measurement. Closing the detector gate also prevented stray light from entering the detector, resulting in noisy measurements.

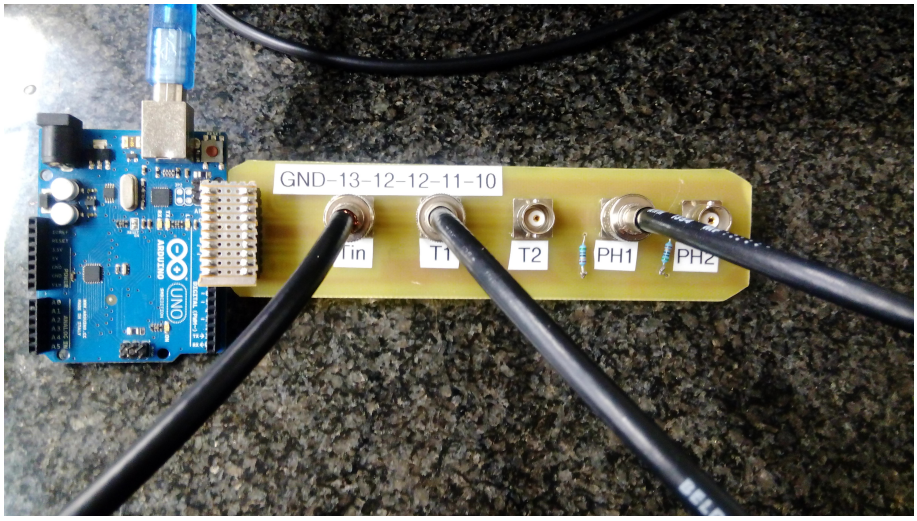

Figure 3.13: A photo of the panel of coaxial connections on the adapter box which linked the green LED, trigger signal and detector signal to the microcontroller.

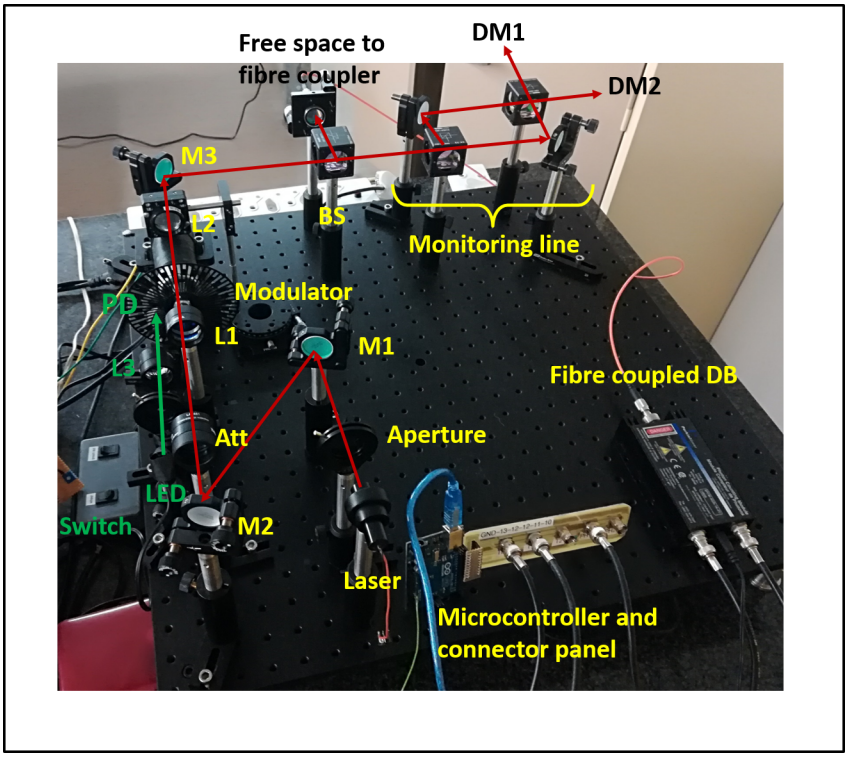

Figure 3.14: An image of the full setup showing the optical setup and synchronisation subsystem. The path of the 808 nm laser is shown with the red line. The laser passes through an aperture, mirrors M1 and M2, the attenuator Att, lens L1, the modulator wheel, lens L2 and mirror M3. At the beamsplitter BS, the path splits between the free space to fibre coupler which leads to the detection line detector DB and the monitoring line. In this image, an example of a free space Mach-Zehnder interferometer is shown as the monitoring line. The outputs of the interferometer should lead to detectors DM1 and DM2 which will be developed in the future.

Trigger	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
808 nm laser	0	0	1	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0
Measured bits	0		1		1		0		1		1		1		0		0		1	
Key		1				0				D				0				1		

Table 3.2: Time correlated measurements by the respective photodiodes of the 808 nm laser and the green trigger LED and the resulting bit sequence. The measured bit sequence was separated into pairs. A consecutive set of bits 0 and 1 result in a key bit 1. A consecutive set of bits 1 and 0 result in a key bit 0. A consecutive set of bits 1 and 1 result in a key bit Decoy.

The programme enforced the condition that the trigger should not be sent to the detector again until the synchronisation signal was switched to high and back to low again. Since the pulse width used in the system was much larger than the gate width of the detector, the detector may attempt several measurements within one modulated pulse. The detector must take just one measurement per pulse and hold the recorded value for the duration of that time bin. If the detector took multiple measurements, it might only transmit the last measurement of that pulse to the microcontroller and if the last measurement missed the single photon, the measurement will be regarded as loss. This is shown in Figure 3.15.

The programme recorded the measurements for 100 time bins, thus looping through the events of 100 synchronisation pulses and the results were held in the microcontroller's memory. After 100 cycles, the results were transmitted to the computer via the usb cable. The data transmitted to the computer was the raw key which was ready to be sifted via a classical connection between Alice and Bob. A logic flow chart for the synchronization software is shown in Figure 3.16 and Appendix A1 shows the software code used for synchronisation.

A fixed, ten bit encoding for the 808 nm laser was added to the wheel with a repetitive sequence of 0110111001 and a correlation measurement was done using the temporary photodiode in order to verify the accuracy of the synchronisation system. The results in Table 3.2 show that the green LED provided a stable trigger signal of 1010101010. The bit encoding was measured whenever the trigger had a value of 1, which corresponded to the green LED being blocked by the modulator. The measured bits therefore show that the bit encoding was preserved while remaining synchronised with the trigger. For the COW protocol, two measured bits form one bit in the cryptographic key. Using equations (2.1) and (2.2), the resulting key was 1001. The decoy signal which was measured would only be used to verify the security of the transmission and would be discarded from the key.

As mentioned, the microcontroller stored 100 measurements and transmitted them collectively to the computer for storage. An error occurred after every 100 bits, resulting in

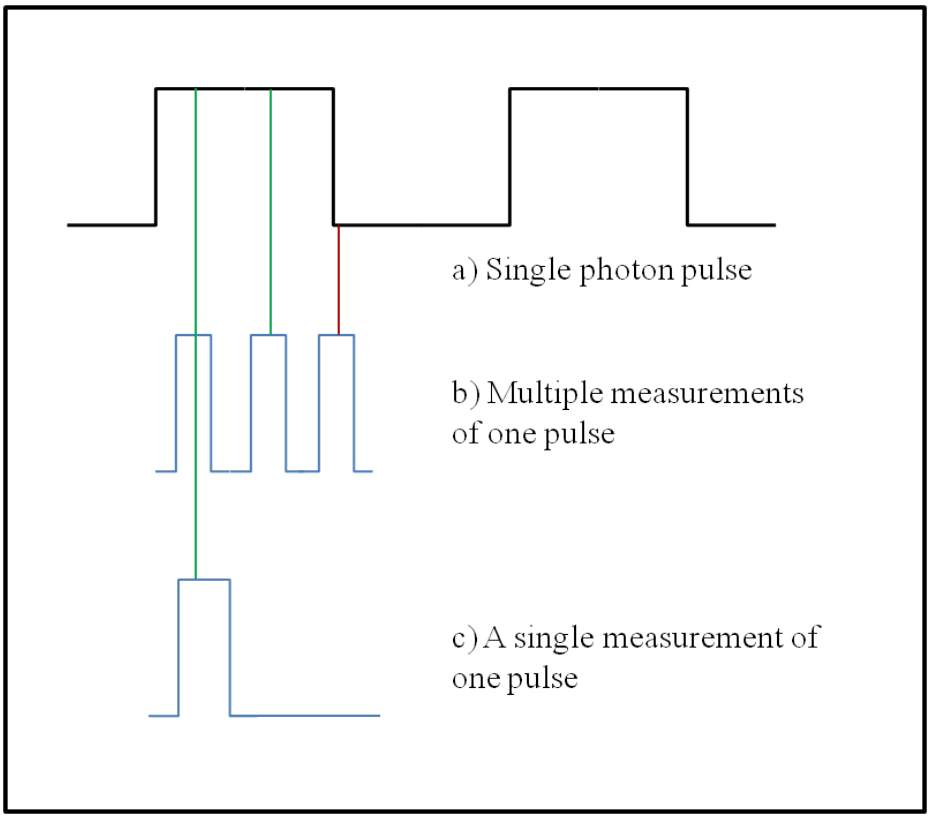

Figure 3.15: This figure shows the necessity of allowing just one detector measurement per photon pulse. a) shows the width of the photon pulse incident on the detector gate. b) shows 3 consecutive measurements made on the pulse since the trigger was not switched off in this time. The first two measurements were able to potentially measure the photon (shown in green) but the third measurement mostly falls out of range and will return a value of zero (shown in red). Since only the last measurement is recorded, the information in this photon will be lost. c) shows the scenario where the trigger is switched off once one measurement is made, allowing the value of the photon to be held by the programme.

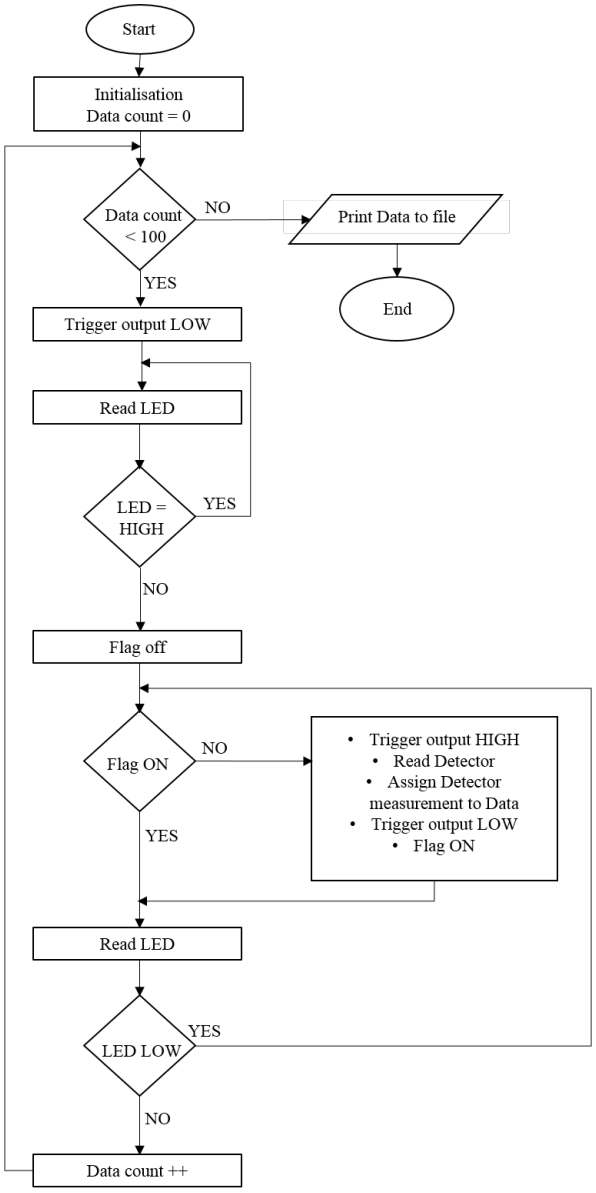

Figure 3.16: The logic flow chart of the programme illustrates the processes behind the synchronisation system. The microcontroller stored the detector data in an array of 100 data points and transmitted the data to the computer once the programme processed 100 loops and the array was full. The logic diagram showed that the green LED was measured and when it output a logical LOW, the detector was triggered and a measurement was accepted from the detector. A flag was used to check that only one detector measurement was allowed per synchronisation pulse.

an empty time bin with no bit recorded. This was due to the transmission time taken by the microcontroller in order to transmit the stored data to the computer. The microcontroller would not record any measurements during this time. The effect of this error was minimised by increasing the measurement array to 200 bits and identifying and removing the extra bit. A microcontroller with a larger internal storage, an example of which is proposed in [120], would be able to store a larger array of measurements before needing to transmit them to the computer, therefore minimising the error further.

3.3 Working in the single photon regime

Once the system was precisely aligned and synchronised, the temporary photodiode was removed and replaced by the single photon detector in the detection line. The 810 nm laser was also attenuated to contain an average of one photon per pulse.

Since the single photon detectors were fibre coupled, free-space-to-fibre couplers were added to the system and aligned at the end of the detection line and the monitoring line. The characteristics of the quantum channel are detailed in the next chapter.

4

Characterisation of the detection line

Once the Alice and Bob modules have been synchronised, the system is ready to exchange a key. In order to determine the length and security of the key, it is important to first characterise the key exchange. The expected key generation rate and error rate should be established before transmission so that any irregularities in the key exchange can be identified during post processing. This section will discuss the characterisation of the system as well as the software used to sift the raw key.

The defining criteria for characterising the performance of a QKD system include the secret key generation rate as well as the Quantum Bit Error Rate (QBER) generated by the apparatus [121]. The secret key generation rate is indicative of the speed of the system. A faster key generation rate will enable the encryption of larger files, such as videos, in a shorter time. The QBER measured during the sifting procedures of the protocol indicate the number of errors in the sifted key and is an indication of the security of the key. It is vital that the QBER of the key does not exceed its theoretical prediction since all errors in the system must potentially be attributed to the interference of an eavesdropper. Therefore, if the QBER is high, it is automatically assumed that the eavesdropper possesses a high percentage of the information and the key distribution must be cancelled.

For the COW protocol, the security of the key is verified by measuring the coherence of consecutive photon pulses by monitoring the visibility of the interferometer in the monitoring line. The presence of an eavesdropper cannot be detected in the detection line since there is only one measurement basis used by Bob. The eavesdropper would just have to measure for the presence of a photon and recreate the result to transmit to Bob, as in the intercept-resend attack. There would be no detectable differences in this signal, making the role of the monitoring line imperative. For this protocol, QBER measured from the detection line gives an indication on the noise in the channel or dark count rate of the detector [121].

4.1 Factors contributing to the key generation rate

The raw key generation rate can be predicted by considering the factors that may deteriorate the quantum signal. The potential key generation rate starts with the pulse rate of Alice's modulator and this value is then decreased depending on the efficiency of the quantum channel and optical components. The probability of detecting a photon in Bob's detectors is given by $1 - e^{-\mu T \eta}$ [71], where μ is the mean photon number per pulse, T is the transmission coefficient of the channel and η is the quantum efficiency of the single photon detectors. In the limit $\mu T \ll 1$,

$$1 - e^{-\mu T \eta} \approx \mu T \eta \,. \tag{4.1}$$

The mean photon number is set by the faint laser source and variable attenuators. The visibility of the channel is dependent on the attenuation caused by each optical component and will provide the transmission coefficient for the system. The detector efficiency indicates how many photon pulses that reach the detectors are actually measured. Also consider that for the COW protocol, two pulses contribute to one qubit, therefore, the theoretical prediction for the raw key generation rate can be expressed as [5]:

$$\text{Raw Key Generation Rate} = \frac{A}{2} \mu T \eta \,. \tag{4.2}$$

The Alice modulator rate, A, is halved since two pulses contribute to one qubit and this term is multiplied by the probability of detecting a photon in Bob's detectors. This expression does not include the portion of pulses that are assigned as decoy states. Therefore, to simplify the characterisation of Bob's detection line, no decoy pulses were inculded with Alice's originial key for this experiment. Note that when measuring the raw key, the expected measurement will be higher than the theoretical value due to the presence of dark counts and channel noise, which will need to be removed during error correction. Each of the factors in this expression will be discussed in detail.

4.1.1 Modulator rate

The initial rate of pulse generation from Alice is the starting point for the calculation of the key generation rate. The continuous wave laser was externally modulated by a motorised optical modulation wheel. The rotational speed of the wheel was controlled by varying the voltage applied to the motor. The green synchronisation LED and photodiode, mentioned in Chapter 3, were used to monitor the rotational speed of the modulator. The output

of the photodiode was digitised and transmitted to the co-axial connector panel, which was then interfaced with the microcontroller. In order to check the modulation rate, the digitised photodiode signal was displayed on an oscilloscope. With an input of 25 V to the motor, the modulator was able to create a pulse width of 100 μs with a duration of 100 μs between pulses. The modulation rate for the Alice module is therefore 5 kHz.

4.1.2 Mean photon number

When using a faint laser source for QKD implementation, an attenuator is used to decrease the power of the optical signal so that each optical pulse contains an average of one photon. For this experiment, the attenuation of the laser beam was achieved using neutral density filters. The components in Alice's module also provide a small factor of attenuation and this will also be considered in the building of the pseudo-single photon source. The initial laser power was 7.26 mW which had to be significantly attenuated in order to produce the power of a single photon per laser pulse. The laser beam was first transmitted through an aperture which assisted in decreasing the power of the laser to 0.489 mW.

The required power of each laser pulse, in order to obtain the equivalent power of a single photon per pulse, is calculated as [122]

$$P_{\text{Watts}} = \frac{hc}{\lambda t}, \tag{4.3}$$

where h is Planck's constant, c is the speed of light, λ is the wavelength of the laser and t is the period of the laser pulse.

For this experiment, the wavelength of the laser source was 808 nm and the period of each pulse was 100 μs. Substituting these values, and $h = 6.626\times10^{-34}$ m^{2}kg/s and $c = 3\times10^8$ m/s into equation (4.3), the power of each laser pulse was required to be 2.46×10^{-15} W in order to obtain an average of one photon per pulse. The neutral density filters used to attenuate the pulses were categorised by their fractional transmittance of incoming light [123]. A combination of 0.01% filters were combined to create an attenuator for the laser.

After the faint laser source in Alice's module, the only other necessary optical component is the modulator. The modulator does not affect the attenuation of the pulses while it is open, and therefore, does not affect the mean photon number of non-empty pulses. In cases where a laser with a wide wavelength bandwidth is used, a filter is needed to narrow the bandwidth. This will prevent noise in the channel since the detector will be able to measure a range of wavelengths. The filter will lower the power of the laser and this factor can be combined with the attenuation of the laser pulses.

In this setup, two mirrors were used in order to align Alice's laser beam. The mirrors did not have perfect reflectivity and a portion of the laser beam was transmitted through the mirrors. This loss was measured and it contributes to the attenuation of the beam. A lens system was used to decrease the spot size of the beam as it transmitted through the modulator. The lenses reflected a portion of the beam and, therefore, contributed to the attenuation .

The attenuation obtained from the neutral density filters and the other components in Alice's module collectively lowered the optical power from 0.489 mW to 2.46×10^{-15} W, creating a pseudo single photon source at the output of Alice's module. The details of the attenuation by each of Alice's components is shown in Figure 4.1.

The COW protocol is resistant to photon number splitting attacks and therefore, the laser pulses did not need to be attenuated to have a mean photon number less than one, as is common which most QKD protocols. The mean photon number per pulse remained at one and, therefore, did not affect the key generation rate of the system in equation (4.2).

4.1.3 Transmission coefficient of the system

The transmission coefficient of the system is a combination of the transmission of the channel and the components in Bob's module, until the input port of Bob's detectors. As mentioned in the previous section, the attenuation from Alice's components contribute to the single photon source. The attenuation caused by the channel between the two modules becomes especially prevalent in long distance communication, but since this device is meant for short range communication, the decrease in optical power due to the channel between Alice and Bob was not significant.

The components in Bob's apparatus contributed significantly to the decrease in the transmission coefficient. The beam splitter in Bob's apparatus caused the first substantial decrease to the number of measured photons. The device presented in this thesis utilised a 50/50 beamsplitter, due to it's availability. Upon measuring the outputs of the beam splitter, it was noted that the split in optical power is not perfectly at 50% for each output port. The paths were instead measured to be 48.8% for the detection line and 46.4% for the monitoring line. The 5% loss from the beam splitter can be attributed to reflection. The factor contributing to the transmission coefficient for the raw key generation rate is from the detection line output port, 48.8%.

The other limiting component in Bob's apparatus in terms of transmission efficiency was the freespace-to-fibre coupler. The coupler worked as a lens system, which focused incoming light onto a point. The fibre connector for the coupler was situated at the focal

point of the lens, which allowed most of the light to enter the fibre. The coupler focused incoming light into the core of a multimode fibre optic cable. Multimode fibre was chosen since the diameter of the core was larger than that of single mode fibre and it was therefore, more practical to couple light into it. The coupling process, however, is not fully efficient and the losses due to the fibre coupler as well as the attenuation due to the fibre were collectively measured. The fibre coupler was mounted on a clamp which allowed X and Y rotational adjustments. The ouput of the fibre was measured using an optical powermeter. The clamp dials were adjusted until the measurement on the powermeter was optimised, ensuring that the fibre coupler was aligned with the incident beam. The combination of the fibre coupler and the fibre patchcord decreased the incident optical power by 56%, as measured at the ouput of the fibre patchcord. The fibre patchcord was connected to the single photon detector in Bob's monitoring line, and is, therefore, the end point for calculating the transmission coefficient.

An optical powermeter was used to monitor the attenuation of the laser beam at various points in the system. Since the powermeter was not sensitive enough to measure in the single photon range, the neutral density filters were removed and the decrease in optical power was measured from the original power of the laser. Figure 4.1 shows a schematic diagram of the Alice and Bob modules, detailing the loss of optical power with respect to each relevent component. The diagram focuses on Bob's detection line, showing the decrease in optical power before the laser pulses reach Bob's single photon detector. The total decrease in optical power, due to the channel and all components, was 98.76%. For this system, it is only the components in Bob's module that contribute to the transmission coefficient. The decrease in optical power within Bob's module was 78.47%, and was calculated from the output of mirror M3 to the output of the fibre coupler FC, as shown in Figure 4.1. This resulted in a transmission coefficient of 0.2153.

4.1.4 Detector efficiency

The quantum efficiency of a detector is characterised by how many potential measuremets the detector actually measures. The advantage of using near-infrared wavelengths, typically used for free space communication, is that this wavelength range requires silicon detectors. The average efficiency for a silicon detector is 65% and the Perkin Elmer silicon avalanche photodiode used for this experiment had an efficiency of 60% when measuring a wavelength of 808 nm, as shown in Figure 4.2.

In order to get a true reflection of the number of detections measured by the detector per second, a correction factor was calculated with regards to the detector dead time and the detection rate [9]. The correction factor is usually multiplied to the overall count rate of

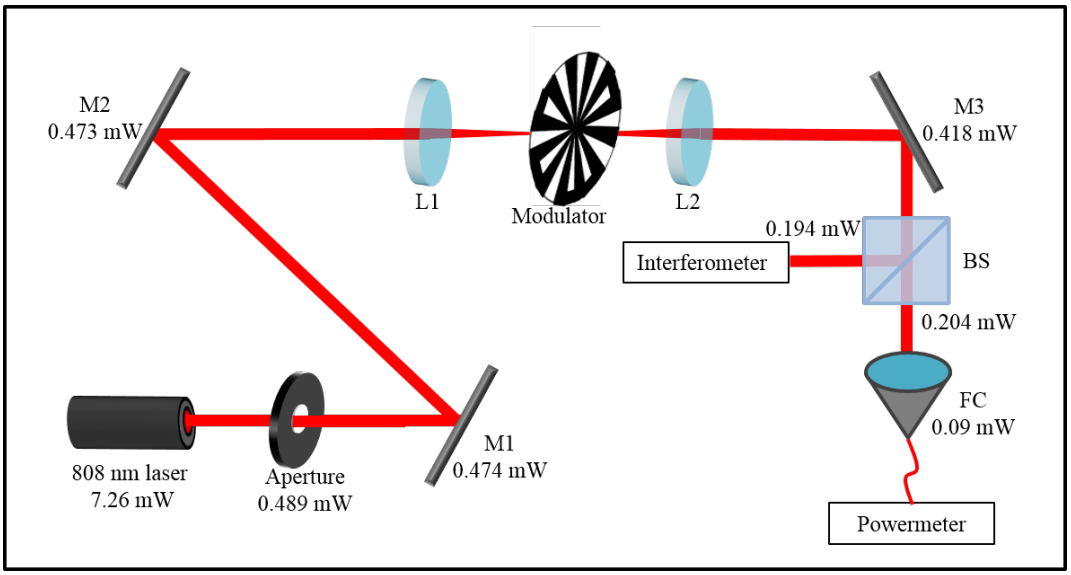

Figure 4.1: A schematic diagram showing the decrease in optical power due to the components in the Alice and Bob modules. The optical power, in mW, shown with each component, is the optical power measured by a powermeter after that corresponding component. The power of the laser source used for the system was 7.26 mW. An aperture was used to initially decrease the power of the source. Mirrors M1, M2 and M3 and lenses L1 and L2 each attenuated the beam in Alice's module. The attenuation due to L1 and L2 could not be measured separately, due to the limited space between the lenses and the modulator. The combined attenuation was, therefore, measured after M3. In Bob's module, the beamsplitter, BS, and the fibre coupler and fibre patchcord, FC, attenuated the beam, contributing to the transmission coefficient.

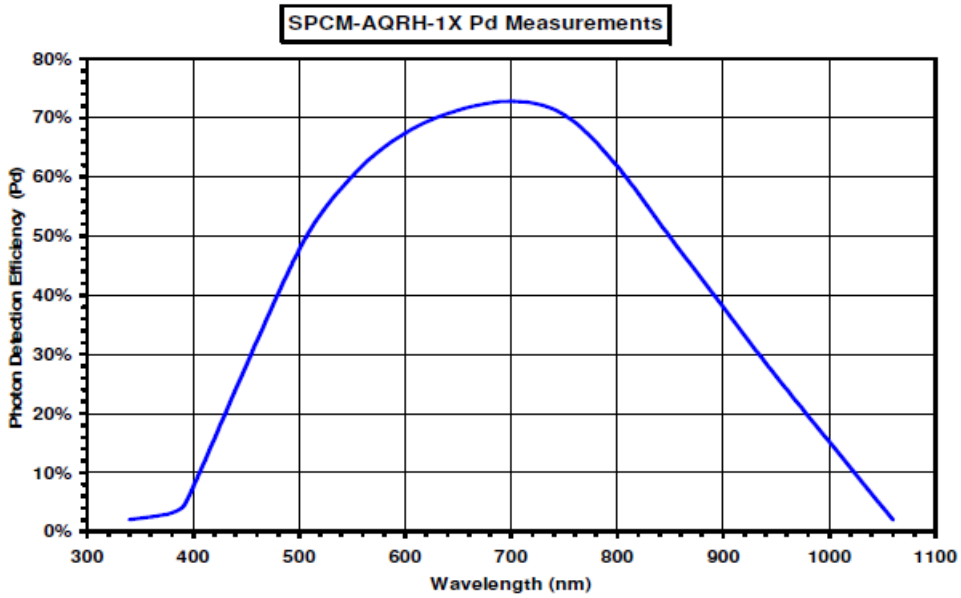

Figure 4.2: A figure showing the detection efficiency of the single photon detector with respect to operating wavelength. For the 808 nm laser used for this system, the detection efficiency was 60%. This image is sourced from [9].

the system, similar to the detector efficiency, but it is low for systems with a low pulse rate. The detector dead time was 32 ns, and since the detector was triggered to measure pulses at a low frequency of 5 kHz, the time interval before the next pulse allows the detector enough time to quench itself before being commanded to open the detection gate again. The correction factor can be calculated as

$$\frac{1}{1-(t_{\mathrm{d}} \times C_{\mathrm{R}})}, \tag{4.4}$$

where t_{d} is the dead time of the detector and C_{R} is the output count rate of the detector. Even by using the maximum output count rate of 5 kHz, the correction factor is negligibly small at 1.00016. The correction factor was, therefore, not taken into account when calculating the key generation rate.

4.1.5 Measurement of the raw key rate

Following Equation (4.2), the theoretical raw key generation rate of the system was calculated to be 323 qubits per second, using the parameters summarised in Table 4.1. The raw key generation rate was measured using the full experimental system. The electronics and software used for the data acquisition are detailed in Chapter 3.2.3. The software used for sifting the raw key is detailed in Chapter 4.3. Figure 4.3 shows the raw key generation

Parameter	Contributing Factor
Modulation rate A	5 kHz
Mean photon number μ	1
Transmission coefficient T	0.2153
Detector efficiency η	0.6

Table 4.1: The list of parameters contributing to the raw key generation rate and their corresponding theoretical values.

rate measured per second, continuously for one minute. The key rate was measured at an average of 329.33 qubits per second with a standard deviation of 56.53 counts per second. The average is above the theoretical value of 323 qubits per second since this measurement included the detector dark counts, explained in Chapter 4.2.1. Once the errors due to dark counts were subtracted, the measurements were more consistent with the theoretical value for the key generation rate. Instances of unusually low or high key rates may be due to detector malfunction. When there is a surplus of noise or multiple avalanche events, the detector counts first increase and then saturate and output low counts.

As mentioned, the key used to characterise the detection line did not include any decoy pulses. Usually, for the COW protocol, Alice and Bob would publicly announce the time bins of the decoy pulses so that they can be removed. Any detections in the monitoring line would also be publicly announced and removed. This sifting procedure was not necessary for the key tested for this setup, so the raw key rate measured above is the same as the sifted key rate for the system. The only sifting that is necessary for this key is the removal of the empty pulses that were attributed to loss in the system. The removal of lost bits does not impact the key generation rate since the meaurements of the raw key and sifted key use units of bits per second.

4.2 Factors contributing to the QBER

An interesting characteristic of the COW protocol is the role of the QBER compared to other protocols. In other protocols, such as BB84, every pulse is expected to have a single photon, unless using a mean photon number per pulse smaller than one. The bit value is determined by monitoring which detector registers a measurement for each time bin. When there are no detector clicks for a time bin, this is discarded as loss. Simultaneous clicks on more than one detector, caused by noise or eavesdropping, are also discarded. The QBER is calculated based on the number of incorrect bit values measured by the detectors. This can occur due to loss, followed by noise or a dark count in the incorrect detector or it can be due to a malfunction in the equipment. If an unusually high QBER is

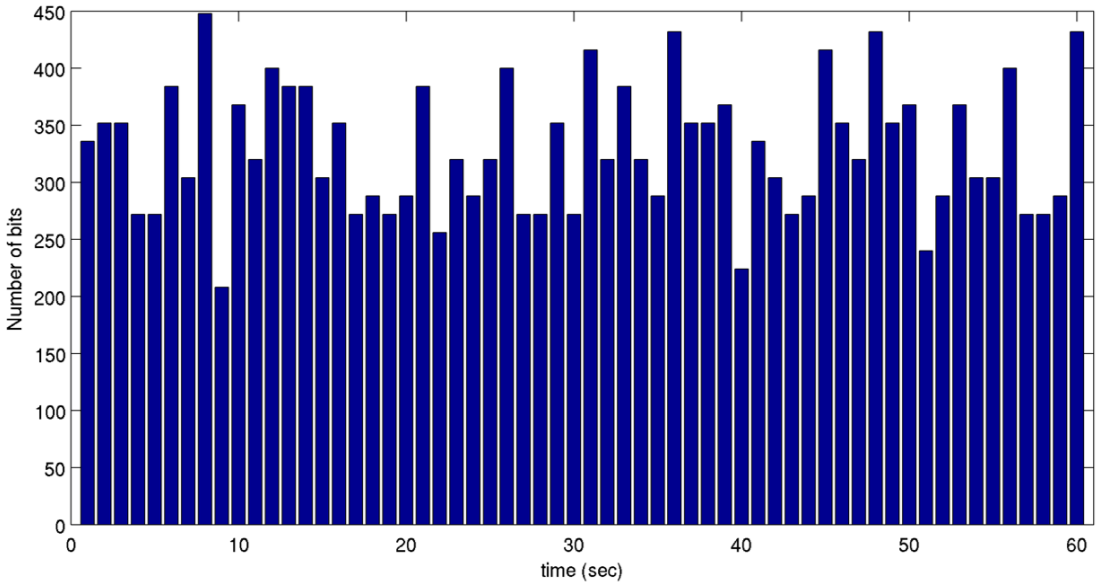

Figure 4.3: A plot of the raw key generation rate per second, measured over one minute.

measured, it is assumed that an eavesdropper is intercepting the transmission and the key distribution should be cancelled.

The QBER can be expressed as the ratio of the number of incorrect bits to the number of total bits measured. This ratio can be approximated to the rate of incorrect bits to the rate of the sifted key produced by the system [6],

$$\mathrm{QBER} = \frac{\mathrm{N_{wrong}}}{\mathrm{N_{right}} + \mathrm{N_{wrong}}} = \frac{\mathrm{R_{error}}}{\mathrm{R_{sift}} + \mathrm{R_{error}}} \approx \frac{\mathrm{R_{error}}}{\mathrm{R_{sift}}}. \tag{4.5}$$

In the COW protocol, the absence of a photon can still correctly contribute to the bit value. It is only when both pulses of a qubit are empty, that it is considered a loss. Similarly to other protocols, the QBER is dependent on the following factors of the system:

• Detector dark counts

• Noise in the channel

Contrary to other protocols, the QBER is not a direct measure of the security of the key. It is rather the visibility of the monitoring line that indicates the presence of an eavesdropper. In some instances, the eavesdropper may use techniques that cannot be detected in the monitoring line. The eavesdropper may attack vulnerabilities in the apparatus by interrogating the detectors or the modulator with bright light [124]. While preventative measures can be taken to minimise these types of attacks by placing additional filters in the Alice and Bob modules, any stray light in the channel can result in high levels of noise

in the transmission. Noise in the channel will lower the signal - to - noise ratio and set an upper bound for the channel length of the transmission.

It is, therefore, important to monitor the QBER in the detection line of the system and not just rely on the interferometer in the monitoring line to verify the key security. Monitoring the QBER also gives Alice and Bob an indication of the characterisation of the system. The performance of the optical components and the synchronisation system can be monitored throught the QBER. The channel noise and detector dark counts for the experimental setup will be discussed in detail.

4.2.1 Dark count rate of the detector

Before any measurements can be made with the single photon detectors, it is necessary to first monitor the rate of dark counts for each detector. The dark counts differ at different operating temperatures. For this experiment, the ambient room temperature was at 22^{o}C, yielding a typical dark count rate for this detector model at 100 counts per second [9]. Since the detection frequency of this system is low and the detector measurements are monitored for a short gating period, not all the dark counts will be registered during the key exchange. The dark counts were measured for the detector in Bob's detection line at an average of 10.38 counts per second with a standard deviation of 2 counts per second. The results are shown in Figure 4.4. When using single photon detectors in the monitoring line, it is important to note that the dark count rate may not be the same for all detectors. The dark count rates must, therefore, be measured separately and subtracted from the measurements of the corresponding detector.

In instances of high noise measured during the key exchange, Bob can check the temperature of the detectors. If the temperature is at a normal level, it can be inferred that the noise is not due to dark counts, but to channel noise or misaligned components.

4.2.2 Background noise of the channel

Any stray light from the environment around the device or back-scattering from components within the system can potentially increase the number of false measurements made by the detectors. Methods used to minimise the effects of background noise include:

- Spatial filters which minimise the field of view of the receiving optics in Bob's module, receiving only the light that is correctly aligned with Bob's module.

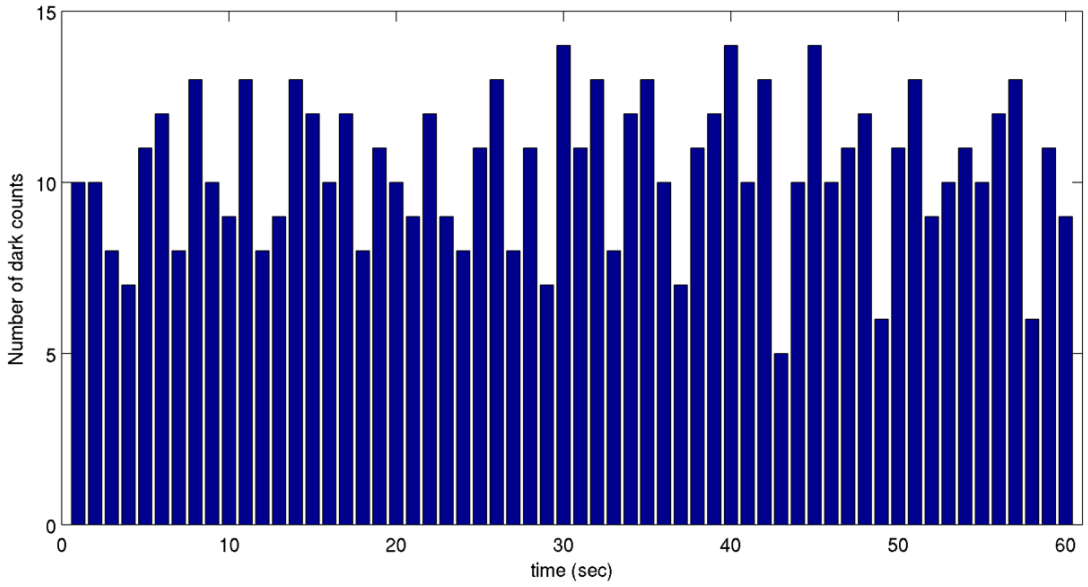

Figure 4.4: A plot of the dark count rate per second, measured over one minute for the single photon detector in Bob's detection line.

- Spectral filters with a narrow bandwidth which only transmit the wavelength of the laser used in the system. While this method will reduce ambient light in the environment, it will not reduce back-scattered light from within the system.
- Accurately timed detector gating which will reduce the effects of noise and dark counts.

These methods can be used to minimise the effects of noise but cannot completely remove its effects. The experimental results for this system were obtained in a dark room, hence minimising any background noise in the system. For a real implementation of a commercial system, it is necessary to account for the effects of background noise in different environments and characterise the suitability of that environment. The background noise rate will need to be subtracted from the raw key rate so it is important to minimise noise in order to maintain a viable signal-to-noise ratio.

The background noise was measured for different lighting conditions in the laboratory, as shown in Figure 4.5. These measurements were done without the key transmission from Alice, hence, all measurements are a result of background noise incident on the fibre coupler which leads to the detectors. When the laboratory was under dark conditions, the detector measurements were due to the dark counts of the detectors. These measurements were consistent with the previous detector dark count measurements. A dim light was used in the laboratory and the background noise was measured at an average of 1809 counts per second. Under fluorescent lighting, the background noise was measured at an

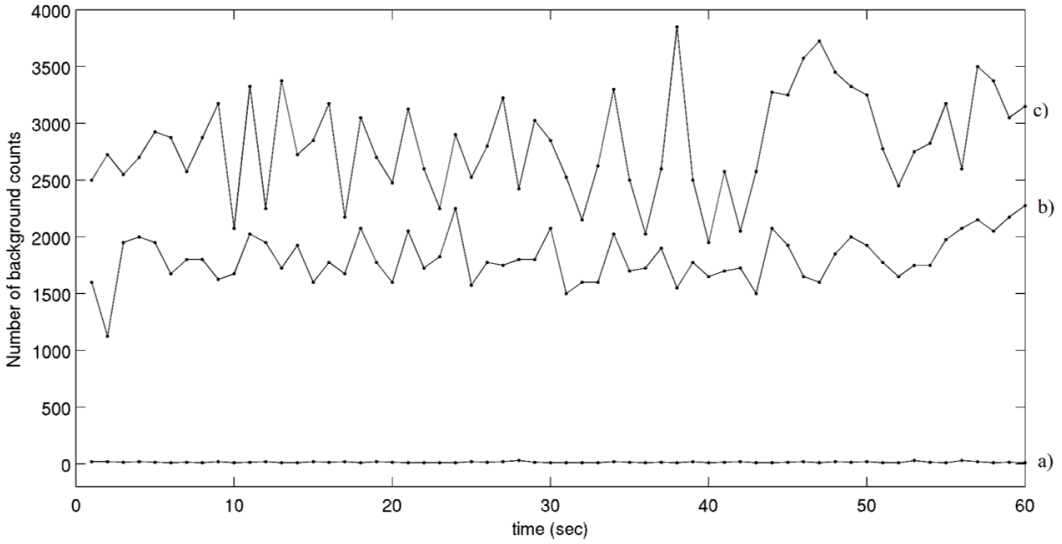

Figure 4.5: A graph showing the measurements of background noise for different lighting conditions in the laboratory. Graph a) shows the detector dark count rate, measured in a dark room. Graph b) shows the background noise measured with dim laboratory lights on. Graph c) shows the background noise with fluorescent laboratory lights on.

average of 2825 counts per second. For a detector that is triggered at 5 kHz, the fluorescent lighting creates a count rate close to the 60% detection efficiency of the detector. This level of noise under an indoor fluorescent light is significantly higher than the raw key generation rate and it would be impractical to exchange a key when the system has a low signal - to - noise ratio.

The device is designed to be handheld and a commercial application would require use in similar environments to ATM machines. Most ATM machines are situated outdoors or in rooms with fluorescent lighting. In order to use the handheld device in these environments, the special filtering techniques mentioned above will need to be applied to reduce stray light [97]. Alternatively, the device can be connected to the node via a docking station which can create a dark channel, protecting the system from ambient light.

4.2.3 Measurement of the QBER

The QBER of the system is calculated by the ratio of the rate of incorrect bit values and the rate of the sifted key measured by the system, as seen in Equation (4.5). The sifted key is created after the time bins containing loss (no measurements) or decoy pulses are removed. The remaining time bins will contain bits that contribute to the key as well as the errors.

The key was measured in a laboratory environment with no background light leaking into

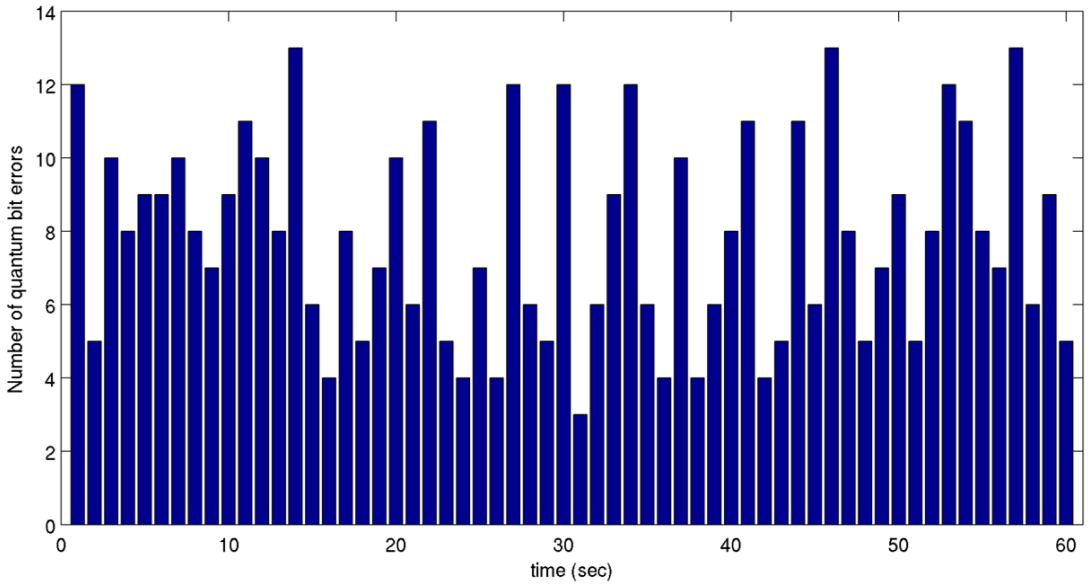

Figure 4.6: A graph showing the total errors per second identified in the sifted key for a duration of one minute. The errors represent dark counts and noise in the system.

the channel. The QBER was, therefore, due to the single photon detector dark counts and any potential malfunctions in the equipment. Malfunctions may have included any backscattered light that was in the channel, contributing to the QBER. The measured QBER is shown in Figure 4.6. The average error rate was measured to be 7.86 errors per second with a standard deviation of 3 errors per second. Using Equation (4.5) and an average sifted key rate of 329.33 bits per second, the QBER of the system was calculated to be $2.39\% \pm 0.91\%$.

It is important to note that even though the QBER was primarily due to the dark counts of the detector, the measured QBER differed from the measured dark count rate in Chapter 4.2.1. The error in the key due to dark counts was actually lower than the expected dark count rate. This was due to the dark counts that occurred in a time bin when a photon was expected. Even though these counts were not from the single photon source, they were indistinguishable from the key measurements and could not be considered as errors.

This measurement of the QBER served as a preliminary measurement to gauge the rate of errors in the sifted key. The sifted key would then need to undergo error correction algorithms, such as Cascade [125], and privacy amplification algorithms before it can be used as a key.

4.3 Software used for key sifting

The output signal from the single photon detector was collected via a coaxial cable which was connected to a digital input pin on the microcontroller, via an adapter box, shown previously in Figure 3.13. The raw data was collected in batches, the size of which was determined by the user, and transmitted to the computer per batch. The batch size was limited by the internal memory of the microcontroller. The data was read into a program which collected the raw key as a string of binary values, discussed in Chapter 3.2.3. The total raw key was then loaded into a sifting program.

In the sifting programme, the data was first split into batches of 5000 bits, so that the data could be analysed and displayed in counts per second. The programmed then looped through each batch and compared consecutive pulse pairs. Each pulse pair was looked at individually. The sifting programme compared the binary key received from the detector to the predetermined sequence encoded by Alice. The number of deviations from the sequence was recorded as well as the type of error that occurred.

For simplicity, the optical modulator was set to create a repetitive sequence of 10101010. This simple sequence allowed for a straightforward analysis of the quantum channel. If the pair was measured as 00, this pair was flagged as loss in the channel. If a pair was measured to be 10, this pair was added to the key output of the programme. The programme also checked for the number of errors per batch. A scenario that could lead to an error would be the loss of the photon in one of the pulses but the presence of a photon due to noise which may have occurred in the other pulse of the pair, therefore changing a 10 to a 01. Since no decoy pulse pairs were intentionally encoded into the sequence, the measurement of a 11 pair also indicated noise. The number of 01 pairs and 11 pairs were totalled per second and displayed in order to gain insight into the QBER. Once the QBER was determined by the sifting programme, the key generation rate was determined by recording the total number of usable bits from the measured data. Figure 4.7 shows a logic flow chart for the key sifting software and Appendix A2 shows the software code used for the sifting programme.

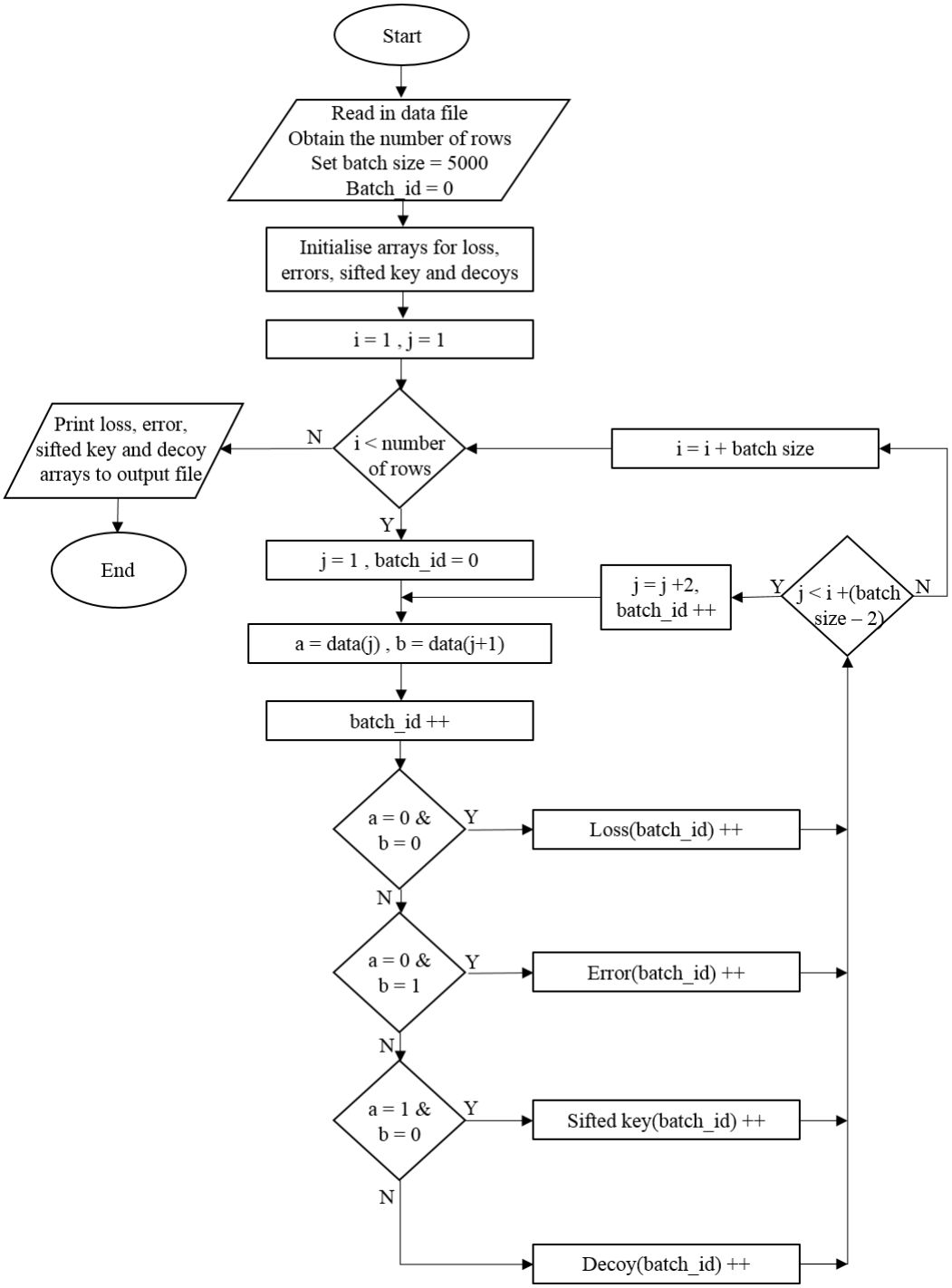

Figure 4.7: The logic flow chart of the sifting programme illustrates how the raw key measured from the system is separated into the sifted key and losses. The errors in the key are counted and this value is used to calculate the QBER. The raw key data was separated into batches of 5000 bits so that the key generation rate and error rate could be calculated per second.

4.4 Discussion

The implementation of the COW protocol over a short range free space channel serves as a proof of principle towards a handheld COW protocol device. The measurements taken under lab conditions show that the system is stable and predictable in a dark environment. By implementing spectral, spatial and temporal filtering techniques, the system may be more suitable for outdoor environments. The COW protocol is not usually implemented in free space channels, but a handheld device operational over a short distance is feasible. With recent techniques developed for quantum coherent measurements in free space, the implementation of the COW protocol over longer free space channels may be viable. A investigation on the synchronisation techniques required for a free space COW protocol implementation is presented in the next chapter. The investigation specifically considers free space communication between a satellite and a ground station.

5

Radio synchronisation for satellite QKD

Free space QKD is an evolving field of research which aims to use satellite networks to increase the distance over which a key can be distributed. Most free space QKD research makes use of polarisation encoding to create the quantum key since polarisation states are not affected by turbulence effects in the atmosphere. Usually, quantum coherent measurements, as is needed for the COW protocol, are not implemented for free space channels due to wave front distortion caused by turbulence. A recent study proposed the use of quantum coherent measurements coupled with continuous variable QKD technology for a free space channel [59]. The detection of field quadratures, i.e. continuous variables, is robust against turbulence effects and background noise in the quantum channel. The study characterised the preservation of quantum coherent states after propagation through the atmosphere from a geostationary satellite.

The use of quantum coherent states in a free space channel opens up the possibility of implementing the COW protocol in a satellite network. This chapter will focus on the synchronisation system required for satellite QKD implementation, specifically using radio communication. This investigation will work towards the future implementation of the handheld COW protocol device for long range applications via satellite. Since the COW protocol relies strongly on accurate measurement of the time of arrival of photons, a reliable synchronisation system is imperative. Most free space QKD implementations have used Global Positioning System (GPS) for tracking and synchronisation between Alice and Bob modules [126]. GPS is an external system which cannot be controlled by the authenticated users. QKD is used to encrypt sensitive data, often for banking or military use, therefore requiring a reliable synchronisation system which cannot be tampered with by an external party. Asynchronous transmission may also be used, but the bit rate of the system may be lowered, as explained below. A radio signal is a reliable alternative which will work in the absence of a GPS signal and it can be fully operated by Alice

and Bob. A radio synchronisation system can be built by off-the-shelf components and it can be used for synchronisation and tracking, authentication and as the public channel for post processing. A radio transmitter and receiver are also easier to align in comparison to an optical signal. A system using a radio signal for synchronisation and tracking was proposed in [127]. In this chapter, we present simulations to describe a synchronisation signal between Alice and Bob using radio transmission. We focus especially on the Doppler effects on the synchronisation signal during transmission between a ground station and a Low Earth Orbit (LEO) satellite. The simulations in this chapter were done using Simulink, a Mathworks graphical programming package.

5.1 Asynchronous Transmission

Asynchronous transmission intersperses the data signal with a synchronisation sequence using the same light source [128]. The advantage of aligning just one light source makes this method simpler to implement than a synchronous method such as the optical synchronisation detailed in Chapter 3. The bit rate of the signal is established before the transmission begins and it is, therefore, only necessary for the transmitter to indicate when the receiver should start to take measurements. The bit sequence for asynchronous transmission must begin with an indicative "Start" bit followed by 8 bits of data. A "Stop" bit indicates the end of the data and the beginning of another synchronisation iteration, as seen in Figure 5.1. The key generation rate of the system will decrease when using asynchronous transmission since the start and stop indicators do not contribute to the key. However, the COW protocol produces a higher bit rate compared to other QKD protocols, therefore compensating for the large overhead.

In order to implement asynchronous transmission for the COW protocol, the pseudo-single photon source in the transmitter must be controlled by a variable attenuator so that the mean photon number of each pulse can be adjusted. It is necessary for each start and stop pulse to be measured by the single photon detectors. Since single photons can be lost during transmission, the mean photon number of the start and stop pulses should be increased to increase the probability of detection. Should the start and stop pulses not be measured, the receiver will not open the detector gates to receive a new set of bits, thus resulting in high losses in the channel. The mean photon number can be decreased to one during the transmission of the data bits. Asynchronous transmission can be used for geostationary satellites but would not be appropriate for communication with a LEO satellite, since the frequency of the transmission will change due to Doppler effects.

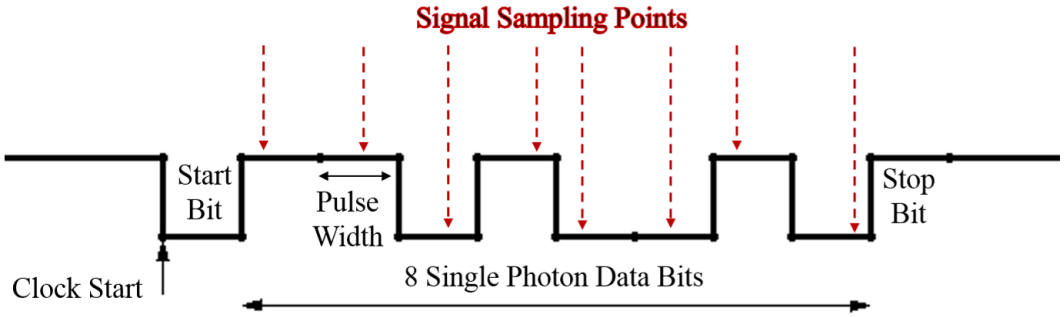

Figure 5.1: A figure showing the signal structure of asynchronous transmission. Asynchronous transmission begins with a Start bit which serves as the synchronisation indicator. The pulse width of each bit is agreed upon before the transmission begins and the receiver is able to measure the 8 data bits following the Start bit. The Stop bit indicates that the data has stopped, pending the transmission of another Start bit.

5.2 Synchronous communication using BPSK modulation

A radio signal can be encoded with information using phase modulation [129]. Phase-Shift Keying (PSK) refers to the phase modulation of a sine or cosine wave,

$$s_n(t) = \sqrt{\frac{2E_b}{T_b}} cos(2\pi ft + \pi(1-n)), \tag{5.1}$$

where $E_b$is the energy per bit, T_b is the bit duration, f is the frequency of the wave and t is the time variable. Binary Phase Shift Keying (BPSK) specifically modulates the wave by π rad, creating a binary code. The possible values for n are, therefore, n = 0 or n = 1, resulting in the following equations for each:

$$s_1(t) = \sqrt{\frac{2E_b}{T_b}} cos(2\pi ft + \pi) \tag{5.2}$$

and

$$s_0(t) = \sqrt{\frac{2E_b}{T_b}} cos(2\pi ft). \tag{5.3}$$

The binary bit values can be observed in the signal by measuring for phase changes in each pulse. If the phase matches that of the original wave, the bit value is 0. If the phase has undergone a shift of πrad, the bit value is 1. BPSK is more resistant to errors compared to other types of PSK since the binary values are πrad, or half a wavelength, apart. An erroneous phase-shift will have to be greater than $\frac{\pi}{2}$ rad to change the binary bit value.

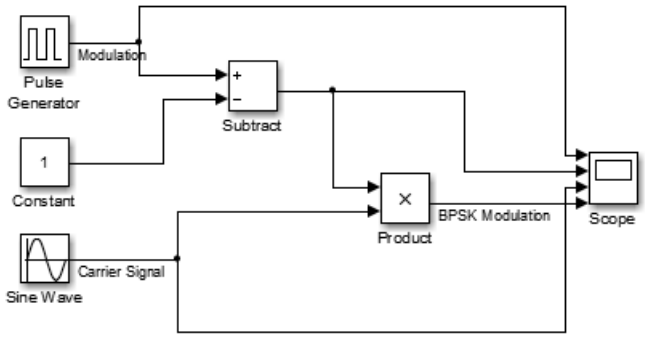

Figure 5.2: A simulation setup to generate a BPSK signal. The Carrier Signal, a sinusoidal wave of amplitude 1 V and frequency of 0.5 Hz, undergoes phase modulation according to the bit values of the Modulation signal. The Modulation signal was in the form of a square wave with an amplitude between 0 V and 2 V and a frequency of 4 seconds. A constant value of 1 V was subtracted from the Modulation signal so that the amplitude now varied from -1 to 1 V. The new Modulation signal was then multiplied to the Carrier signal. In instances when the Modulation value was 1 V, the phase of the Carrier remained unchanged. When the Modulation value was -1 V, the Carrier was inverted, thereby shifting the phase by πrad.

In order to create a simulated BPSK signal, the sinusoidal wave, or carrier signal, was multiplied by a modulation signal which controlled the phase shift of the carrier. The modulation signal represented the bit values for transmission over the public channel. Bob will need to extract the carrier signal in order to synchronise his device with Alice. The simulation setup to generate a general BPSK signal is shown in Figure 5.2 and the results of the simulation are shown in Figure 5.3.

5.3 Demodulation using the Costas loop

5.3.1 Phase Locked Loop

One of the uses of a Phase Locked Loop (PLL) is to lock the frequency of a signal in order to synchronise two parties [130]. This technique is applicable to long range, satellite QKD but can also be applied to a short range, handheld device. The PLL can assist in correcting any frequency deviation due to malfunction or temperature gradient. A PLL circuit includes a Voltage Controlled Oscillator which forms a feedback loop with the incoming signal [131]. The incoming signal v_{i} and VCO signal v_{o} are combined using a mixer and the VCO is adjusted using the differences in the two signals. The output signal v_{f} is maintained at a constant frequency due to the adjustments received from the VCO, regardless of the changes in v_{i}. A diagram of a PLL is shown in Figure 5.4.

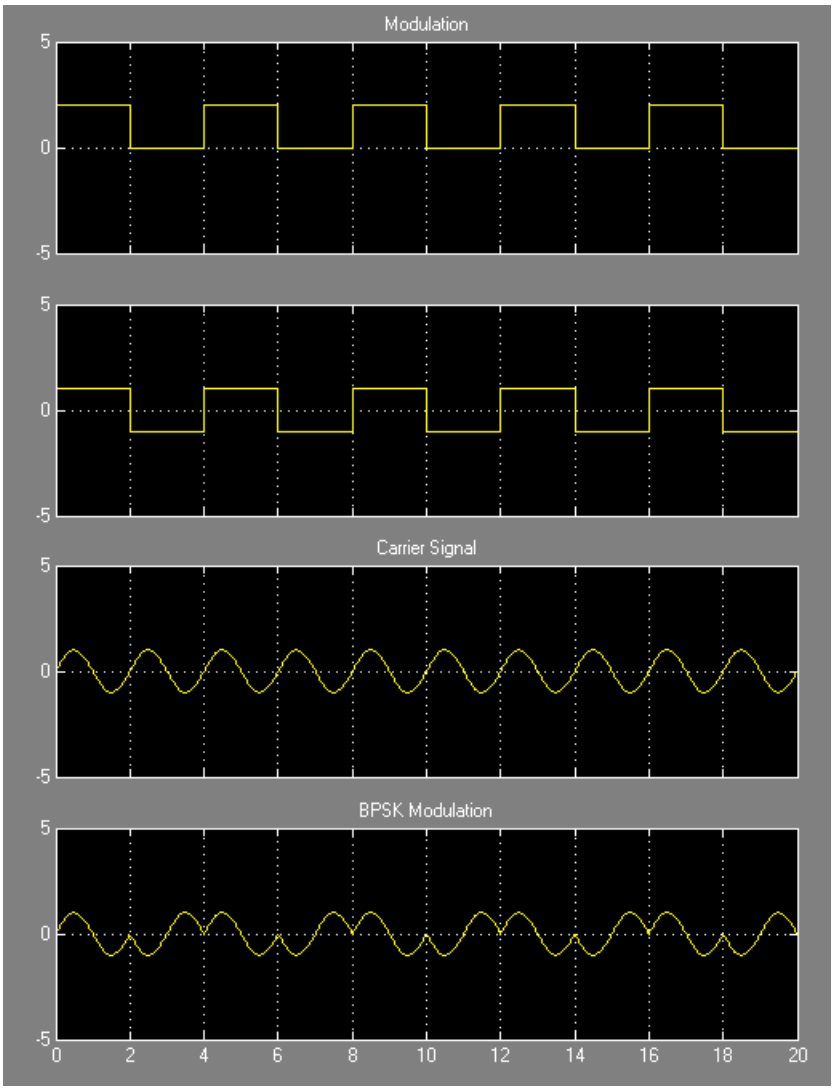

Figure 5.3: The result of the BPSK simulation is shown. a) shows the Modulation signal with an amplitude of 2 V. b) shows the Modulation signal, now shifted by -1 V so that the amplitude is between -1 V and 1 V. c) shows the Carrier signal and d) shows the product of the Carrier signal and the shifted Modulation signal. A phase change occurs every 2 seconds, representing a change in the bit value of the Modulation signal.

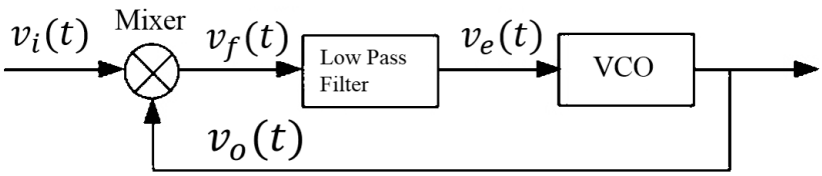

Figure 5.4: A schematic diagram of a PLL. The VCO signal is combined with the incoming signal v_i. The resulting signal is filtered so that only low frequency terms remain. The filtered signal is used to adjust the VCO, providing a continuous feedback loop.

5.3.2 Costas Loop

The coherent demodulation of the incoming signal from Alice and the carrier recovery can be performed by using a Costas loop [130]. The Costas loop is based on a PLL and can be used to recover the carrier frequency of a phase-modulated signal, such as BPSK. A circuit diagram of the Costas loop is shown in Figure 5.5. In the Costas loop, the VCO is a free oscillator centered on the carrier frequency ω_0, that can change the frequency in function of an applied voltage, named V_{CON}. The output signal can be synthesized by the equation

$$V_{\mathrm{VCO}}(t) = cos[\omega t + \int_0^t kv V_{\mathrm{CON}}(\tau) d\tau] \tag{5.4}$$

where *kv* is the sensitivity of the VCO expressed in rad/V. A BPSK signal can be represented according to the following function:

$$V_{\mathrm{BPSK}}(t) = AS_{\mathrm{p}}(t) cos(\omega_0 t), \tag{5.5}$$

where ω_0 is the angular frequency of the carrier, S_{p}(t) contains the bit to transmit and A is the amplitude of the received carrier. The angular frequency ω_0 is the frequency of the local oscillator of the VCO. The synchronisation frequency for the Bob's QKD device is extracted from the carrier frequency.

Suppose that the signal from the VCO is

$$V_{\mathrm{VCO}}(t) = cos(\omega_0 t + \varphi_e), \tag{5.6}$$

where φ_{e} represents the difference in phase between V_{BPSK} and V_{VCO}. The VCO signal in Equation (5.6) is sent to analog multiplier 1 and a -90° phase shifter. The signal at the output of the analog multiplier is

$$V_1(t) = V_{\mathrm{BPSK}} \times V_{\mathrm{VCO}} = \frac{AS_{\mathrm{p}}}{2}[cos\varphi_{\mathrm{e}} + cos(2\omega_0 t + \varphi_{\mathrm{e}}]. \tag{5.7}$$

It is possible to attenuate the components cos (ω_{p}t + φ_{e}) of the signal V_1(t) through the low pass filter F1. The signal at the output of F1 is:

$$V_{\mathrm{q}} = \frac{AS_{\mathrm{p}}}{2} cos\varphi_{\mathrm{e.}} \tag{5.8}$$

V_{q} is not dependent on the frequency ω_0. When V_{VCO}, crosses the phase shifter, the signal V_{SH}(t) is

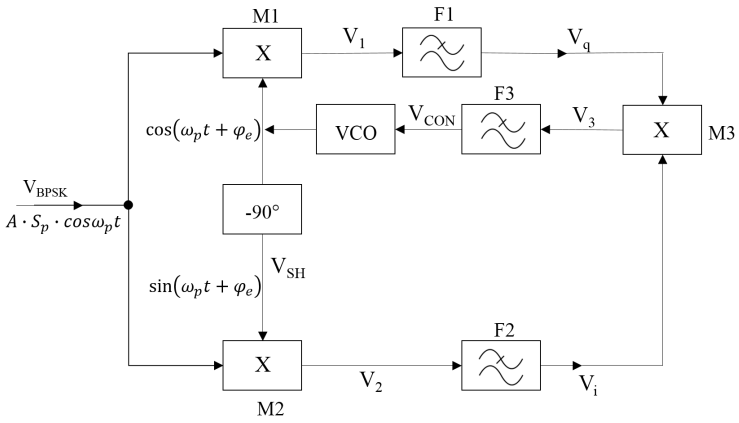

Figure 5.5: The Costas loop is designed to match the VCO frequency to that of an incoming signal. In this case, the incoming signal is modulated with BPSK, called V_{BPSK}. The VCO signal is combined with V_{BPSK}, at multiplier M1. The VCO signal is shifted in phase and combined with V_{BPSK} at multiplier M2. The outputs of M1 and M2 are both passed through low pass filters, F1 and F2 respectively. The outputs of F1 and F2 are multiplied at M3 and passed through low pass filter F3. The output of F3 is used to adjust frequency of the VCO signal.

$$V_{\mathrm{SH}}(t) = cos(\omega_0 t + \varphi_{\mathrm{e}} - 90°) = sin(\omega_0 t + \varphi_{\mathrm{e}}). \tag{5.9}$$

V_{SH} multiplied by V_{BPSK} is

$$V_2(t) = \frac{AS_{\mathrm{p}}}{2}[cos(90° - \varphi_{\mathrm{e}}) + cos(2\omega_0 t + \varphi_{\mathrm{e}} + 90°)]. \tag{5.10}$$

Since the signal has double frequency components, the signal can be filtered to obtain a signal $V_{\mathrm{i}}(t)$,

$$V_{\mathrm{i}}(t) = \frac{AS_{\mathrm{p}}}{2} cos(90° - \varphi_{\mathrm{e}}) = \frac{AS_{\mathrm{p}}}{2} sin(\varphi_{\mathrm{e}}). \tag{5.11}$$

The signals V_{q} and V_{i} are multiplied to obtain the voltage control of the VCO, V_{CON},

$$V_{\mathrm{CON}} = V_{\mathrm{q}} \times V = \frac{A^2 S_{\mathrm{p}}^2}{32} sin(2\varphi_{\mathrm{e}}). \tag{5.12}$$

From Equation (5.4), it is possible to observe that V_{CON} changes the frequency V_{VCO} proportionally to the phase φ_{e}. If φ_{e} increases, V_{CON} and V_{VCO} increase in order to follow the signal V_{BPSK} received. When $\varphi_{\mathrm{e}} = 0$, V_{VCO} is 0 and the signal V_{VCO} is in phase with V_{BPSK}. The synchronisation signal for Bob's QKD module is now obtained from the V_{VCO} signal.

A simulation of the Costas loop was done to demonstrate how the VCO is able to adjust its

initial frequency to match the frequency of the incoming signal. The Simulink simulation is shown in Figure 5.6a). A detailed view of the phase-shifter subsystem used in the Costas loop is shown in Figure 5.6b). The incoming BPSK signal was set to have an initial phase difference of $\frac{\pi}{2}$ compared to the VCO frequency of the Costas loop. The amplitudes of both the BPSK and the VCO signals were set to 1 V and both frequencies were set to 1 Hz. The low pass filters were set to allow a bandwidth of 0.001 Hz to 0.01 Hz and the VCO sensitivity was set to 0.6 Hz/V. The result, shown in Figure 5.7, shows that despite the initial phase difference between the VCO signal and the BPSK signal, the Costas loop was able to shift the VCO signal to match the incoming BPSK signal after four pulses. This result demonstrates the effectiveness of the Costas loop in synchronising two separate QKD modules. The above example was a static case, where only the initial phase condition was different for each signal. In a real application, the relative phase of each wave will change in real time. This case will be discussed in the following section.

5.4 Doppler effects

When communicating with a LEO satellite, or any moving module, the Doppler effects on the transmission signal must be taken into account. Better synchronisation can be achieved if the satellite oscillator is corrected with regards to the relativistic effects [132]. The ability of the Costas loop to match Bob's VCO frequency to the frequency of the incoming signal from Alice will be useful when Alice's signal undergoes a frequency shift Δf during transmission. A proof of principle simulation of this application was done with a linear frequency shift in Alice's signal. In a real scenario, the change in frequency due to Doppler effects in non-linear and a simulation was done to show that the Costas loop can be used to recover the carrier frequency in these conditions.

5.4.1 Using the Costas loop for a linear Δf

A simulation was done to show the effects of Doppler shift on the transmission between Alice an Bob. The frequency of Alice's signal and Bob's VCO were set to 2.4 GHz, since this is a typically used frequency for radio communication. In a scenario where Alice's module is situated on a LEO satellite, a typical average shift in frequency for a carrier frequency of 2.4 GHz, as the satellite passes over Bob's module, is 13 kHz per second. Figure 5.8 shows the amplitude difference between Alice's signal and Bob's VCO signal. As the frequency of Alice's signal increased, the two signals periodically moved in and out of phase with respect to each other. As shown in Figure 5.8, the amplitude difference

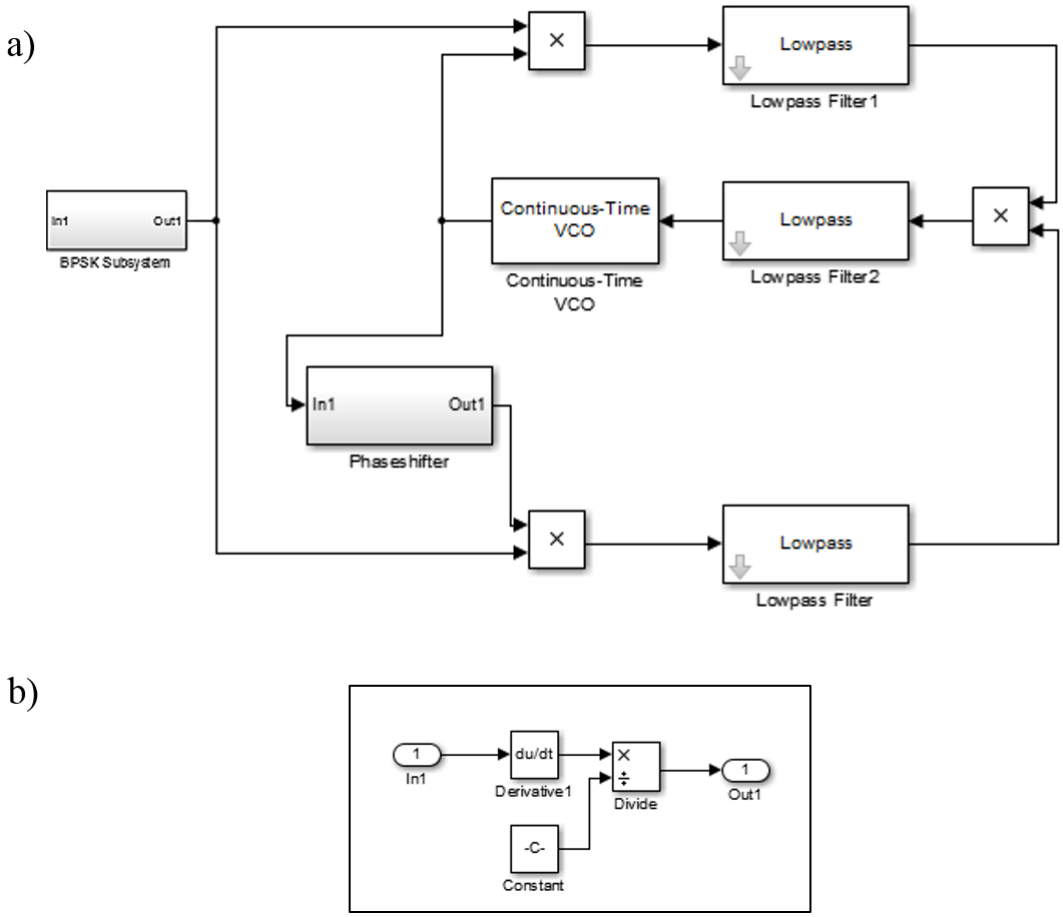

Figure 5.6: A figure showing the simulation setup for a Costas loop, used to extract the carrier signal of a BPSK signal. The entire setup is shown in a) and a focused schematic of the phase shifter subsystem is shown in b). The amplitude of both the BPSK signal and the VCO signal were set to 1 V. The frequency of both signals were set to 1 Hz and a phase difference of $\frac{\pi}{2}$ was set between the signals. The lowpass filters were set with a bandwidth between 0.001 Hz and 0.01 Hz. The VCO was set with a sensitivity of 0.6 Hz/V so that the VCO could be gradually adjusted to match the BPSK signal. In b), a 90° phase shift was created for the sinusoidal VCO signal by using the first derivative of the signal. The resulting wave was then multiplied by a constant in order to compensate for any amplitude changes

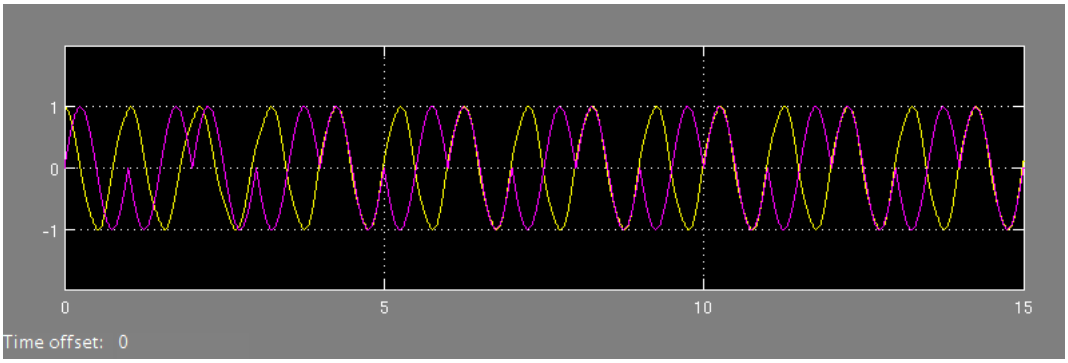

Figure 5.7: A figure showing the effectiveness of the Costas loop in phase-locking two signals. The incoming BPSK signal from Alice, shown in pink, was set to have an initial phase difference to the VCO signal in Bob's module, shown in yellow. The Costas loop was able to adjust the frequency of the VCO signal until it was in phase with the BPSK signal after four pulses. The adjusted VCO signal represents the carrier signal extracted from the BPSK signal which can be used to establish synchronisation between the two QKD modules.

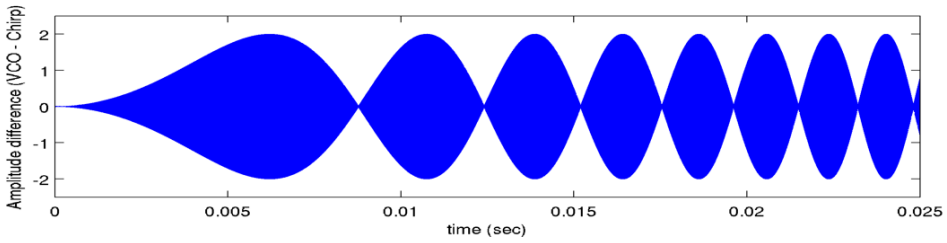

Figure 5.8: A graph showing the difference in amplitude between Alice's signal and Bob's VCO signal. As Alice's signal increased in frequency due to Doppler shift, the two signals moved in and out of phase with each other. Points of maximum amplitude on this graph indicates when the signals were out of phase by πrad. Points of zero amplitude on this graph indicate when the signals were in phase.

between the signals reached its first maximum at approximately 6.2 ms. This indicated the first instance of the signals being out of phase. In the simulation, both the signals from Alice and Bob were set to the same initial conditions, but the frequency of Alice's signal shifted by 13 kHz per second. Figure 5.9 a), b) and c) shows the difference between Alice's signal and Bob's VCO at different time periods, until they were irrecoverably out of phase at 6.2 ms. Figure 5.9d) shows that, by implementing the Costas loop, the frequency of the VCO was able to change in order to stay in phase with the Doppler shifted signal from Alice.

Now that it has been shown that the Costas loop is effective in compensating for Doppler effects, a simulation was done to show how it can be applied to extracting the carrier signal from a Doppler shifted BPSK signal. The first step was to create a BPSK signal with a varying frequency. A chirp signal was used to create the carrier signal. A chirp signal is a sinusoidal wave which has a linearly changing frequency [133]. A BPSK subsystem was built to create a BPSK modulation for the chirp signal. The previous method to create a

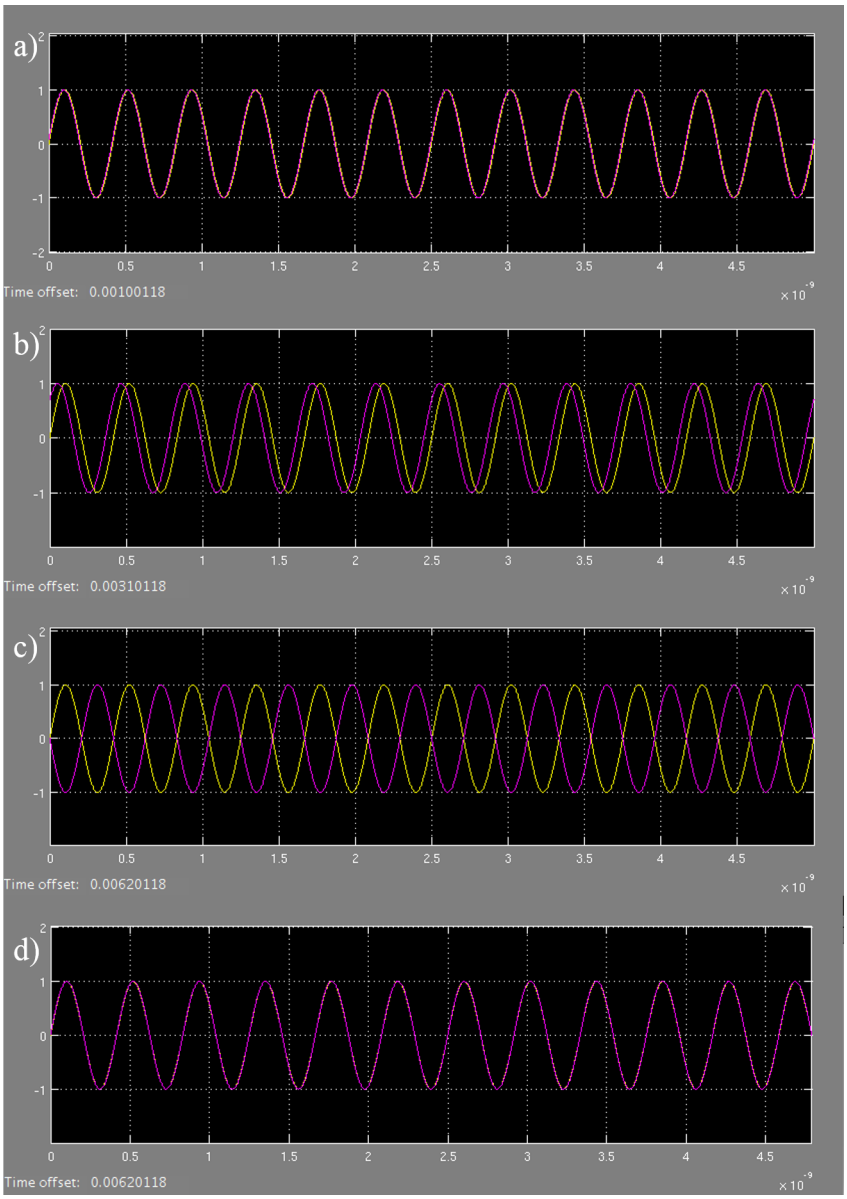

Figure 5.9: Simulation results showing the effect of a linearly changing frequency from the Alice module, shown in pink. The VCO signal from Bob is shown in yellow. Both signals were set with an initial frequency of 2.4 GHz and the results in the above figure show a 5 ns snapshot of the signals at different points in time. a) shows that the signals are still in phase with each other after 1.0 ms. b) and c) show how the signals move out of phase at 3.10 ms and 6.20 ms respectively. With the use of the Costas loop, the signals are able to remain in phase. d) shows the effects of the Costas loop and the snapshot of the signal was taken at 6.20 ms to show the effects of the VCO compensation at the point of maximum phase difference.

BPSK modulated signal could not be applied to the chirp signal, since it would require a square wave which changes in frequency with the same rate as the chirp signal.

For the BPSK subsystem, the frequency of the chirp signal was extracted in real time using an interval test. A T-configuration JK flip-flop was used to create a square wave using the extracted frequency. The square wave was then multiplied by the chirp signal in order to create a a BPSK modulation. The BPSK subsystem is shown in Figure 5.10. The output of the BPSK subsystem is shown in Figure 5.11. The BPSK subsystem using the chirp signal was then set as the incoming Alice signal for the Costas loop. The simulation setup is shown in Figure 5.12.

The VCO and BPSK signals were set with an initial frequency of 2.4 GHz. The BPSK signal was set to shift in frequency by 13 kHz per second. The VCO sensitivity was set to 48 MHz/V which is a parameter typically used for commercial VCO components [131]. The voltage input to the VCO needed to have an amplitude between 0.5 V and 1 V, which was also a requirement of a commercial VCO. The voltage input to the VCO therefore required amplification after lowpass filter F3, as shown in Figure 5.12. Without amplification, the input to the VCO had an amplitude with a maximum of 0.5 V. In order to amplify this signal to the required range, a gain of 2 was applied to the signal. The lowpass filters were set for a transmission bandwidth between 0.001 and 0.01 GHz. The result of this simulation is shown in Figure 5.13a), demonstrating that the Costas loop was able to extract the carrier signal of a BPSK signal with a linearly varying frequency. Figure 5.13b) shows the amplified signal after lowpass filter F3, used to control the VCO.

5.4.2 Using the Costas loop for a non-linear Δf

When simulating the transmission between a LEO satellite and a ground station, the Doppler shift of the frequency of the transmission should be considered. The previous section approximated an average Doppler shift and simulated the transmission signal using a linear change in frequency. In a real application, the Doppler shift Δf is non-linear and can be described by [129]:

$$\Delta f = \frac{1}{\lambda} V_{\mathrm{T}} cos\theta, \tag{5.13}$$

where λ is the wavelength used for the transmission, V_{T} is the tangential velocity of the satellite with respect to the circular trajectory and θ is the angle between V_{T} and the direction of transmission, as seen in Figure 5.14. In order to use the centre of the Earth as a reference frame, it is simpler to express θ in terms of the angle γ between the ground station and the vertical direction of the satellite. For this simulation, the trajectory of the

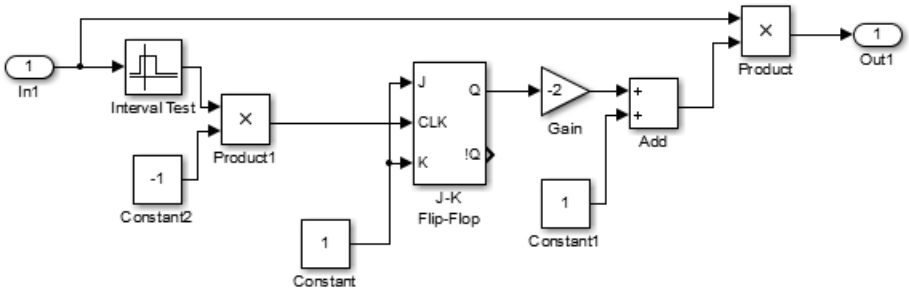

Figure 5.10: A figure showing the BPSK subsystem used to apply a BPSK modulation to a chirp signal. The Input In1 is the sinusoidal chirp signal which was then passed through an interval test. The output of the interval test is True for values above 0 and False for values below 0. The interval test therefore outputs a square wave with amplitude between 0 and 1 with a frequency that matches the chirp signal. The flip-flop was used to double the period of the square wave, so that the bit value of the square wave changed after a complete wavelength of the chirp signal. Additional operations were used to invert, shift or amplify the signal as required. The square wave was then multiplied with the original chirp signal in order to create the BPSK modulation. The results of this simulation are shown in Figure 5.11.

satellite is an orbit around the equator of the Earth. The angle γ becomes the longitudinal coordinate of the satellite. If the longitudinal coordinate of the satellite is known, it is simpler to calculate the frequency of the sinusoidal signal with respect to time $f_{\mathrm{f}}(t)$ using the following equation [129]:

$$f_{\mathrm{f}}(t) = f_{\mathrm{T}} + \frac{1}{\lambda} V_{\mathrm{T}} cos\left(\frac{\pi}{2} - arctan\left(\frac{R_{\mathrm{eq}} sin\left(\gamma_{\mathrm{i}} + \omega_{\mathrm{T}} t\right)}{R_{\mathrm{s}} - R_{\mathrm{eq}} cos\left(\gamma_{\mathrm{i}} + \omega_{\mathrm{T}} t\right)}\right)\right). \tag{5.14}$$

In the above equation, f_{T} is the initial frequency of the signal. The term R_{eq} is the equatorial radius of the Earth and R_{s} is the sum of R_{eq} and the altitude of the satellite from the Earth's surface. γ_i is the longitudinal coordinate at the beginning of the transmission. The angular frequency of the Earth's rotation and the angular frequency of the satellite's orbit were summed to create the term ω_{T}. The parameters substituted for each of the terms in Equation (5.14) are shown in Table 5.1.

A graph illustrating the change of the frequency of the signal using the parameters specified in Table 5.1 is shown in Figure 5.15. The change in frequency was a function of the change in the angle θ, between the tangential velocity of the satellite and the direction of the transmission. As the angle θ increased, the frequency of the transmission decreased. The frequency was plotted for 56 seconds, which was the time taken for the satellite to orbit from a longitudinal angle of -2$^{\mathrm{o}}$ to 2$^{\mathrm{o}}$. The frequency began at a value higher than the initial frequency of 2.4 GHz. As the satellite moved directly above the ground station,

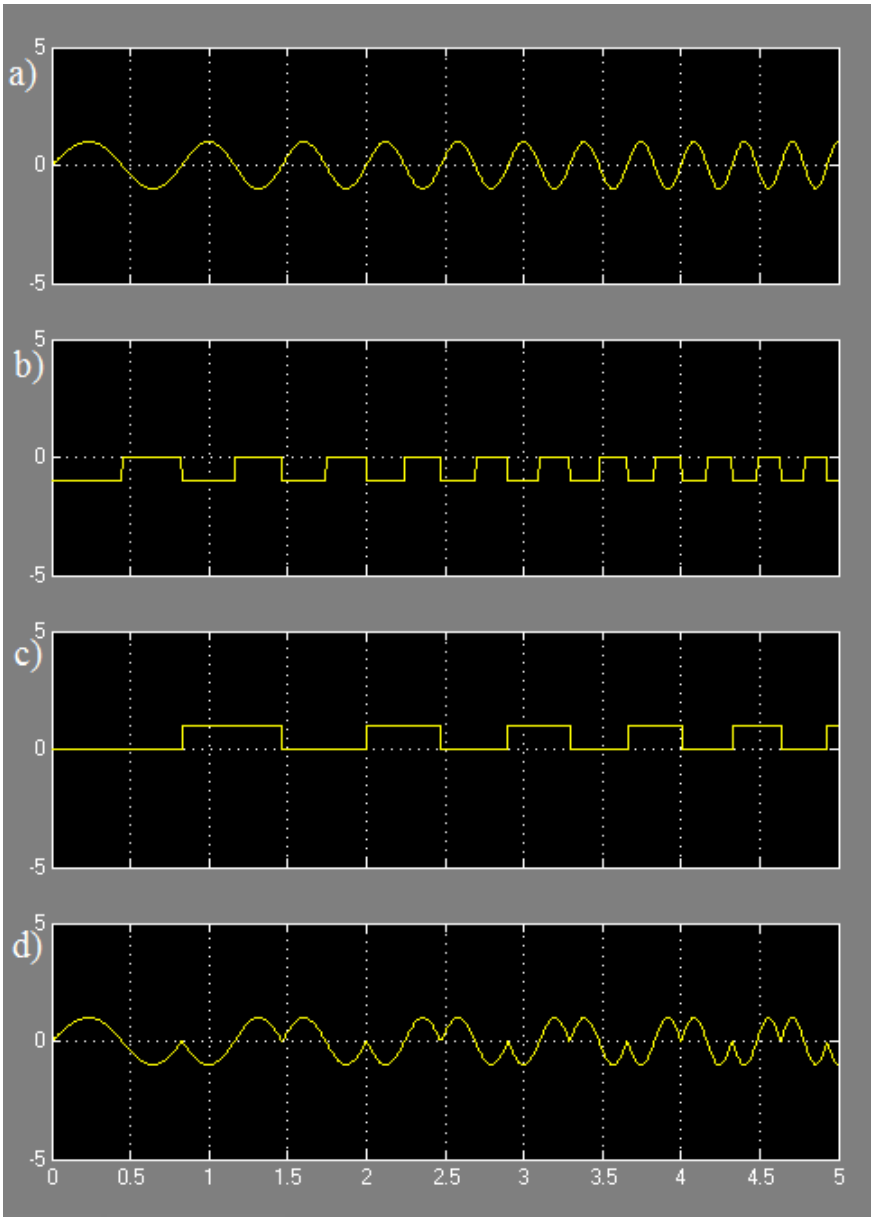

Figure 5.11: A figure showing the output of the BPSK subsystem. a) shows the chirp signal used as the carrier signal for Alice. The chirp signal underwent an interval test and was inverted, the result of which is shown in b). A flip-flop was used to double the period of the square wave. The flip-flop was set so that only a bit change from 1 to 0 in the square wave shown in b) would result in a bit change for the square wave shown in c). The result in c) was then multiplied with the chirp signal in a), forming the BPSK modulation shown in d).

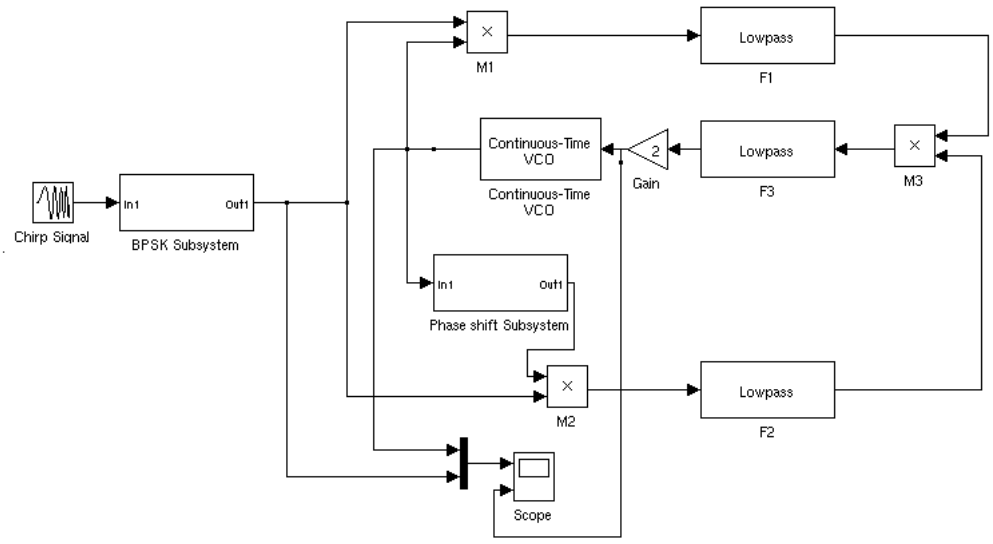

Figure 5.12: A figure showing the simulation setup for the Costas loop, with a BPSK modulated signal with a linearly changing frequency from Alice. The parameters for the VCO were set to those of a commercially available VCO. Since the input of the VCO needed to be of the order of 0.5 V to 1 V, the signal required amplification. The scope indicates the points from which the output results were viewed. The results are shown in Figure 5.13.

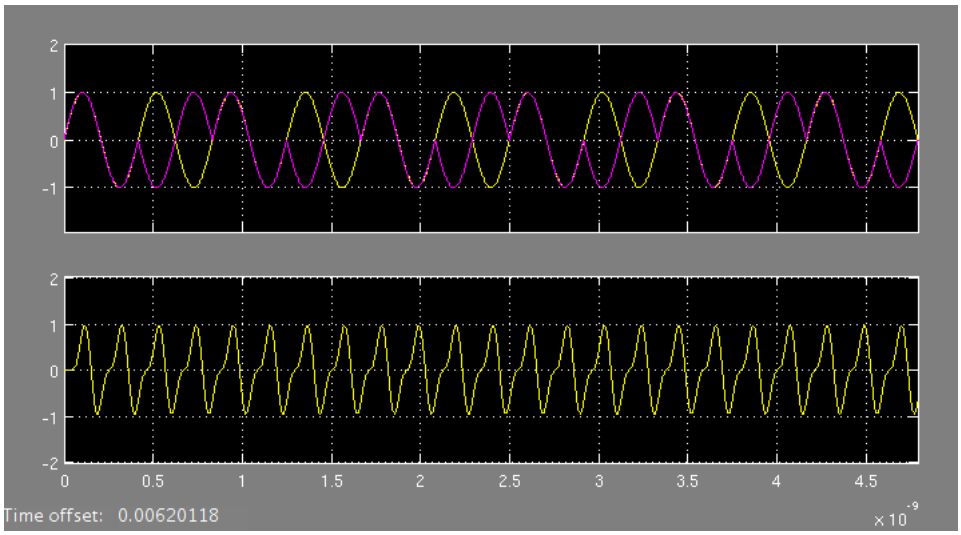

Figure 5.13: The simulation result showing the extraction of the carrier signal from a BPSK modulated signal with a linearly changing frequency. a) shows the comparison of Alice's BPSK modulated signal, shown in pink, with Bob's VCO signal, shown in yellow. The sinusoidal VCO signal was able to match the changing frequency of the BPSK modulated signal, thus synchronising the two modules. The amplified input to the VCO is shown in b).

Parameter	Value
f_T	2.4 GHz
λ	0.125 m
V_T	9.058 km/s
R_{eq}	6378.137 km
R_s	7378.137 km
γ_i	-2^o
ω_T	1.2278 x 10^{-3} rad/s

Table 5.1: A table listing the values used for the simulation of the frequency of a sinusoidal wave with a non-linear change in frequency described in Equation (5.14).

the transmission frequency was equal to 2.4 GHz and as the satellite moved away, the frequency decreased further. The total change in frequency for the duration of 56 seconds was 31.4 kHz.

In order to simulate a BPSK modulated signal using a sinusoidal wave with a frequency term following Equation (5.14), a subsystem was created. The subsystem replaced the chirp signal that was used in the previous section. The schematic of the full simulation is shown in Figure 5.16a). The details of the subsystem to create a sinusoidal wave with a non-linear frequency shift is shown in Figure 5.16b). Equation (5.14) was programmed into a function block in the subsystem. Since the frequency shift is dependent on time, a clock was used as the input to the function. Another function block was programmed to create the sine wave, using the formula $sin(2\pi ft)$. The generated frequency and the clock were both used as inputs for the sine wave function block. The output of the sine wave subsystem was then used as the input for the BPSK subsystem, thus generating a BPSK modulated signal with a non-linear shift in frequency.

The amplitude difference between Alice's signal and Bob's VCO signal are shown in Figure 5.17, indicating the phase difference between the two signals. As shown in Figure 5.15, the frequency difference between the two signals at the beginning of the transmission was 15 687 Hz. The phase difference between the signals reached a maximum at just 31.8 μs. As the satellite moves closer to the ground station and the frequency of Alice's signal decreases, the phase difference would take a longer time to reach a maximum of π rad. The results of the Costas loop simulation to compensate for the frequency shift are shown in Figures 5.18 and 5.19. The VCO in Bob's apparatus was able to recover the carrier signal of the BPSK signal, as shown in Figure 5.18. The result shows a snapshot of the signals starting at t = 31.8 μs. The synchronisation signal was extracted from the output of the VCO. The VCO signal was squared and Figure 5.19 shows that the frequency is consistent with the BPSK signal. The synchronisation signal can be used to trigger Bob's single photon detectors and data acquisition subsystem.

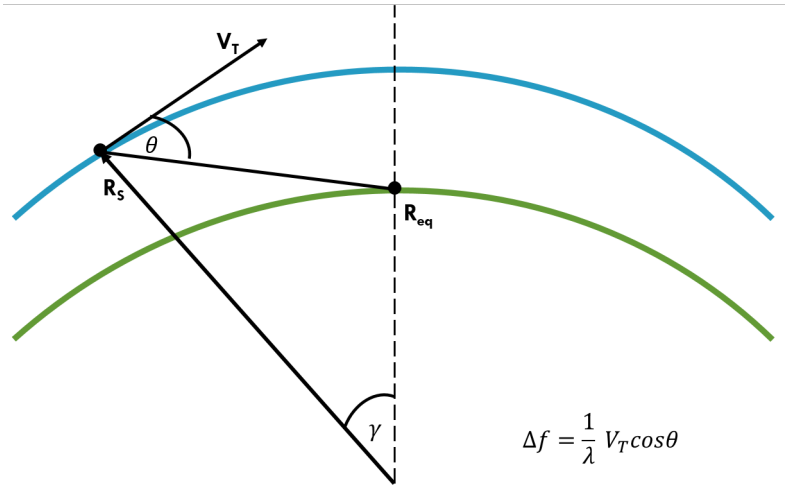

Figure 5.14: A diagram showing the trajectory of a LEO satellite, orbiting the equator of the Earth, and it's transmission to a ground station. The ground station is located at R_{eq}, which is the radius of the Earth. The satellite is located at R_{s}, which is the sum of the Earth's radius and the satellite's altitude. V_{T} is the tangential velocity of the satellite with respect to its orbit and θ is the angle between the tangential velocity and the direction of the transmission. The angle γ, between R_{eq} and R_{s}, is the longitudinal coordinate of the position of the satellite.

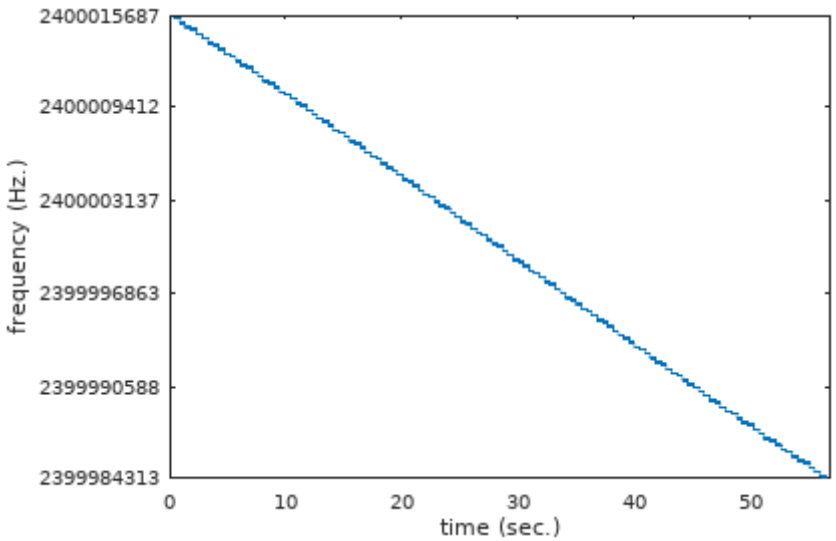

Figure 5.15: A graph showing the change in frequency of the satellite transmission as it orbits above the ground station and continues to move away from the ground station. As the angle θ increased, the frequency of the transmission decreased. The frequency was plotted for 56 seconds and, for the first half of the transmission, as the satellite moved directly overhead the ground station, the frequency decreased by 15 687 Hz, resulting in a frequency equal to the initial frequency of 2.4 GHz. As the satellite moved away, the frequency decreased further by 15 687 Hz. The total change in frequency for the duration of 56 seconds was 31.374 kHz.

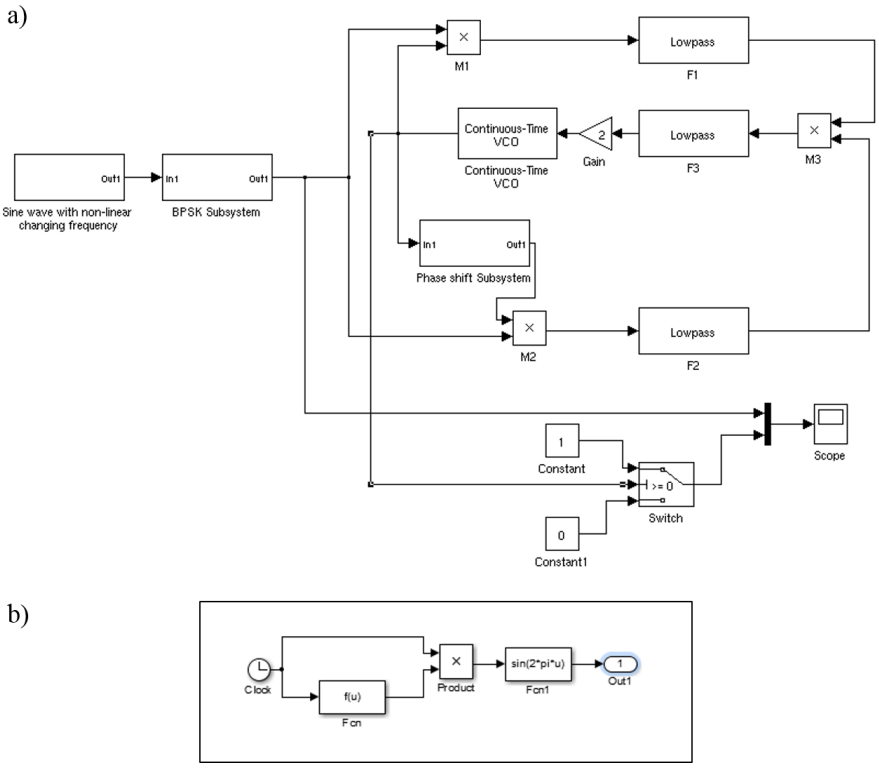

Figure 5.16: A figure showing a) the simulation of the Costas loop, used to extract the carrier signal from a BPSK modulated sinusoidal wave. The BPSK modulated signal and the output of the VCO are displayed on the scope. The VCO output was converted into a square wave using a switch in order to extract the synchronisation signal used to trigger Bob's components. The result of this simulation is shown in Figure 5.19. The frequency of the sine wave varied non-linearly and a schematic of the subsystem used to create the sine wave is shown in b). The time-dependent function derived to describe the change in frequency of the signal is shown in the function block f(u). The output of the function and the time variable (clock) were multiplied to form the input of the sine wave function block, sin(2*pi*u). The output of the subsystem formed a sinusoidal wave with frequency varying non-linearly with time.

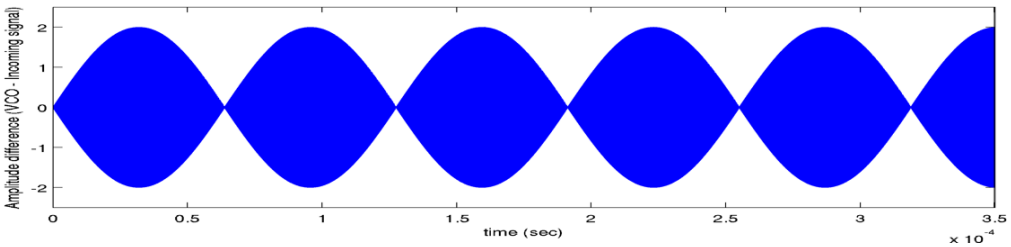

Figure 5.17: A graph showing the amplitude difference between Alice's signal and Bob's VCO signal. In the non-linear case using the parameters listed in Table 5.1, the frequencies of the two signals differed by 15 687 Hz at the beginning of the transmission, hence the signals move in and out of phase with each other at a faster rate compared to the linear case. In this graph, the signals are out of phase by π rad at 31.8 μs.

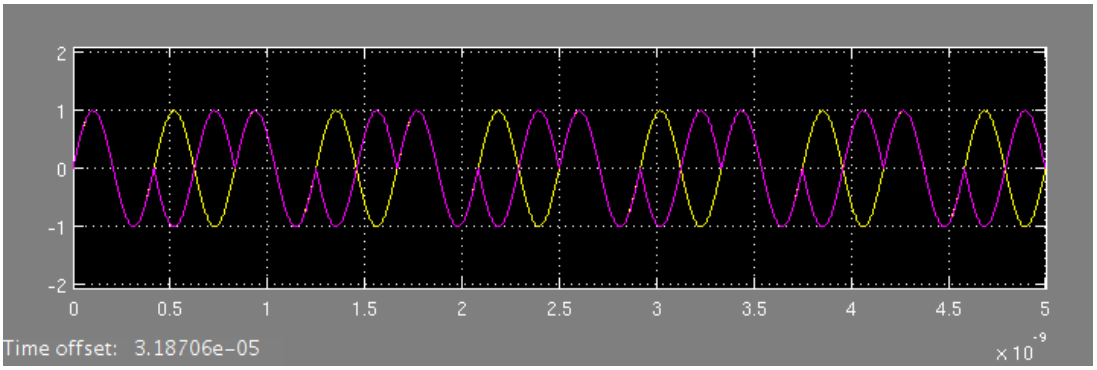

Figure 5.18: A figure showing the synchronisation maintained between the BPSK signal from Alice and the VCO in Bob's module. The BPSK signal is shown in pink and the output of the VCO is shown in yellow. The results in this figure are a 5 ns snapshot of the signals, taken after 31.87 μs of transmission. The results show that the VCO is able to adjust its frequency to match Alice's signal and recreate the effect of the Doppler shift in Bob's synchronisation signal. At 31.87 μs, the signals would have been out of phase by π rad without the effect of the VCO, but as shown in this figure, the simulated Costas loop was able to maintain the phase between the signals.

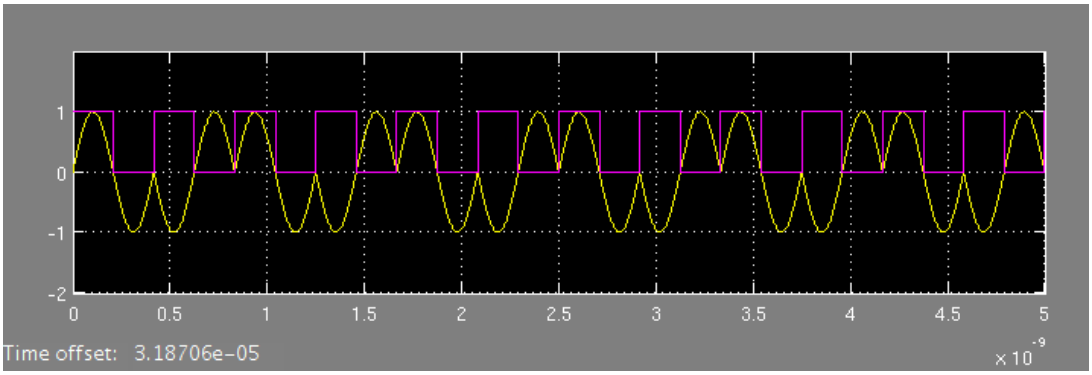

Figure 5.19: A figure showing the extraction of the synchronisation signal from the VCO output. The original BPSK modulated signal from Alice is shown in yellow. The results in this figure are a 5 ns snapshot of the signals, taken after 31.87 μs of transmission. The output of the VCO in Bob's module was converted to a square wave, shown in pink, which can be used to trigger Bob's QKD components. The synchronisation signal was able to match the frequency of the BPSK signal as it changed due to Doppler effects. This will ensure that Bob's detectors will take measurements at the precise time of the arrival of a photon from Alice and the key generation rate of the system will not decrease due to a timing mismatch.

5.5 Discussion

The synchronisation system for satellite QKD must be developed to compensate relativistic effects in order to implement QKD using LEO satellites. To date, geostationary satellites have been considered for QKD transmission but the use of LEO satellites will allow for greater flexibility in the serviceable area for each satellite. The use of the COW protocol in a free space channel will rely heavily on accurate synchronisation between Alice and Bob since the time of arrival of pulses contains the bit value for each qubit. The work presented in this chapter proves through simulations that the use of a Costas loop will be effective in maintaining the synchronisation between an orbiting satellite and a stationary ground station. The next step for this application would be to demonstrate this proof of principle using a satellite link. We aim towards the planning and implementation of the COW protocol via satellite for future work.

6 Conclusion

The necessity for secure data transmissions has become more prevalent in today's data-driven society. With the increase use of services such as internet banking and e-voting, unconditional encryption security needs to become available for individual use. QKD provides a secure means to distribute an encryption key between authenticated parties and the recent research trends on handheld QKD devices can facilitate the implementation of QKD technology for personal use. While research for handheld devices to date has focused on the use of polarisation states to encode qubits, this project proposed the design of a handheld device using the COW protocol. The practical implementation and compact size of the Alice module for this protocol made it well suited for a handheld device.

A laboratory prototype of the Alice module and the detection line of the Bob module was built. An optical synchronisation system between Alice and Bob was built and tested. The optical synchronisation system allowed for a wireless connection between the modules which could serve as the synchronisation link as well as the public channel. The key distribution was characterised by measuring the sifted key rate and QBER of the system. The sifted key rate was consistent with the theoretical prediction for this setup. The QBER was due to the dark counts of the single photon detector, since the measurements were taken under dark conditions and there were no errors due to background noise.

The implementation of the COW protocol for QKD between a ground station and a LEO satellite was proposed. Simulations were done to investigate the modulation and demodulation of the synchronisation signal between the Alice and Bob modules. The Costas loop was implemented in the simulations in order to compensate for Doppler shifts in the frequency of the synchronisation signal due to the trajectory of the satellite. The experiments and simulations proposed in this work are aimed towards making QKD a contemporary encryption technology. In order to build a quantum network with both short range and long range channels, spanning over fibre optic and free space networks, each component of the network must be optimised and integrated.

Future work

In order to complete the design and implementation of the COW protocol for a handheld device, the monitoring line for Bob's module must be developed and tested. The monitoring line consists of a Mach-Zehnder interferometer and two single photon detectors. The visibility of the interferometer must be characterised for the system by monitoring the typical count rates for each detector. The presence of an eavesdropper can be identified with changes to the visibility of the interferometer during transmission. In order to create a practical monitoring line, the length of the optical delay line in the long arm of the interferometer must be suitable for single photon transmission. If the delay line is too long, the loss of the system would be too significant and it would not be possible to determine the interferometer visibility. The length of the delay line is proportional to the pulse width and the time between each pulse, created by Alice's modulator. The next step for this project would be to replace the optical modulator used for the laboratory implementation with a faster modulator, which can be controlled by a QRNG. The optical synchronisation system must be adjusted to suit the design of the modulator, alternatively, radio synchronisation can be used for the system.

Once a faster modulator and QRNG have been implemented, the system can be tested using longer bit sequences, particularly with sequences of recurring 1's or 0's. Telecommunications systems are tested using long bits sequences of the length of $2^{23} - 1$ bits. While this was not practical to implement with the optical chopper wheel, it can be implemented with a lithium niobate modulator. The only components in the system that may be affected by bit patterning are the single photon detectors. At high bit rates, approaching the quenching time of the detector, a recurring sequence of 1's, i.e. decoy sequences, may cause an avalanche effect that is not quenched. It will be important to test the upper limit of the bit rate with patterning effects in mind.

The software used for the post processing of the key must be extended to include the monitoring line. Bob's software must be able to acquire measurements from the detection line detector and both monitoring line detectors simultaneously and store the measurements for post processing. The programme must monitor which detector clicked for each time bin so that Alice and Bob can discard the detector clicks from the monitoring line from the sifted key. The programme should also monitor simultaneous detections in more than one detector. The programme should alert the users if the occurrences of double clicks is too high in relation to the dark count rate of the detectors. This could be as a result of a high average photon number per pulse or an excess of dark counts due to a detector malfunction. The miniaturisation of the Alice and Bob modules will steer towards making this system commercially viable. The aim for the Alice module, in particular, is to design an

on-chip optical and electronic system which can be easily integrated into mobile devices or used as a compact, stand-alone device.

Once the full system has been set up for the automated implementation of the COW protocol, different eavesdropping techniques can be implemented to test the system's robustness. A simple intercept-resend attack can be used to characterise the monitoring line [66]. Other eavesdropping techniques which exploit the practical vulnerabilities of the system can also be tested. This includes detector blinding [65] and trojan horse attacks [67] which interrogate the Alice module with bright light.

The implementation of the COW protocol presented in this thesis used an optical wavelength of 808 nm. An investigation can be done on the feasibility of using an optical wavelength of 1550 nm. This is a wavelength typically used for fibre optic communication but it is also able to transmit through a free space medium without high loss or dispersion. The use of 1550 nm will decrease the sensitivity of the system to background light, making the device simpler to implement in daylight conditions. It would also allow for a simpler integration into a fibre optic network, necessary for the transmission between a node and central node. The detectors used for the 1550 nm range are typically of low efficiency. In order to optimise the detection efficiency, superconducting detectors can be used to increase the detection rate and minimise noise.

A study by Chun *et al*. developed a motion compensation system for use with handheld QKD devices [134]. The compensation system used a dynamic beam-steering technique which included electro-mechanical mirrors and an LED tracking system for feedback. The use of reference-frame-independent, polarisation based coding allowed for variations in the orientation of the measurement basis, without affecting the key generation rate of the system. The use of the COW protocol does not require reference-frame-independent coding, since the measurement apparatus is not directionally dependent. The dynamic beam-steering system will be an advantageous addition to the handheld device, as this will allow for a longer transmission window and, therefore, a longer secret key.

The investigation of a satellite application for the COW protocol can be expanded to a practical demonstration. The compensation techniques for the relativistic effects must be implemented by building and testing a Costas Loop and linking it to the central clock in Bob's apparatus. In order to implement the proposed COW protocol device over a long range, free-space channel, compensating techniques must be set in place against the turbulence effects of the atmosphere. The device must also be combined with the continuous-variable QKD techniques proposed in [59], introduced in Chapter 5.

7

Appendices

A1. Synchronisation software code written with Arduino software

```
void setup() {
Serial.begin(9600);
pinMode(13,INPUT); // Trigger signal input
pinMode(12,OUTPUT); // Trigger command OUTPUT
pinMode(10,INPUT); // Photodetector key   }

void loop() {
byte c=0;
byte k[100];// key string
byte app;// Momentary storage variable
byte loopcount=0;

while(c<100){
digitalWrite(12,LOW);
while (digitalRead(13)==HIGH){
loopcount =0;}

while (digitalRead(13)==LOW){
if (loopcount==0) {
digitalWrite(12,HIGH);
app=digitalRead(10); // Read the key bit
        k[c]=app;
```

```
digitalWrite(12,LOW);
loopcount = 1;
       }
}
c=c+1;
}
Serial.print(String (k[c]));
```

A2. Key sifting software code written with Matlab

```
%read in the raw key
raw_key = load('data.txt');

% batch size
batch = 5000;

% get the size of the data file
[rows cols] = size(raw_key);

% create the sifted key array
sifted_key = 0;

% loop counter for sifted key array
id = 1;
% output to file
fid = fopen('output.txt', 'w');

% create the output arrays
num_batch = rows/batch;
loss  = zeros( 1, num_batch );
error = zeros( 1, num_batch );
key   = zeros( 1, num_batch );
decoy = zeros( 1, num_batch );

batch_id = 1;

fprintf('Output from the program \n');
```

```
fprintf('========================= \n\n');

for i = 1 : batch : rows
for j = i : 2 : i+(batch-2)

% read in point 1
a = raw_key( j );
b = raw_key( j+1 );

if    ( a == 0 && b == 0 )
loss( batch_id ) = loss( batch_id ) + 1;

   elseif( a == 0 && b == 1 )
sifted_key = 0;
error( batch_id ) = error( batch_id ) + 1;

   % write to file
fprintf(fid, '%d \n', sifted_key);

   elseif( a == 1 && b == 0 )
sifted_key = 1;
key( batch_id ) = key( batch_id ) + 1;

   % write to file
fprintf(fid, '%d \n', sifted_key);

   elseif( a == 1 && b == 1 )
decoy( batch_id ) = decoy( batch_id ) + 1;
       end
end

batch_id = batch_id + 1;
end
% close output file
fclose(fid);
```

Bibliography

[1] Mirza A. Towards Practical Quantum Cryptography. MSc Thesis. 2009;University of KwaZulu-Natal.

[2] Stucki D, Brunner N, Gisin N, Scarani V, Zbinden H. Fast and simple one-way quantum key distribution. Applied Physics Letters. 2005;87(19):194108.

[3] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N, Scarani V. Towards practical and fast quantum cryptography. arXiv preprint. 2004;quant-ph/0411022.

[4] Chen W, Han ZF, Zhang T, Wen H, Yin ZQ, Xu FX, et al. Field experiment on a star type metropolitan quantum key distribution network. IEEE Photonics Technology Letters. 2009;21(9):575–577.

[5] Duligall J, Godfrey M, Harrison K, Munro W, Rarity J. Low cost and compact quantum key distribution. New Journal of Physics. 2006;8(10):249.

[6] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Reviews of Modern Physics. 2002;74(1):145.

[7] [Online]. Zener Diagram; Available at. http://www.elemania.altervista.org/diodi/immagini/ZenerDiagram.jpg.

[8] [Online]. Guide to detector selection; Available at. http://www.hamamatsu.com/jp/en/community/optical_sensors/articles/guide_to_detector_selection/index.html.

[9] [Online]. SPCM-AQ Single-Photon Counting Module Data Sheet; Available at. https://sites.fas.harvard.edu/ phys191r/Bench_Notes/D4/SPCMAQR.pdf.

[10] [Online]. Dupuy P, Cryptology; Available at. http://hiwaay.net/ paul/cryptology/history.html.

[11] [Online]. Williams Stallings; Available at. http://williamstallings.com/Extras/Security-Notes/lectures/classical.html.

[12] Kozaczuk W. Enigma: how the German machine cipher was broken, and how it was read by the Allies in World War Two. Univ Pubns of Amer; 1984.

[13] Stucki D, Legre M, Buntschu F, Clausen B, Felber N, Gisin N, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New Journal of Physics. 2011;13(12):123001.

[14] Ferguson B N Schneier. Practical Cryptography. John Wiley and Sons Inc.; 2003. 207-222.

[15] Katzenbeisser S. Recent advances in RSA cryptography. vol. 3. Springer Science & Business Media; 2001.

[16] Ghernaouti-Helie S, Tashi I, Laenger T, Monyk C. SECOQC business white paper. arXiv preprint. 2009;arXiv:0904.4073.

[17] Konheim A. Cryptography: A Primer. John Wiley and Sons Inc.; 1981.

[18] Shannon CE. Communication theory of secrecy systems. Bell Labs Technical Journal. 1949;28(4):656–715.

[19] Weedbrook C, Pirandola S, García-Patrón R, Cerf NJ, Ralph TC, Shapiro JH, et al. Gaussian quantum information. Reviews of Modern Physics. 2012;84(2):621.

[20] Deng FG, Long GL. Secure direct communication with a quantum one-time pad. Physical Review A. 2004;69(5):052319.

[21] Wiesner S. Conjugate coding. ACM Sigact News. 1983;15(1):78–88.

[22] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing Int. In: Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984); 1984. p. 175–179.

[23] Nielsen MA, Chuang I. Quantum information Processing and Communication. United Kingdom: Cambridge University Press; 2002.

[24] Renner R. Security of quantum key distribution. International Journal of Quantum Information. 2008;6(01):1–127.

[25] De Broglie L. Matter and Light-The New Physics. Read Books Ltd; 2013.

[26] Zettili N. Quantum mechanics: concepts and applications. John Wiley and Sons Inc.; 2003. p28.

[27] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982;299(5886):802–803.

[28] Scarani V. Quantum physics: a first encounter: interference, entanglement, and reality. Oxford University Press; 2006. 67-80.

[29] Kwiat PG, Mattle K, Weinfurter H, Zeilinger A, Sergienko AV, Shih Y. New high-intensity source of polarization-entangled photon pairs. Physical Review Letters. 1995;75(24):4337.

[30] Chen G, Church DA, Englert BG, Henkel C, Rohwedder B, Scully MO, et al. Quantum computing devices: principles, designs, and analysis. CRC press; 2006.

[31] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. Journal of Cryptology. 1992;5(1):3–28.

[32] Hecht E. Optics. Reading MA: Addison-Wesley; 2001. 325-379.

[33] Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters. 1992;68(21):3121.

[34] Ma L, Xu H, Tang X. Polarization recovery and auto-compensation in quantum key distribution network. National Inst of Standards and Technology Gaithersburg MD; 2006.

[35] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H, Gisin N. Plug and play systems for quantum cryptography. Applied Physics Letters. 1997;70(7):793–795.

[36] Hughes RJ, Morgan GL, Peterson CG. Quantum key distribution over a 48 km optical fibre network. Journal of Modern Optics. 2000;47(2-3):533–547.

[37] Fickler R, Lapkiewicz R, Plick WN, Krenn M, Schaeff C, Ramelow S, et al. Quantum entanglement of high angular momenta. Science. 2012;338(6107):640–643.

[38] Marcikic I, De Riedmatten H, Tittel W, Zbinden H, Legré M, Gisin N. Distribution of time-bin entangled qubits over 50 km of optical fiber. Physical Review Letters. 2004;93(18):180502.

[39] Hughes RJ, Nordholt JE. Long-range Quantum Cryptography: Amplified Quantum Key Distribution (AQKD). arXiv preprint. 2014;arXiv:1406.6990.

[40] Van Loock P, Ladd T, Sanaka K, Yamaguchi F, Nemoto K, Munro W, et al. Hybrid quantum repeater using bright coherent light. Physical Review Letters. 2006;96(24):240501.

[41] Wabnig J, Bitauld D, Li H, Laing A, O'Brien J, Niskanen A. Demonstration of free-space reference frame independent quantum key distribution. New Journal of Physics. 2013;15(7):073001.

[42] Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science. 1999;283(5410):2050–2056.

[43] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Reviews of Modern Physics. 2009;81(3):1301.

[44] Buttler WT, Lamoreaux SK, Torgerson JR, Nickel G, Donahue C, Peterson CG. Fast, efficient error reconciliation for quantum cryptography. Physical Review A. 2003;67(5):052303.

[45] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A. Quantum privacy amplification and the security of quantum cryptography over noisy channels. Physical Review Letters. 1996;77(13):2818.

[46] Lo HK, Zhao Y. Quantum cryptography. arXiv preprint. 2008;arXiv:0803.2507.

[47] Hwang WY, Ahn DD, Hwang SW. Eavesdropper's optimal information in variations of Bennett–Brassard 1984 quantum key distribution in the coherent attacks. Physics Letters A. 2001;279(3):133–138.

[48] Mirza A, Petruccione F. Realizing long-term quantum cryptography. JOSA B. 2010;27(6):A185–A188.

[49] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters. 2000;85(2):441.

[50] Scarani V, Acin A, Ribordy G, Gisin N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters. 2004;92(5):057901.

[51] Lutkenhaus N, Jahma M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New Journal of Physics. 2002;4(1):44.

[52] Hwang WY. Quantum key distribution with high loss: toward global secure communication. Physical Review Letters. 2003;91(5):057901.

[53] Ekert AK. Quantum cryptography based on BellŠs theorem. Physical Review Letters. 1991;67(6):661.

[54] Grosshans F, Acin A, Cerf N. Continuous-variable quantum key distribution. In: Quantum Information With Continuous Variables Of Atoms And Light. World Scientific; 2007. p. 63–83.

[55] Furrer F, Franz T, Berta M, Leverrier A, Scholz VB, Tomamichel M, et al. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. Physical Review Letters. 2012;109(10):100502.

[56] Usenko V, Lasota M, Filip R. Continuous-and discrete-variable quantum key distribution with nonclassical light over noisy channels. In: Telecommunications and Signal Processing (TSP), 2016 39th International Conference on. IEEE; 2016. p. 753–756.

[57] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Physical Review A. 2007;76(4):042305.

[58] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photonics. 2013;7(5):378–381.

[59] Gunthner K, Khan I, Elser D, Stiller B, Bayraktar O, Muller CR, et al. Quantum-limited measurements of optical signals from a geostationary satellite. Optica. 2017;4(6):611–616.

[60] Inoue K, Honjo T. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. Physical Review A. 2005;71(4):042305.

[61] Inoue K, Waks E, Yamamoto Y. Differential phase shift quantum key distribution. Physical Review Letters. 2002;89(3):037902.

[62] Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, et al. Chip-based quantum key distribution. Nature Communications. 2017;8:13984.

[63] Gottesman D, Lo HK, Lutkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. In: Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on. IEEE; 2004. p. 136.

[64] Hu Y, Peng X, Li T, Guo H. On the Poisson approximation to photon distribution for faint lasers. Physics Letters A. 2007;367(3):173–176.

[65] Vakhitov A, Makarov V, Hjelme DR. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. Journal of Modern Optics. 2001;48(13):2023–2038.

[66] Makarov V, Hjelme DR. Faked states attack on quantum cryptosystems. Journal of Modern Optics. 2005;52(5):691–705.

[67] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G. Trojan-horse attacks on quantum-key-distribution systems. Physical Review A. 2006;73(2):022320.

[68] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C, Leuchs G. Trojan-horse attacks threaten the security of practical quantum cryptography. New Journal of Physics. 2014;16(12):123030.

[69] Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Physical Review Letters. 2012;108(13):130503.

[70] Moroder T, Curty M, Lim CCW, Thinh LP, Zbinden H, Gisin N. Security of Distributed-Phase-Reference Quantum Key Distribution. Physical Review A. 2012;109(26):260501.

[71] Branciard C, Gisin N, Scarani V. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. New Journal of Physics. 2008;10(1):013031.

[72] Stucki D, Barreiro C, Fasel S, Gautier JD, Gay O, Gisin N, et al. Continuous high speed coherent one-way quantum key distribution. Optics Express. 2009;17(16):13326–13334.

[73] Korzh B, Lim CCW, Houlmann R, Gisin N, Li MJ, Nolan D, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photonics. 2015;9(3):163–168.

[74] Elliott C. The DARPA quantum network. Quantum Communications and Cryptography. 2006;p. 83–102.

[75] Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, et al. Field test of quantum key distribution in the Tokyo QKD Network. Optics Express. 2011;19(11):10387–10409.

[76] Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics. 2009;11(7):075001.

[77] [Online]. Durban's high tech stadium; Available at. http://www.fifa.com/worldcup/news/y=2010/m=5/news=durban-high-tech-stadium-1217593.html.

[78] Lancho D, Martinez J, Elkouss D, Soto M, Martin V. QKD in standard optical telecommunications networks. In: International Conference on Quantum Comunication and Quantum Networking. Springer; 2009. p. 142–149.

[79] Vallone G, Marangon DG, Canale M, Savorgnan I, Bacco D, Barbieri M, et al. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. Physical Review A. 2015;91(4):042320.

[80] Ji L, Gao J, Yang AL, Feng Z, Lin XF, Li ZG, et al. Towards quantum communications in free-space seawater. Optics Express. 2017;25(17):19795–19806.

[81] Kihara M, Nagasawa S, Tanifuji T. Return loss characteristics of optical fiber connectors. Journal of Lightwave Technology. 1996;14(9):1986–1991.

[82] Hecht J, Long L. Understanding fiber optics. vol. 3. 4th ed. Columbus: Prentice-Hall; 2002.

[83] [Online]. Application Notes; Available at. www.kingfisherfiber.com.

[84] [Online]. Chromatic dispersion; Available at. http://www.fiberoptic.com/fiber_characterization/pdf/chromatic_dispersion.pdf.

[85] [Online]. Optical Fibres; Available at. http://macao.communications.museum/eng/exhibition/secondfloor/MoreInfo/2_8_3_OpticalFibres.html.

[86] Gobby C, Yuan Z, Shields A. Quantum key distribution over 122 km of standard telecom fiber. Applied Physics Letters. 2004;84(19):3762–3764.

[87] Stucki D, Walenta N, Vannel F, Thew RT, Gisin N, Zbinden H, et al. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. New Journal of Physics. 2009;11(7):075003.

[88] Takesue H, Nam SW, Zhang Q, Hadfield RH, Honjo T, Tamaki K, et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. Nature Photonics. 2007;1(6):343–348.

[89] Astafiev O, Abdumalikov Jr A, Zagoskin AM, Pashkin YA, Nakamura Y, Tsai J. Ultimate on-chip quantum amplifier. Physical Review Letters. 2010;104(18):183603.

[90] Dixon AR, Yuan Z, Dynes J, Sharpe A, Shields A. Continuous operation of high bit rate quantum key distribution. Applied Physics Letters. 2010;96(16):161102.

[91] Yuan Z, Dixon A, Dynes J, Sharpe A, Shields A. Gigahertz quantum key distribution with InGaAs avalanche photodiodes. Applied Physics Letters. 2008;92(20):201104.

[92] Patel K, Dynes J, Choi I, Sharpe A, Dixon A, Yuan Z, et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. Physical Review X. 2012;2(4):041010.

[93] Ramaswami R, Sivarajan K, Sasaki G. Optical networks: a practical perspective. Morgan Kaufmann; 2009.

[94] Capraro I, Tomaello A, DallŠArche A, Gerlin F, Ursin R, Vallone G, et al. Impact of turbulence in long range quantum and classical communications. Physical Review Letters. 2012;109(20):200502.

[95] Resch K, Lindenthal M, Blauensteiner B, Böhm H, Fedrizzi A, Kurtsiefer C, et al. Distributing entanglement and single photons through an intra-city, free-space quantum channel. Optics Express. 2005;13(1):202–209.

[96] Capraro I, Occhipinti T, Bonora S, Villoresi P. Free space quantum key distribution system with atmospheric turbulence mitigation by active deformable mirror. In: International Conference on Quantum Information. Optical Society of America; 2008. p. JMB64.

[97] Benton DM, Gorman PM, Tapster PR, Taylor DM. A compact free space quantum key distribution system capable of daylight operation. Optics Communications. 2010;283(11):2465–2471.

[98] Liao SK, Yong HL, Liu C, Shentu GL, Li DD, Lin J, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. Nature Photonics. 2017;11(8):509–513.

[99] Scheidl T, Ursin R, Fedrizzi A, Ramelow S, Ma XS, Herbst T, et al. Feasibility of 300 km quantum key distribution with entangled states. New Journal of Physics. 2009;11(8):085002.

[100] Villoresi P, Jennewein T, Tamburini F, Aspelmeyer M, Bonato C, Ursin R, et al. Experimental verification of the feasibility of a quantum channel between space and Earth. New Journal of Physics. 2008;10(3):033038.

[101] Mariola M, Mirza AR, Petruccione F. System and method for identifying and/or measuring orientation mismatches between stations. Google Patents; 2015. US Patent App. 15/310,625.

[102] Tan MR, Fattal DA, Morris T. Misalignment tolerant free space optical transceiver. Google Patents; 2012. US Patent 8,315,526.

[103] Vest G, Rau M, Fuchs L, Corrielli G, Weier H, Nauerth S, et al. Design and evaluation of a handheld quantum key distribution sender module. IEEE Journal of Selected Topics in Quantum Electronics. 2015;21(3):131–137.

[104] Nordholt JE, Hughes RJ, Newell RT, Peterson CG, Rosenberg D, McCabe KP, et al.. Quantum key distribution using card, base station and trusted authority. Google Patents; 2017. US Patent 9,680,641.

[105] Bunandar D, Lentine A, Lee C, Cai H, Long CM, Boynton N, et al. Metropolitan quantum key distribution with silicon photonics. arXiv preprint. 2017;arXiv:1708.00434.

[106] Sanguinetti B, Martin A, Zbinden H, Gisin N. Quantum random number generation on a mobile phone. Physical Review X. 2014;4(3):031056.

[107] Consortini A, Ronchi L, Scheggi AM, di Francia GT. Deterioration of the Coherence Properties of a Laser Beam by Atmospheric Turbulence and Molecular Scattering. Radio Science. 1966;1(4):523–530.

[108] Noh CH, Asada T. Liquid crystal optical shutter. Google Patents; 1995. US Patent 5,455,083.

[109] Yahav G, Iddan GJ. Opto-electronic shutter. Google Patents; 2001. US Patent 6,327,073.

[110] de Sterke CM, van der Laan CJ, Frankena HJ. Nonpolarizing beam splitter design. Applied Optics. 1983;22(4):595–601.

[111] Hadfield RH. Single-photon detectors for optical quantum information applications. Nature Photonics. 2009;3(12):696–705.

[112] Zetie KP, Adams SF, Tocknell RM. How does a Mach-Zehnder interferometer work? Physics Education. 2000;35(1):46.

[113] [Online]. idQuantique Clavis 3; Available at. https://www.idquantique.com/single-photon-systems/products/clavis3-qkd-platform/.

[114] Ribordy G, Gautier JD, Zbinden H, Gisin N. Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters. Applied Optics. 1998;37(12):2272–2277.

[115] [Online]. What's a SPAD?; Available at. http://www.everyphotoncounts.com/spad.php.

[116] Buller G, Warburton R, Pellegrini S, Ng J, David J, Tan L, et al. Single-photon avalanche diode detectors for quantum key distribution. IET optoelectronics. 2007;1(6):249–254.

[117] Castelletto S, Degiovanni IP, Schettini V, Migdall AL. Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array. Journal of Modern Optics. 2007;54(2-3):337–352.

[118] Hiskett PA, Rosenberg D, Peterson CG, Hughes RJ, Nam S, Lita A, et al. Long-distance quantum key distribution in optical fibre. New Journal of Physics. 2006;8(9):193.

[119] [Online]. ATmega328; Available at. http://www.microchip.com/wwwproducts/en/ATmega328.

[120] Mariola M, Ismail Y, Petruccione F. Open source electronic board designed in South Africa for Africa. In: of the 60th Annual Conference of the South African Institute of Physics (SAIP2015) TP, editor. Makaiko Chithambo (RU) and André Venter (NMMU); 2015. p. 457–462.

[121] Stucki D, Barreiro C, Fasel S, Gautier J, Gay O, Gisin N, et al. High speed coherent one-way quantum key distribution prototype (2008). arXiv preprint;arXiv:0809.5264.

[122] [Online]. Energy of a photon; Available at. http://www.pveducation.org/pvcdrom/properties-of-sunlight/energy-of-photon.

[123] [Online]. Edmund Optics; Available at. https://www.edmundoptics.com/resources/application-notes/optics/understanding-neutral-density-filters/.

[124] Lydersen L, Skaar J, Makarov V. Tailored bright illumination attack on distributed-phase-reference protocols. Journal of Modern Optics. 2011;58(8):680–685.

[125] Carter JL, Wegman MN. Universal classes of hash functions. Journal of Computer and System Sciences. 1979;18(2):143–154.

[126] Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. Physical Review Letters. 2007;98(1):010504.

[127] Mariola M, Mirza A, Petruccione F. Quantum cryptography for satellite communication. In: the 56th Annual Conference of the South African Institute of Physics S, editor. I. Basson and A.E. Botha (University of South Africa, Pretoria); 2011. p. 403–408.

[128] [Online]. Asynchronous Transmission; Available at. http://www.pccompci.com/Asynchronous_ and Synchronous_ Communication.html.

[129] Bernardini A. Lezioni del corso di sistemi di comunicazione satellitari. vol. 1. Edizioni Ingegneria (Rome); 2008. 403-408.

[130] Kostopoulos A. Corso di telecomunicazioni. Dai sistemi di comunicazione ai servizi telematici. 2nd ed. (Petrini); 1995. 466-467.

[131] [Online]. Voltage Controlled Oscillator User Manual; Available at. https://www.fairviewmicrowave.com/images/productPDF/FMVC31012.pdf.

[132] Mariola M. Free space communication in quantum key distribution. PhD Thesis. 2015;University of KwaZulu-Natal.

[133] [Online]. Chirp Signal; Available at. https://www.mathworks.com/help/dsp/ref/chirp.html.

[134] Chun H, Choi I, Faulkner G, Clarke L, Barber B, George G, et al. Motion-Compensated Handheld Quantum Key Distribution System. arXiv preprint. 2016;arXiv:1608.07465.