UNIVERSITY OF CALGARY

Quantum Key Distribution with Temporal Mode Encoding

by

Allison Rubenok

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF PHYSICS AND ASTRONOMY

INSTITUTE FOR QUANTUM INFORMATION SCIENCE

CALGARY, ALBERTA

September, 2011

UNIVERSITY OF CALGARY
FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Quantum Key Distribution with Temporal Mode Encoding" submitted by Allison Rubenok in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE.

Supervisor, Dr. Wolfgang Tittel
Department of Physics and Astronomy

Dr. Christoph Simon
Department of Physics and Astronomy

Dr. Eric Donovan
Department of Physics and Astronomy

Dr. Mike Potter
Department of Electrical and Computer Engineering

Sept 23, 2011
Date

Abstract

Quantum Key Distribution (QKD) exploits the principles of quantum mechanics in order to achieve the secure distribution of a cryptographic key between two parties. QKD is able to provide unconditional security, which is unattainable with the use of conventional cryptographic techniques. This thesis provides a side-by-side comparison of two different QKD systems employing different methods of temporal mode qubit encoding. To achieve this, the QKD systems were designed and implemented in a proof-of-principle demonstration. Furthermore, an active stabilization system based on quantum frames, consisting of alternating bursts of strong pulses and quantum data sent over the same communication channel, was developed and implemented over the course of this work.

Acknowledgements

First, thank you to my supervisor Dr. Wolfgang Tittel for all of his help, support, and encouragement over the course of this degree. As well thank you to members of the QC2 lab: Terence Stuart, Jeongwan Jin, Félix Bussières, Michael Lamont, Ahdiyeh Delfan, Neil Sinclair, Erhan Seglamyurek, Cecilia La Mela, Daniel Oblak, Chris Healey, Steve Hosier, Vladimir Kiselyov and especially the crypto team who provided a lot of advice througout this work: Itzel Lucio Martinez, Philip Chan and Xiaofan Mo. Thank you especially to Joshua Slater for advice and support (related to and unrelated to this project) and for being an amazing friend throughout all of this. Thank you to Tracy Korsgaard and Hyejeong Hwang for administrative support. Also to Pat Irwin for providing technical advice and a place to drink warm coke and have long conversations.

Thank you to all of the graduate students who have helped to make this a great experience: Adam D'Souza (for his excellent spatial mastery of conversation), Nathan Babcock, Michael Skotiniotis, Elliot Martin, Orion Penner, Jayme Derrah, Alexander Hentschel and Lydia Mitchell. As well my friends from outside of grad school[1]: Nicolas Choquette-Levy, Ray Crowder, Chris Dascollas, Randy Squires, Robin Hunter, Zach High-Leggett, Benjamin Blumer, Katie Underwood, Monika Deviat, Kristina Wasyleczko, Julia Pulwicki, Michael Underwood and John Nguyen. Especially to Jyotsna Kashyap who is an amazing friend and often able to find humor in even the most dismal situations. Thank you to all of my circus friends and military friends for helping me to maintain my sanity, especially the 2008 crews of the HMCS Edmonton and HMCS Nanimo.

Finally, thank you to my family: My parents Kent and Paulette Rubenok who have always encouraged me and supported every pursuit that I undertook and to my brother Robert Rubenok who always made fun of every pursuit that I undertook.

[1]This does not necessarily mean they are not graduate students

Table of Contents

List of Tables

List of Figures

Glossary

μ	Mean Number of Photons per Pulse
AES	Advanced Encryption Standard
APD	Avalanche Photodiode
ASE	Amplified Spontaneous Emission
BS	Beam Splitter
CHSH	J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt
DES	Data Encryption Standard
EPR	A. Einstein, B. Podolsky and N. Rosen
FM	Faraday Mirror
InGaAs	Indium Gallium Arsenide
IM	Intensity Modulator
LD_C	Classical Laser Diode
LD_Q	Quantum Laser Diode
LDPC	Low Density Parity Check
PBS	Polarizing Beam Splitter
PM	Phase Modulator
PNS	Photon Number Splitting
QBER	Quantum Bit Error Rate
QC2 lab	Quantum Cryptography and Communication Labs
QKD	Quantum Key Distribution
RSA	R. Rivest, A. Shamir, and L. Adleman
SPD	Single Photon Detector
TDC	Time-to-Digital Converter

Chapter 1

Introduction

Ensuring the security of information, which involves keeping information secret, is a problem that has concerned humanity throughout all of history. Nearly everyone has information that he wants protected. This includes individuals who want their personal correspondence kept private, all the way up to governments who need to protect knowledge concerning matters of national security from falling into the wrong hands.

1.1 The History of Secure Communication

Keeping information protected requires the ability to safely store information, but it is also often required to communicate information securely between two physically separated parties. Out of the need for secure communication the field of cryptology has developed, devoted to the science of secure communication. Cryptology has two main branches. The first is cryptography, which involves techniques for hiding and recovering the meaning of a message, usually using some additional information known as the key. The second is cryptanalysis, which involves methods for uncovering the content of a message whose meaning has been hidden, without any prior knowlege of the key.

Communication takes place between two parties often denoted as Alice, the sender, and Bob, the receiver. Before transferring a message to Bob, Alice hides its meaning through a process called encryption. Bob receives the encrypted message and recovers the original message using the key, this process is called decryption. The goal of cryptography is to prevent an Eavesdropper, whom we will call Eve, from gaining access to the information. Eve can use cryptanalysis to try to find a way to gain access to the

message. If she succeeds then the encryption is said to be broken.

The complex history of cryptology has been a never ending battle with the constant development of new and better forms of encryption, and the continual progression of science and technology towards the ability to break increasingly advanced encryption techniques.

1.1.1 Classical Cryptography

The history of cryptology goes back nearly as far as the history of writing itself. Some of the earliest confirmed examples of encryption can be found in ancient Egyptian hieroglyphics dating back to 1900 BC [1]. For thousands of years the most common cryptographic algorithms or ciphers were based on simple substitutions and transpositions.

A transposition cipher is one in which the encrypted message (or ciphertext) is the result of letters of the original message (or plaintext) being scrambled into a different order. An example of this is writing the plaintext onto rows of a grid and then reading off the ciphertext as columns in some predetermined order. Transposition ciphers are relatively easy to break by shifting around chunks of the ciphertext and looking for patterns.

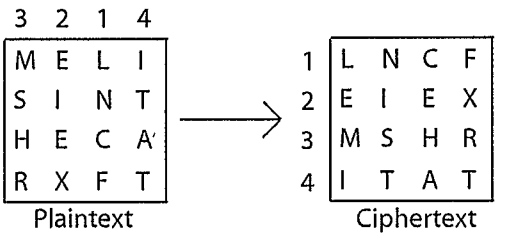

Figure 1.1: Transposition Cipher: The plaintext, "Mel is in the car" is written out from left to right along the rows of a 4x4 grid. Extra letters, 'xft', are added to fill in the grid. The key is the number 3214 written above the columns of the grid. The order of the columns is rearranged to be 1234 and each column is rewritten as a row in the 4x4 ciphertext grid. The resulting ciphertext is "LNCFEIEXMSHRITAT"

In the most basic form of a substitution cipher every letter of the plaintext maps onto a corresponding letter in the ciphertext. For example, in the famous Caesar shift cipher each letter of the alphabet is replaced by a letter three letters farther along in the alphabet. 'A' maps to 'D', 'B' maps to 'E' and so on. Letters at the end of the alphabet wrap back around such that 'Z' maps to 'C'. The Caesar shift cipher can also be generalized such that the ciphertext letters correspond to any shift (i.e. $n \neq 3$) of the plaintext alphabet that is selected. The cipher alphabet can also be any random permutation of the regular alphabet.

Simple substitution ciphers are easily broken through frequency analysis. The frequency of occurrence of each letter in the English language is given by table 1.1. This distribution is different and unique for every language. Given a large enough sample of ciphertext, these frequencies can be compared against the frequency of occurrence of letters contained in the ciphertext, and from this it is straightforward to deduce the ciphertext alphabet and uncover the message[1]. Digraphic substitution ciphers, where each pair of letters in the plaintext is mapped onto a pair of ciphertext letters make frequency analysis slightly more difficult, but far from impossible.

Another way to add complexity to a substitution cipher is by using multiple cipher alphabets, in what is called a polyalphabetic substitution cipher. Polyalphabetic substitution ciphers generally employ the use of a key that instructs how to encrypt each letter of the plaintext. The same key is used for the decryption process. It is essential that the key remains secret. A simple key would be in the form of a word or a phrase. Each letter of the key can represent a number that prescribes how far down the alphabet to shift the plaintext letter to generate the resulting ciphertext. For example if A = 0, B = 1 and so on, then the phrase "Mel is in the car" can be encrypted with the key "fold" as

[1]This is provided that the text was not written in any artificial manner, such as only using words that do not contain the letter 'e'.

Table 1.1: Letter Frequencies in English [2]

Letter	Frequency (%)	Letter	Frequency (%)
A	8.12	N	6.95
B	1.49	O	7.68
C	2.71	P	1.82
D	4.32	Q	0.11
E	12.02	R	6.02
F	2.30	S	6.28
G	2.03	T	9.10
H	5.92	U	2.88
I	7.31	V	1.11
J	0.10	W	2.09
K	0.69	X	0.17
L	3.98	Y	2.11
M	2.61	Z	0.07

shown in figure 1.2. The resulting ciphertext reads, "RSWLXWYWMSNDW".

If the length of the key is discovered, then the task of breaking a polyalphabetic substitution cipher reduces to that of breaking n monoalphabetic substitution ciphers, where n is the length of the key. Simple techniques exist for estimating the length of a key used in a polyalphabetic substitution cipher, such as the kappa test [3]. A longer key leads to more security as a larger sample of ciphertext is required in order to perform enough analysis to break the cipher.

The only way to ensure that the cipher cannot be broken no matter how much ciphertext an attacker has access to is by using a key that is completely random and as long as the message to be encrypted. This type of encryption, commonly called a one-time pad, was first formally proposed by Joseph Mauborgne in 1917 based on ideas by Gilbert Vernam [4]. It was proven unbreakable by Shannon in 1949 [5]. In practice there are a lot of difficulties with using a one-time pad, as the cipher is easily compromised if the key is not truly random or if the same key is used to encrypt more than one message. Also a unique key is required to be shared between each pair of parties wishing to communicate.

Plaintext	Key	Ciphertext
M = 12	F = 5	R = 17
E = 4	O = 14	S = 18
L = 11	L = 11	W = 22
I = 8	D = 3	L = 11
S = 18	F = 5	X = 23
I = 8	O = 14	W = 22
N = 13	L = 11	Y = 24
T = 19	D = 3	W = 22
H = 7	F = 5	M = 12
E = 4	O = 14	S = 18
C = 2	L = 11	N = 13
A = 0	D = 3	D = 3
R = 17	F = 5	W = 22

Figure 1.2: Example Encryption: The plain text is written down the leftmost column, each letter corresponding to a numeric value. The key is written down the central column repeating until the length of the plaintext is reached. The cipher text written down the rightmost column is found by adding together the numeric values of the plaintext and the key. For example: M + F = 12 + 5 = 17 = R

This results in the need for vast amounts of key material to be exchanged in advance and stored securely until it is required, often rendering a true one-time pad impractical.

By the the early 1900s most of the best ciphers were those combining both substitution and transposition. A well known example of this is the German World War I cipher ADFGVX, considered to be one of the most sophisticated ciphers of its time [1].

During World War II the use of rotor machines began. A rotor machine is a mechanized way to implement a polyalphabetic substitution cipher, allowing for the use of very long although not randomized keys. Rotor machines remained popular from the 1940s into the 1970s, but during this time the field of cryptography was slowly beginning to change. The advent of information theory and the emergence of computers into mainstream use allowed cryptography to enter a new age. Security could now be quantified and carefully analyzed, allowing cryptography and cryptanalysis to become more mathematically and computationally complex than had previously been possible.

1.1.2 Modern Cryptography

The 1970s saw two major advancements in the field of cryptography. One was the introduction of the Data Encryption Standard (DES) by the National Bureau of Standards, the first widely used standard for encryption [6]. DES was publically released and approved for both the encryption of classified government material as well as encryption of non-classified private material. It was the first time a government standard for cryptography was made publically available. Around the same time Diffie and Hellman published the first form of public key encryption [7]. Public key cryptography can also be called asymmetric to distinguish it from more traditional forms of cryptography, called symmetric, where the encryption and decryption keys are the same or easily derived from each other. The development of Diffie and Hellman's protocol was followed closely by the publication of RSA[8] (named for its creators Rivest, Shamir and Adleman) another public key algorithm that would become widely used. The development of DES and RSA, details of which are discussed in further detail below, made high level cryptography more publically accessible than ever before [4]. As well, both DES and public key cryptography depended heavily on the use of computers and helped to usher cryptography into the computer age.

This new reliance on computers brought about the notion of computational security. A cipher is considered to be computationally secure if breaking it would require more computational power than one would reasonably expect an adversary to have. For example, if it would take all of the computational power in the world hundreds of years to break a cipher, that cipher can be considered computationally secure. Computational security can be somewhat difficult to quantify and is constantly changing as computers continue to advance and become more powerful.

In contrast an algorithm is considered to be unconditionally secure (also called information theoretically secure) if the cipher cannot be broken regardless of how much

computational power an adversary may possess, and independent of other scientific advances. No new developments in mathematics or computers will ever break a cipher if it is unconditionally secure. The one-time pad, as discussed previously, is unconditionally secure when implemented properly[2].

DES is a symmetric cryptosystem in the form of a block cipher. In a block cipher the plaintext is broken up into fixed length segments that are each encrypted separately resulting in a block of ciphertext for every block of plaintext. Many iterations of substitutions and permutations are used ultimately resulting in blocks of ciphertext in which every bit is dependent upon each bit of the plaintext and each bit of the key.

In its original form DES uses a block length of 64 bits and a key of 56 bits. By today's standards DES is no longer considered to be secure. Attacks can be successfully performed against it in less than 24 hours [9]. Triple DES (3DES) is a more secure form of DES, involving three rounds of DES with two keys resulting in an effective key that is twice as long. This adds more security but is slower to implement.

Although 3DES is often still used today, DES was officially superseded by AES in 2002 [10]. AES uses a block size of 128 bits with a possible key length of up to 256 bits. Today AES is widely used and is even integrated into Intel and AMD chips [11].

The other type of cryptography in wide use today, public key cryptography, relies on the use of one-way functions. A one-way function is a mathematical construct that is easy to compute in one direction, but the reverse computation is significantly more difficult. An example is factoring the product of two large prime numbers. It is easy to compute the product $n = pq$ of two prime numbers p and q, however, given only n, it is significantly more difficult to recover p and q. A trapdoor one-way function is a one way function with the added feature that reversing the calculation becomes easy given

[2]Unconditional security refers to the protocol only. Any unconditionally secure protocol will not be secure if implemented poorly.

an additional piece of information.

In a public key cryptosystem Bob has two keys: a private one, known only by him, and a public one that he publishes so that anyone can use it to encrypt a message to send to him. The message is encrypted using the public key via a one way function. The private key acts as a trapdoor allowing only Bob to easily reverse the encryption and recover the message. It is also difficult to figure out the private key from the public key. One problem with public-key encryption is that there is generally no proof that an efficient algorithm to reverse the one-way function does not exist. For example, RSA relies on factorization of large integers and although no efficient classical algorithm is known for this, a quantum computer using Shor's algorithm [12] would be able to factor in polynomial time and thus break RSA. Public-key cryptosystems are not only vulnerable to advances in computer science but also to possible new developments in mathematics and physics.

Public key cryptography is computationally intensive making it very slow to implement. As a result it is normally only used to encrypt very short messages. Often it is used as a means of secure exchange of a key for symmetric key cryptosystems like 3DES or AES. This alleviates the problem in a symmetric key cryptosystem of having to securely exchange and store keys before they are required.

Classical information, which is information that is encoded as bits of 0 or 1 as opposed to quantum information that is encoded in qubits (see section 1.2.1), can be easily intercepted and copied without detection. As a result the eavesdropper can monitor all communication that takes place while remaining undetected. If a key is distributed using a classical information based protocol, an eavesdropper can save the information that she obtains during the distribution for analysis at some later point in time. At this later time, new developments in computers or mathematics may allow her to easily break the encryption and discover the key. She is then able to easily decipher any messages, that she has copied and saved and that were encrypted with that key. One of the only

ways to guarantee the secure exchange of a key is by exchanging it in person before it is required to be used. A more functional means of distributing a truly secure key would improve upon modern day cryptosystems.

1.2 Quantum Security

As the age of modern cryptography reached maturity and began to flourish, the emergence of a promising new generation in cryptography had already begun. Advances in the field of Quantum Mechanics gave rise to new possibilities in information processing, communication technology and security, which are not possible using only classical means. One notable development is that of Quantum Key Distribution (QKD), which is able to provide, for the first time, an information-theoretical secure means of establishing a secret key between two separated parties over an untrusted, but authenticated channel.

1.2.1 Qubits and Entanglement

Classical information is encoded in the form of bits, each representing a value of 0 or 1. The quantum information equivalent is the qubit. A qubit, like a classical bit, is able to take on a value of 0 or 1, however, unlike a classical bit, it is also able to exist in a quantum superposition of 0 and 1. It is this unique property of a qubit that sets quantum information apart from classical information and allows for improvements over a number of the best possible classical protocols including those used for key distribution.

Any two-level quantum system can be used to encode qubits. The values 0 and 1 are encoded in two orthogonal states of the system. One example of a two level system that can be used for qubits is electron spin states. In this case, we can define 0 as being encoded into spin up state prepared along the z-axis of the electron (z-spin up) and 1 to be encoded into the spin down state prepared along the z-axis of the electron (z-spin down), where z-spin up and z-spin down are the eigenstates of the S_z operator with

eigenvalues $+\hbar/2$ and $-\hbar/2$, respectively.

$$|\uparrow\rangle = |0\rangle$$
$$|\downarrow\rangle = |1\rangle$$

A qubit encoded in this way can exist in any spin state of the electron, comprising every possible superposition of these basis states. The most general state of a qubit can be written as:

$$\begin{aligned}|\psi\rangle &= \cos(\theta/2)|\uparrow\rangle + e^{i\phi}\sin(\theta/2)|\downarrow\rangle \\ &= \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle\end{aligned}$$

Projecting this arbitrary state onto the S_z basis will result in an outcome of 0 with probability:

$$\begin{aligned}pr(0) &= |\langle 0|\psi\rangle|^2 \\ &= |\cos\theta\langle 0|0\rangle + e^{i\phi}\sin\theta\langle 0|1\rangle|^2 \\ &= \cos^2\theta\end{aligned}$$

and an outcome of 1 with probability:

$$\begin{aligned}pr(1) &= |\langle 1|\psi\rangle|^2 \\ &= |\cos\theta\langle 1|0\rangle + e^{i\phi}\sin\theta\langle 1|1\rangle|^2 \\ &= \sin^2\theta\end{aligned}$$

Unless the qubit has been prepared in an eigenstate of the measurement, in this case the computational basis $|0\rangle$ and $|1\rangle$, the measurement result will be probabilistic and the original state of the qubit will be changed by the measurement process. Quantum states, and therefore qubits, are impossible to be perfectly copied, as per the no cloning theorem [13].

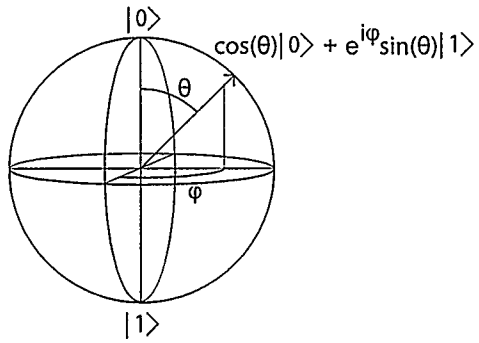

Figure 1.3: The Bloch Sphere: The Bloch Sphere is used as a means of visually representing a qubit. The upper pole of the Bloch Sphere corresponds to the qubit state $|0\rangle$, and the lower pole represents the qubit state $|1\rangle$. The angles θ and ϕ point to a position on the surface of the Bloch Sphere representing the qubit: $\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$. States lying on the equator of the Bloch Sphere are equal superpositions of $|0\rangle$ and $|1\rangle$.

Another way of representing quantum states is in the form of a density matrix. Any two-level quantum state can be represented as a 2 x 2 matrix of the form:

$$\rho = \frac{1}{2}(\mathbb{I} + \vec{m}\vec{\sigma}) = |\phi\rangle\langle\phi| \tag{1.1}$$

$\vec{m} = (m_1, m_2, m_3)$ is a normalized three component vector known as the Bloch vector and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ is a vector containing the three Pauli matrices. The components of the Bloch vector are given by:

$$\begin{aligned} m_1 &= \cos\phi \sin\theta \\ m_2 &= \sin\phi \sin\theta \\ m_3 &= \cos\theta \end{aligned} \tag{1.2}$$

from which it follows that $m_1^2 + m_2^2 + m_3^2 = 1$. As a result quantum states can be represented on the surface of a sphere, called the Bloch Sphere. The vector $\vec{m}$ points to a position on the Bloch sphere (figure 1.3) representing the qubit.

Another unique property that sets qubits apart from classical bits is the possibility to entangle them [14]. Entanglement is a property that can exist between two or more

quantum systems, in this case qubits, such that the complete state of all of the qubits cannot be represented as a product of the individual states of each of the qubits. Entanglement results in correlations in the detection statistics of the entangled qubits that are stronger than those predicted by any classical model [15]. Four entangled states, known as the Bell States, form an orthogonal set of basis states for any two qubit system, as sometimes used in QKD. The Bell states are:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

When selecting a two-level system as a physical medium for the qubits it is important to consider the requirements of the application and select a two-level system that is suited for the task. The ability to send qubits over long distances is essential for many communication applications, including key distribution. In this case photons provide a good solution as they can be easily transmitted. Much of the existing telecommunication industry is built around fibre optics, which is designed for the transmission of light. As a result, qubits in the form of photons can easily be integrated into existing infrastructure.

Photons have several degrees of freedom that can be used to encode qubits, including polarization and temporal or spatial modes. For example, 0 can be encoded as horizontal polarization and 1 can be encoded as vertical polarization. All other polarizations are a superposition of these two basis states. This is directly analogous to the previous example using electron spin states.

1.2.2 Quantum Cryptography

Most of the cryptosystems that are commonly used today, including 3DES, AES and all forms of public key cryptography are only computationally secure. The one-time pad is rarely used due to impracticalities associated with the secure exchange and storage of the large amounts of key material that the protocol requires.

Quantum Key Distribution, first proposed in 1984 by Charles Bennett and Gilles Brassard [16], offers a promising alternative solution to the problem of secure key exchange. The probabilistic nature of quantum mechanics allows two parties to exchange a key while detecting the presence of an eavesdropper. Alice and Bob are able to quantify and distill out any information an eavesdropper might have learned about the key during the exchange; if it turns out that the eavesdropper has learned too much for the security of the key to be assured, then Alice and Bob don't use that key. This results in a protocol offering unconditional security.

The short-term security of the key is assured because there is no way for the eavesdropper to gain information about the quantum states being exchanged without changing them. Long-term security of the key is assured because quantum information cannot be copied (no cloning) therefore there is no need to worry about future attacks once the key has been successfully exchanged.

In contrast, other commonly used key exchange protocols including public key cryptography are only computationally secure. In many cases, including RSA, although no good classical algorithms are currently known, there are quantum algorithms that could easily break the cryptography.

After a key has been exchanged via QKD it can be used in a number of ways. One option is to use it in conjunction with one-time pad encryption resulting in an information-theoretic secure cipher. Another option is to use the key with a symmetric cryptosystem such as AES. This ultimately only results in computational security that is limited to

the security of the symmetric cryptosystem being used. However QKD enables more frequent rekeying of the symmetric cryptosysem than may otherwise be possible.

In addition to QKD quantum cryptography also offers other improvements over currently used techniques in cryptography. This includes quantum algorithms for coin flipping [17], secret sharing [18], database queries [19] and digital signatures [20]. Although still in the developmental stages the field suggests many exciting advancements to the existing infrastructure of security today.

1.3 This Thesis

1.3.1 Motivation

Security of information is a topic of critical importance in society. Advances in various fields including mathematics, physics and computer science are continually having an effect on the ability to keep information secure. QKD is one of many developing technologies aimed at improving our ability to maintain and protect secret information during communication. As such investigations aimed at creating more robust and stable QKD systems are necessary.

Encoding qubits in temporal modes of photons has been implemented in QKD systems since as early as 1992 [21]. Systems in which the measurement is done through an active selection of the measurement basis have been widely implemented and studied [22], [23], [24], [25]. However, systems employing a passive selection of the measurement basis have, to the best of our knowledge, only been implemented with a couple of entanglement based QKD systems [26], [27], and never with faint pulses (pulses attenuated to the single photon level). This project aims to provide, for the first time, a side-by-side comparison of these two possibilities by implementing both with the same components and nearly identical experimental setup. This will provide us with a more complete comparison than

could be done by comparing the two systems on paper.

Another important issue for the advancement of QKD systems is long-term stability, which ideally should enable these systems to run continuously for several days, months, or even years at a time. Different means of achieving long term stabilization with time-bin qubits have been demonstrated [28], [29], [30]. Another goal of this project investigates a new technique for long-term stabilization using strong reference pulses in quantum frames[3].

The work done for this thesis involves the initial design and development of two time-bin encoding QKD systems and the design and development of an active stabilization system. One system employs active measurement basis selection and the second employs passive measurement basis selection. The two systems share a simillar design and use the same components allowing for a direct side-by-side comparison of the performance of the two systems.

1.3.2 Organization

The organization of this thesis is as follows: Chapter 1 covers some of the history of security from classical cryptography through to modern cryptography. Important cryptosystems are discussed including RSA, DES and AES. The ideas of computational security and unconditional security are introduced and the one-time pad is discussed. Next, the field of quantum information and its applications to security are discussed.

Chapter 2 provides an overview of the field of QKD. A few important protocols are introduced including BB84, which is the protocol used for the QKD system developed for this thesis. Techniques for post processing of the key are discussed in detail. Next, attacks on QKD are covered including various eavesdropping strategies and their relationship to security. Finally a selection of important side-channel attacks is discussed along with

[3]A related stabilization scheme is discussed in [28]

techniques for circumventing them.

In chapter 3 time-bin qubits are introduced along with a description of how they can be prepared and measured. Details about the design and construction of the interferometers that were used for the QKD systems developed for this work are presented.

Chapter 4 introduces the idea of quantum frames. An active stabilization system based on quantum frames that was developed is described including details about the design and operation of the system. Results from testing of the active stabilization system are presented.

The QKD systems developed for this work are described in chapter 5. Details of the experimental setup including optical and electronic components are covered. Experimental results from the operation of both systems are presented for comparison. An estimation of secret key-rates for both systems is presented. Finally an analysis of the overall performance of both systems based on the experimental results obtained is given.

Chapter 6 is a summery of the results from this thesis as well as some discussion of future directions for this project.

Chapter 2

Quantum Key Distribution

Quantum Key Distribution has been intensively studied since it was first proposed in 1984. During this time many improvements have been investigated, including new protocols, different methods of encoding the qubits, and more efficient post processing. The security has been rigorously assessed against both an Eavesdropper attacking the quantum states, and an Eavesdropper attempting to exploit side channels or possible imperfections in the implementation.

2.1 Quantum Key Distribution Protocols

Several different protocols for QKD have been developed. A selection of these representing slightly different principles are described in this section. This includes a simple prepare and measure protocol, a protocol based on the detection correlations from entanglement and a protocol that is not based on the use of qubits at all.

2.1.1 BB84 Protocol

Although it is the oldest known QKD protocol, the BB84 protocol [16] remains one of the most commonly used protocols in QKD systems today. Here is how the protocol works: Alice produces a sequence of qubits representing a random bit string of 0s and 1s. Each qubit is prepared in one of two bases selected at random: either the computational ($|0\rangle, |1\rangle$) basis or the primed ($|0'\rangle, |1'\rangle$) basis. For instance, the four possible states the

qubit can be prepared in are:

$$|0\rangle = |0\rangle$$
$$|1\rangle = |1\rangle$$
$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

where the states $|0\rangle$ and $|0'\rangle$ both correspond to a value of 0, and the states $|1\rangle$ and $|1'\rangle$ both correspond to a value of 1. Alice transmits her sequence of qubits to Bob over a quantum channel. He then measures each qubit in a randomly selected basis (computational or primed). Bob's measurement basis corresponds to Alice's preparation basis for only half of the qubits. In these cases, Bob's measurement yields the same bit that Alice encoded. When Bob selected a measurement basis different from the preparation basis Bob's measurement result will give a bit value of 0 or 1 with equal probability, therefore has no correlation with the value Alice encoded. After Bob has received and measured all the qubits, Alice and Bob compare preparation and measurement bases over a public channel and discard all qubits for which the preparation and measurement bases were incompatible. They also discard all instances in which Bob failed to receive a detection. This process is called sifting, and results in what is called the sifted key.

2.1.2 Entanglement Based Protocols

In 1991 Ekert proposed a QKD protocol using entanglement (see section 1.2.1) between qubits to generate a secure key between Alice and Bob [31]. In this protocol Alice and Bob each receive a sequence of qubits from a maximally entangled pair. Each of them projects their qubit onto one of three bases. For instance, Alice projects her qubit onto one of the following bases:

$$|A_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |A_1^{\perp}\rangle$$
$$|A_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle), |A_2^{\perp}\rangle$$
$$|A_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |A_3^{\perp}\rangle$$

where $|A_i^{\perp}\rangle$ is the state orthogonal to $|A_i\rangle$. Bob projects his qubit onto one of the bases:

$$|B_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{3i\pi/4}|1\rangle), |B_1^{\perp}\rangle$$
$$|B_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle), |B_2^{\perp}\rangle$$
$$|B_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |B_3^{\perp}\rangle$$

Afterwards, they reveal via a public channel which bases they projected each qubit onto. There are nine different possible combinations of bases onto which they could have projected.

In two of the cases they have both projected onto the same bases (i.e. they have both projected onto $(|A_2\rangle, |A_2^{\perp}\rangle) = (|B_2\rangle, |B_2^{\perp}\rangle)$ or they have both projected onto $(|A_3\rangle, |A_3^{\perp}\rangle) = (|B_3\rangle, |B_3^{\perp}\rangle)$), these results can be used to construct a key. Of the remaining cases, the results from four of them are disclosed and can be used in the calculation of a CHSH Bell's inequality [15]:

$$S = E(A_1, B_2) - E(A_1, B_1) + E(A_3, B_2) + E(A_3, B_1) \tag{2.1}$$

where E is the correlation coefficient. The three remaining cases are not used for anything and these results can be discarded.

The Bell parameter, S, can be used to detect the presence of an eavesdropper. The maximum value of S that could be obtained in a perfect system with no eavesdropper,

provided that Alice and Bob share maximally entangled states, is $S = 2\sqrt{2}$. Any value less than this, means that the states have been disturbed and points to the possible presence of an eavesdropper.

In 1992 Bennett, Brassard and Mermin deemed that Ekert's QKD protocol could be simplified to a protocol that is equivalent to BB84 [32], as measurement of the first qubit effectively results in a non-local state preparation of the second qubit.

2.1.3 Differential Phase Shift Protocol

The Differential Phase Shift protocol [33] for QKD is different from other protocols in that instead of being encoded in qubits the key information is encoded into the phase of consecutive pulses of weak coherent light. Alice uses an intensity modulator to carve out pulses of light with a separation on the order of nanoseconds. A laser with a long coherence time is used, so that the coherence of the laser will be spread out over several of these pulses. She modulates the phase of each pulse by 0 or π, and then she attenuates the pulses to the single photon level. This results in most of the pulses being in the vacuum state. The pulses are then sent to Bob through the quantum channel. When a photon is found, Bob is able to measure the phase difference between two consecutive pulses. He communicates to Alice the times when detections occured, so that she can compare against the phase of pulses sent at those times. For instance, pulses with a phase of 0 and π correspond to key values of 0 and 1 respectively.

2.2 Classical Post Processing, Authentication and Message Encryption

The protocol used for preparation and measurement of the qubits is only one step in the overall key distribution. Post processing is required in order to obtain a final key known only to Alice and Bob, called the secret key. An important parameter for a QKD system is the secret key rate, which is defined as the rate of secret key generation. The

post processing consists of two main steps, error correction and privacy amplification, discussed in detail in sections 2.2.2 and 2.2.3, respectively. Also, in order to incorporate QKD into a full cryptosystem, authentication and encryption method need to be taken into account.

2.2.1 Security Assessment

Once Alice and Bob have completed a preparation and measurement protocol and have obtained the sifted key, the next step is to determine whether a secure key can be produced. In order to do this they must estimate the Quantum Bit Error Rate (QBER). The QBER, e, is given by the ratio of the number of bits Bob has incorrect as compared to Alice, n_I, to the total number of bits, N_T.

$$e = \frac{n_I}{N_T} \tag{2.2}$$

One way to assess the QBER is for Alice and Bob to select a subset of the key and disclose it to each other for comparison. The QBER can also be estimated as part of the error-correction process, which is discussed in section 2.2.2.

Ideally, after sifting Alice and Bob each have a copy of an identical string of bits constituting the key. Yet, generally, these keys are not perfectly correlated, errors arise from a number of sources. Among contributors to the QBER are noise in the transmission channel, inherent noise of the detectors, non-ideal preparation of the states, non-ideal measurements, and, most importantly, a possible Eavesdropper. In order to ensure the security of the final key, the entire QBER is attributed to the eavesdropper, and is used to assess how much information an eavesdropper could have obtained about the key. When using one-way error correction (see section 2.2.2), it is possible to produce a secret key if the mutual information between Alice and Bob is greater than either the mutual information between Alice and Eve, or Bob and Eve.

The mutual information between Alice and Bob is given by:

$$I(A:B) = 1 - h_2(e) \tag{2.3}$$

where $h_2(e)$ is the Shannon entropy:

$$h_2(e) = -e\log_2(e) - (1-e)log_2(1-e) \tag{2.4}$$

The amount of mutual information that the eavesdropper is able to obtain is dependent upon the specific attack that has been implemented. To guarantee security we assume Eve's attack has given her the maximum possible information. Assuming $I(A:E) < I(B:E)$, such an attack, called a coherent attack, would result in a mutual information between Alice and Eve of:

$$I(A:E) = h_2(e) \tag{2.5}$$

To be able to produce a secret key we require:

$$I(A:B) > I(A:E) \tag{2.6}$$

$$1 - h_2(e) > h_2(e) \tag{2.7}$$

$$1 - 2h_2(e) > 0 \tag{2.8}$$

The result is that to be able to produce a secret key from the sifted key the QBER is bounded at a maximum of 11%. The next steps towards a secret key are error correction and privacy amplification.

2.2.2 Error Correction

The purpose of error correction is to remove discrepancies between Alice's and Bob's versions of the key, leaving them with identical bit strings. This process is done by means of classical communication.

2.2. CLASSICAL POST PROCESSING, AUTHENTICATION AND MESSAGE ENCRYPTION

Classical error correction protocols need to be adapted for QKD. Many early QKD systems made use of the cascade protocol [34]. However, it requires many rounds of communication and is computationally taxing. As a consequence the protocol is slow to implement, and results in low secret key rates. More recent QKD systems employ faster error correction protocols, enabling higher secret key rates.

Low Density Parity Check (LDPC) codes are an error correction protocol better suited for QKD [35]. In the QC2 lab LDPC codes have been successfully employed in classical post processing for a polarization based QKD system [36]. LDPC codes are a form of one-way error correction, which means that the classical information only needs to be sent from Alice to Bob (in the case of forward error correction) or from Bob to Alice (in the case of backwards error correction). The protocol requires Alice to send a collection of parity check bits to Bob, which he uses to find and correct the errors in his key.

Assuming forward error correction, Alice selects a LDPC matrix, $\hat{H}$, and calculates the parity check vector, $\vec{p}$, as:

$$\vec{p} = \hat{H}\vec{a} \tag{2.9}$$

where $\vec{a}$ is a vector containing the sifted key. For a key of length l, the number of parity check bits, j, required to correct the key can be calculated from the noisy coding theorem [5]:

$$\frac{(l-j)}{l} \geq I(A:B) = 1 - h_2(e) \tag{2.10}$$

Therefore:

$$j \geq l h_2(e) \tag{2.11}$$

The equality applies in the case of an optimal error correcting code. Generally, more

parity bits are required.

Alice sends the LDPC matrix, $\hat{H}$, and parity check vector, $\vec{p}$, to Bob, who then finds the error-corrected key, $\vec{b}_1$, using $\hat{H}$ and his sifted key vector $\vec{b}_0$. This is done through an iterative process that converges on the most probable vector $\vec{b}_1$. The QBER can be estimated from the number of mismatched bits between the vectors $\vec{b}_1$ and $\vec{b}_0$.

2.2.3 Privacy Amplification

Once error correction is completed, Alice and Bob are in possession of identical bit strings. Privacy amplification is the next step. It eliminates any information about the key that an eavesdropper might have learned, and results in a shorter key that is now known only to Alice and Bob. This is the secret key.

Privacy amplification is accomplished by selecting a two-universal hash function that compresses the error corrected key by mapping it to a shorter bit string. The hash function is designed such that Eve's probability to figure out the secret key given her information of the key after error correction is made arbitrarily low.

For an error corrected key of length l, the final secret key length, s, is given by:

$$s = l(1 - h_2(e) - I(A : E)) \tag{2.12}$$

The term $h_2(e)$ removes the information that Eve could have gained by listening to the parity information during the error correction process, and the term $I(A : E)$ removes the information that the Eavesdropper gained during the key distribution protocol. After privacy amplification the resulting secret key can be used to encrypt a secret message.

2.2.4 Authentication and Message Encryption

QKD is often promoted as providing unconditional security. However, the security of QKD does not in itself guarantee the security of the encrypted communication. In order

for the overall cryptosystem to achieve security other aspects of the cryptosystem must be considered.

The channel over which the key distribution takes place must be properly authenticated to avoid a man-in-the-middle attack. In such an attack an eavesdropper intercepts and imitates all quantum and classical communication taking place between Alice and Bob; she impersonates Alice when communicating with Bob and vice-versa. As a result she establishes two keys, one between herself and Alice and the other between herself and Bob. She can therefore intercept and gain access to any information Alice attempts to send to Bob and then reencypt and send it to Bob, so that Alice and Bob are unaware of her presence. If Alice and Bob share a secret bit string before attempting QKD, then authentication can be done with unconditional security. By doing this the part of the secret key is used up and needs to be replenished. If Alice and Bob don't already share a secret bit string, then authentication can be done with computational security through public key forms of authentication. Although this makes the overall cryptosystem less secure than it would be with unconditional secure authentication, this still has advantages over a system that does not employ QKD at all as discussed in section 1.2.2.

Furthermore, the cryptosystem will only be as secure as the final method of encryption. This means that if unconditional security is desired then the key must be used in a one-time pad encryption scheme. It is possible to use the key with another encryption algorithm such as AES, but the overall security is limited to the security of that algorithm. This also has advantages over a system not employing QKD discussed in section 1.2.2.

2.3 Attacking QKD Systems

Attacks on QKD systems have been intensively studied. In this section both attacks against the quantum states themselves, as well as side channel attacks will be discussed along with how security is affected and any relevant countermeasures.

In order to guarantee the security of QKD we assume that a potential eavesdropper has power limited only by the laws of physics. It is possible that she is in possession of advanced technology that far exceeds our own, and will use that technology to attack our system.

Eve is able to attack the system in a number of different ways. She can attack the qubits themselves as they are sent over the channel. Attacks of this kind fall into two categories: individual and coherent. Eve is also able to attack imperfections in the implementation of the QKD system, or conduct a side channel attacks. A selection of some of the most important attacks are discussed in this section.

2.3.1 Individual Attacks

An individual attack is when Eve attacks each of the qubits independently of the other qubits. This can be the result of Eve directly measuring the qubits themselves, or can involve interacting an auxiliary system with each qubit and then measuring the auxiliary system. The latter attack has the added advantage that it allows Eve to store the auxiliary systems in a quantum memory, and measure them after Alice has revealed the preparation bases. Eve can use this information to optimize the measurements she performs.

A simple example of an individual attack is called an intercept/resend attack. In this attack Eve intercepts each qubit as it is in transit between Alice and Bob. She measures it in a random basis from one of the basis being used in the protocol. After the

measurement she prepares a new qubit in the state she measured and sends it to Bob.

Eve's measurement basis will correspond to Alice's preparation basis for only half of the qubits. When Eve's measurement basis is the same as the preparation basis Eve will measure the state that Alice prepared, and therefore will know the bit value. She will send an identical qubit to Bob. However, in the cases where Eve's measurement basis does not correspond to the preparation basis Eve's result is not correlated with the qubit sent by Alice. If Bob then measures the qubit in the same basis Alice prepared it in, he will find the correct result only half of the time. As a result, the sifted key will have a 25% QBER.

The eavesdropper also has the option to attack only some of the qubits in this manner, allowing the others to continue to Bob undisturbed. This introduces less error to the key, proportional to the fraction of the qubits that she attacks. The eavesdropper will have obtained less information than she would have had she attacked all of the states. The mutual information between Alice and Eve that arises as a result of this specific attack is:

$$I(A:E) = 2e \tag{2.13}$$

Under such an attack a secure key can be obtained up to a QBER of 17%.

More powerful individual attacks are possible. Although quantum mechanics prohibits perfect cloning [13], it is possible to imperfectly clone (make non-exact copies) of the qubits. The goal of cloning is to produce two qubits, whose states are as close to the original qubit's state as possible. Fidelity is used as a measure of how close the two generated states match the original state. A fidelity of 1 means that the new states and the original state are identical. A universal cloner is a device that is able to clone any unknown quantum state equally well. The best universal cloner is able to attain a Fidelity of 5/6 [37]. An attack based on an optimal universal cloner would have a maxi-

mum QBER of 16.7% Eve also has the option to use a state dependent cloning technique resulting in some states being cloned better than others. A phase covariant cloner is able to clone all states lying in a chosen plane of the Bloch sphere (see section 1.2.1) equally well with a Fidelity of 0.854. In protocols such as BB84 where all of the states lie along one plane, this attack is better than a universal cloner. The phase covariant cloner is an example of an optimal individual attack, meaning that it maximizes the information about the key [38]. Under an optimal individual attack a secure key can be obtained up to a QBER of 14.6%.

2.3.2 Coherent Attacks

The most powerful form of attack that attacks the qubits directly is known as a coherent attack. To perform a coherent attack an eavesdropper interacts a probe system, consisting of a large number of qubits, with all the qubits Alice sends to Bob and then she stores her probe system in a quantum memory. This results in a large system of qubits in Eve's possession that is entangled with the qubits exchanged in the protocol. After error correction and privacy amplification Eve can optimize her measurements on the probe system to maximize her information about the key.

A special subset of coherent attacks are collective attacks. In a collective attack Eve interacts a different probe with each qubit and stores them in a quantum memory. The difference from a general coherent attack is that Eve has a distinct probe entangled with each qubit Alice sent instead of a larger probe system entangled with all qubits simultaneously. Like above, after classical information has been exchanged Eve can conduct optimized measurements on carefully chosen subsets of the probes to maximize her information about the key.

A coherent attack gives Eve the maximum possible information and leads to the 11% bound on the QBER as shown by Shor and Preskill [39].

2.3.3 PNS Attack and Decoy State Protocol

The security of many QKD protocols relies on Alice sending Bob single photons. In practice, true sources of single photons are not easily available, and as a result the protocols are often implemented using laser pulses attenuated such that the mean number of photons per pulse is less than one. The number of photons in pulses emitted from such a source follow a Poissonian distribution:

$$P_n = \frac{\mu^n e^{-\mu}}{n!} \tag{2.14}$$

P_n is the probability of a pulse containing n photons being emitted, given a mean number of photons per pulse of μ. All of the photons contained in a multi-photon pulse are prepared in an identical state. This opens up the possibility for an Eavesdropper to conduct a type of attack known as a photon number splitting (PNS) attack [40]. Keeping the mean number of photons per pulse low results in very few pulses containing two or more photons, however it is impossible to eliminate the multi-photon pulses altogether.

When conducting a PNS attack the Eavesdropper measures the number of photons in each pulse sent by Alice using a quantum non-demolition measurement. From every pulse containing more than one photon, Eve takes one photon and stores it in a quantum memory, allowing the rest to continue to Bob. She measures the state only after Alice has revealed the preparation bases. In this way she is able to gain perfect knowledge of the key from all multi-photon pulses without introducing any errors. She gains no knowledge from single photon pulses that reach Bob. However, she can block all of these pulses giving her complete knowledge of the key. The extra loss created in the channel might alert Alice and Bob that an attack is being conducted. However, as Eve's technology is unlimited, we must assume she is able to replace the lossy transmission channel and Bob's inefficient detectors with a perfect lossless channel and perfect detectors. After making

these modifications, Eve is able to conduct the PNS attack without being discovered through the increased channel loss, provided that the unmodified channel is lossy enough and the mean number of photons per pulse is high enough. The limiting case for which Eve is able to hide her attack in the channel loss is given by:

$$\mu \geq 2t \tag{2.15}$$

where t is the total transmittance of the channel, taking into account the efficiency of Bob's detectors. In the event that the channel is not lossy enough to permit Eve to block all the single photon pulses, she is still able to remain undetected if she sacrifices some knowledge of the key, by allowing a fraction of the single photon pulses to reach Bob, leaving the loss in the channel unchanged.

A secure key can still be distilled under these conditions as long as Alice and Bob keep the mean number of photons per pulse low enough [40]. All multi-photon contributions to the key have to be removed during privacy amplification. The secret key yield is defined as the fraction of secret key produced per faint pulse. Assuming optimal coherent eavesdropping, it is given by [41]:

$$s = q(Q_1 - Q_\mu h_2(e_\mu) - Q_1 h_2(e_1)) \tag{2.16}$$

q is a sifting factor, for the BB84 protocol $q = 0.5$. Q_1 and Q_μ are the single photon gain, and the multi-photon gain, respectively. The gain is defined as the number of detections per faint pulse emitted by Alice. As there is no phase reference, the output from Alice appears as her sending n photons with probability p_n (i.e. no photons with probability p_0, one photon with probability p_1 etc.) The single photon gain is the probability of a detection per single photon emission by Alice. The transmittance in optical fiber decreases exponentially with increased distance as: $t = e^{-\alpha l}$, where α is the attenuation coeffient ($\alpha = 0.2$ for SMF28) and l is the fiber length in kilometers. In order for Alice

and Bob to distill a secret key in the event of a PNS attack the optimal mean number of photons per pulse is equal to the channel transmittance: $u = t$. As the loss in fibre increases exponentially with increased distance the result is a secret key yeild that quickly drops off with increased distance ($s \propto t^2$).

Several methods of overcoming a PNS attack, while still maintaining high key rates, have been proposed and studied. One method is the decoy state protocol, which was first proposed by Hwang [42] and intensively studied by Wang [43] and Lo [44]. The decoy state protocol requires that for every pulse emitted from Alice's source she choose the mean photon number at random from a set of different mean photon numbers. Each mean photon number results in a different photon number distribution. The pulses generated from one of these distributions are called the signal states, with mean number of photons per pulse given by μ. The pulses generated from the rest of the distributions are called decoy states and each have a different mean number of photons per pulse ($\nu_0 to \nu_n$). It was shown by Lo that two decoy states with mean number of photons per pulse ν_0 and ν_1 are close to optimal for implementing the decoy state protocol [44]. The protocol is closest to optimal for $\nu_0 = 0$.

An eavesdropper is unable to tell which pulses are signal states and which are decoy states, and therefore has no choice but to attack every pulse in the same way. If she chooses to conduct a PNS attack, she will alter each photon number distribution in a different way, such that Bob's detection statistics will be incompatible with channel loss. After the protocol has been completed Alice reveals to Bob which of his detections correspond to signal states and which to decoy states. At this point Eve's attack has already been completed so she is unable to use this knowledge to adapt her eavesdropping strategy. By analyzing the photon number statistics of the signal and all decoy states independently, Alice and Bob are able to lower bound the single photon gain and upper bound the error rate on these pulses. Using the decoy state protocol, the optimal mean

number of photons per pulse for the signal states is $\mu = 0.5$. This is almost independent of the transmittance of the channel, as opposed to without using decoy states where μ must be adapted based on the transmittance. The decoy state protocol allows for an increased mean number of photons per pulse over what could be used without decoy states, enabling higher key rates, close to what one would expect from using a perfect single photon source.

2.3.4 Time-Shift Attack

Single photon detectors that are suitable for detection of photons at telecommunication wavelengths are often very noisy and, as a result, they are uaually gated such that they are only sensitive to an incoming photon for a few nanoseconds when the photon is expected to arrive. This is called the gate. The detection efficiency is not constant over the entire duration of the gate; it normally peaks somewhere near the center. The expected photon arrival time should correspond with the peak detector efficiency. No two detectors have identical detection efficiency at all points during a gate. This results in a detection efficiency mismatch between two detectors, and gives rise to the possibility for a time-shift attack [45].

An eavesdropper is able to exploit the detector efficiency mismatch between these detectors by shifting the arrival time of the photons, altering it such that it arrives at a time where a detection in one detector is more likely than a detection in the other detector. In the extreme case the eavesdropper is able to shift a photons arrival time such that Bob can only detect '0' or only detect '1'. As a result if Bob receives a detection Eve knows what bit-value that detection corresponds to and is thereby able to gain complete knowledge of the key.

Before time-shift attacks were well studied, QKD systems were generally designed such that detections in one detector always correspond to a bit value of '0' and detections in

another detector always correspond to a bit value of '1'. A simple countermeasure against this attack is for Bob to add a switch before the detectors so that he can randomly flip which detector detects which state. Bob knows which qubits he has redirected and therefore knows which detections correspond to '0' and which to '1'. Eve, on the other hand, doesn't know which bits were redirected and because values of '0' and '1' can now be detected in either detector, she is no longer able to gain knowledge of the key.

2.3.5 Faked States Attack

Another type of attack that exploits imperfections in the system is a faked states attack [46]. In this attack the eavesdropper intercepts and measures each qubit as she would if she were conducting an intercept/resend attack. Instead of trying to recreate the quantum states and send them to Bob, Eve creates faked states. The faked states are created in such a way that Bob is forced to detect them in the same basis as Eve conducted her measurement. If Bob's measurement basis happens to be different from Eve's he will not detect anything and this will be attributed to loss in the system. As Eve is able to replace Alice and Bob's channel no additional loss will be seen.

The result of such an attack is that whenever Eve measures in the incorrect basis Bob will not receive a detection unless he too measures in the incorrect basis. As a result these detections won't be included in the final key, and the QBER will not increase. In the cases where Eve measures in the correct basis she has full knowledge of the state and prepares a faked state such that if Bob measures in the correct basis he will measure the same state as her. It is therefore possible for Eve to have full knowledge of the final key without introducing any errors into the system.

There are many different ways of implementing a faked states attack. Each one is dependent on the specific details of the system that is being attacked. As a result countermeasures have to be specifically designed for the system being attacked. Some

examples are discussed in [47] and [48]. Generally, once Alice and Bob realize a faked states attack is possible against their system, it is not difficult for them to design a countermeasure against it.

2.3.6 Trojan Horse Attack

Every optical element reflects some of the light incident upon it. Eve can exploit this to conduct a type of side-channel attack that is known as a Trojan horse attack [49].

In this attack Eve inputs strong pulses of light into Alice's system and analyzes the light that is reflected back. By doing this she is able to gain information about the states Alice is preparing. For example the optical components Alice uses to create different states may have distinctive back reflection signatures for different settings (i.e. for every different qubit state that Alice prepares a unique reflection signature is seen). If Eve can figure out Alice's preparation settings she is able to gain knowledge about the key.

In principle Eve could also conduct a Trojan horse attack by inputting strong pulses of light into Bob's system to gain information about his measurement settings. However, this is more difficult since Bob's apparatus is more sensitive to strong pulses of light because it contains single photon detectors. Therefore Bob would more easily notice that such an attack was being conducted.

A countermeasure for this type of attack is for Alice and Bob to monitor for incoming strong pulses of light. This can be done at Alice's end by adding a circulator at the output of her apparatus such that any light entering the system is directed to a classical detector that will alert Alice if an attack is being conducted.

2.3.7 Device-Independent QKD

An alternative to protecting a QKD system against every conceivable side-channel attack would be to find a way to ensure the security of the system even in the face of an imperfect implementation. This is the idea behind the device independent scenario [50]. Device independent QKD relies on the use of an entanglement based QKD protocol, as a violation of a Bell inequality must be demonstrated for security. Consequently many commonly used protocols such as BB84 are not secure in the device independent scenario. Furthermore, to ensure the security of device-independent QKD the detection loophole must be closed, this is challenging given current technology.

In device-independent QKD neither the source, nor the measurement devices need to be trusted, and all may have been built by and designed by an eavesdropper. The measurement apparatus are thought of as black boxes that take classical inputs (measurement settings) and give back classical outputs (measurement results). No assumptions are made about what processes take place inside of the boxes including whether those processes are actually quantum mechanical, or what the dimensionality of the Hilbert space involved is, or what projection measurements correspond to each measurement setting.

If Alice and Bob are able to violate a Bell inequality, then they know that they share some degree of entanglement, which allows them to distill some secret key.

Chapter 3

Creating and Measuring Time-Bin Qubits

The QKD system discussed in this work is based on time-bin qubit encoding. Time-bin qubits are created by generating a photon in a superposition of two distinct temporal modes, denoted as $|t_0\rangle$ and $|t_1\rangle$. This chapter describes procedures that can be used for the creation and measurement of time-bin qubits. It also details the design and construction of the interferometers used for the preparation and measurement of time-bin qubits in the QKD systems that were developed for this work.

3.1 Time-Bin Qubits

Creation of time-bin qubits requires a method of creating a coherent superposition of two temporal modes. One common method of doing this is to use widely unbalanced interferometers. Measurements can be conducted by interfering the two temporal modes with each other.

3.1.1 Time-Bin Qubits vs. Polarization Qubits

Qubits are often encoded into the polarization states of light, which is advantageous as polarization states are generally easy to create and manipulate. Creation is easy because polarization of light is a naturally occurring two level system. Manipulation of the states and projection measurements require only waveplates and polarizing beamsplitters. However, a drawback to polarization qubits is that they are not optimal for transmission through fiber optic channels. The birefringence of optical fiber causes the polarization qubits to undergo transformations as they travel through the fibre. This transformation is dependent on temperature and mechanical stress and therefore is continually changing

with time. These transformations must be compensated before any measurements can be conducted on the qubits [51].

Time-bin qubits, on the other hand, are well suited to fibre optic communication. The phase, ϕ, between the temporal modes (see section 1.2.1) remains stable during transmission through optical fibre, provided that the separation between the temporal modes is small. However, from a technical standpoint, time-bin qubits are more difficult to generate and measure than polarization qubits are. The two-level system must be created by passing each photon through an unbalanced interferometer, giving rise to two distinct temporal modes. A second interferometer is required to measure the qubits, and the two interferometers must be kept phase stabilized with respect to each other. This creates a stabilization problem that may appear similar to stabilizing the polarization of quibts over the link. However, in this case the effect is isolated to changes within the interferometers, and not dependent on anything happening in the external environment. As well, the problem of stabilizing time-bin qubits only requires manipulating one parameter, whereas the problem of compensating the polarization requires manipulation of two parameters. Fibre optics allow for easy transmission of light over great distances, and are already used for many communication applications, as a result time-bin qubits are a particularly good choice for QKD applications.

3.1.2 Creating Time-Bin Qubits

Preparation of time-bin qubits requires an interferometer with two arms of unequal length. The path-length difference must be larger than the coherence time of the photons in order to prevent interference during preparation of the qubits. Light passing through the shorter arm of the interferometer corresponds to the temporal mode $|t_0\rangle$, and the long arm corresponds to the temporal mode $|t_1\rangle$.

Each photon that passes through the interferometer ends up in a superposition of

having traveled the long path and having traveled the short path. Assuming an equal probability to travel either path, this results in a state lying on the equator of the Bloch Sphere (see section 1.2.1):

$$\begin{aligned} |t_0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\phi_1}|t_1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_1}|1\rangle) \end{aligned} \tag{3.1}$$

Adding a phase modulator or a piezo (by wrapping the fiber around a circular piezo) in one arm of the interferometer enables the phase, ϕ_1, to be manipulated, which allows for the preparation of any state on the equator. Adding a variable beamsplitter to the interferometer, or an intensity modulator following the interferometer allows the amplitude of the temporal modes ($|t_0\rangle$, $|t_1\rangle$) to be manipulated, enabling the creation of any state on the Bloch sphere.

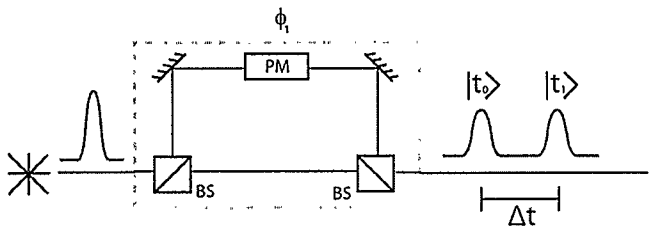

Figure 3.1: Preparation of Time-bin qubits: Preparation of time-bin qubit states lying on the equator of the Bloch sphere.

3.1.3 Measurement of Time-Bin Qubits

Measurement of time-bin qubits requires an interferometer with an identical path-length difference to the one used for preparation. This allows the two temporal modes to interfere and enables projection onto equal superpositions of $|t_0\rangle$ and $|t_1\rangle$ to be performed.

Mathematically this can be seen as:

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|t_0\rangle_{t_0} + e^{i\phi_1}|t_1\rangle_{t_1}) \\ \rightarrow\ & \frac{1}{2}((|t_0\rangle_{t_0} + e^{i\phi_2}|t_1\rangle_{t_0}) + e^{i\phi_1}(|t_1\rangle_{t_1} + e^{i\phi_2}|t_2\rangle_{t_1})) \\ =\ & \frac{1}{2}(|t_0\rangle_{t_0} + (e^{i\phi_2}|t_1\rangle_{t_0} + e^{i\phi_1}|t_1\rangle_{t_1}) + e^{i(\phi_1+\phi_2)}|t_2\rangle_{t_1}) \\ =\ & \frac{1}{2}(|t_0\rangle_{t_0} + e^{i\phi_2}(|t_1\rangle_{t_0} + e^{i(\phi_1-\phi_2)}|t_1\rangle_{t_1}) + e^{i(\phi_1+\phi_2)}|t_2\rangle_{t_1}) \end{aligned} \tag{3.2}$$

Passing through the measurement interferometer, each of the modes ($|t_0\rangle$, $|t_1\rangle$) undergoes the transformation given in equation 3.1. This gives rise to a third temporal mode, $|t_2\rangle$. The state after this transformation is seen in the second line of equation 3.2. The subscripts denote the temporal modes in which that component of the state exited the preparation interferometer, and it is onto these temporal modes that projections are made. After passing through the measurement interferometer a qubit can be detected in one of three temporal modes ($|t_0\rangle$, $|t_1\rangle$, $|t_2\rangle$). A detection in the first temporal mode, $|t_0\rangle$ corresponds to a photon having passed through the short arm of the preparation interferometer and the short arm of the measurement interferometer, this is the short-short path and corresponds to a projection onto the state $|t_0\rangle$ (as indicated by the subscript in equation 3.2). The last temporal mode, $|t_2\rangle$ corresponds to the long-long path, and thus a projection onto the state $|t_1\rangle$ (as indicated by the subscript in equation 3.2). A detection in the central temporal mode, $|t_1\rangle$ corresponds to projections onto equal superpositions of $|t_0\rangle$ and $|t_1\rangle$, lying on the equator of the Bloch sphere. In order to enable the selection of specific projections on the equator, the measurement interferometer must also contain a phase modulator to control the phase, ϕ_2.

3.2 The Interferometers

Two fibre optic interferometers were constructed for this QKD system: a preparation interferometer to be used in Alice's setup and a measurement interferometer to be used

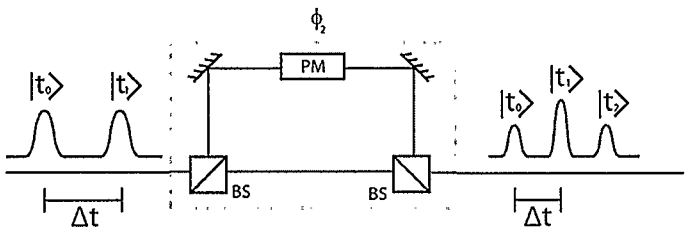

Figure 3.2: Measurement of Time-bin qubits: Detections in the mode $|t_0\rangle$ correspond to a projection onto the state $|t_0\rangle$. Detections in the mode $|t_2\rangle$ correspond to a projection onto the state $|t_1\rangle$. Detections in the mode $|t_1\rangle$ correspond to projections onto an equal superposition of $|t_0\rangle$ and $|t_1\rangle$ $(\frac{1}{\sqrt{2}}(|t_0\rangle + e^{i(\phi_1-\phi_2)}|t_1\rangle))$.

in Bob's setup.

3.2.1 Design

The interferometers are unbalanced Michelson interferometers, with a path-length difference of 1.44 ns, chosen to ensure compatibility with other experiments in our lab using time-bin qubits. The index of refraction of standard SMF28 optical fibre is 1.4682 [52], and therefore a 1.44 ns difference in travel time corresponds to a path-length distance of 29.4 cm through optical fibre. Given the Michelson design of the interferometers this becomes a difference of 14.7 cm in fibre length, since the light passes through each arm twice.

The preparation interferometer was required to output the same polarization of light as was input to it, due to polarization sensitive optics contained in the preparation set up for the QKD system, as discussed further in chapter 5. It contains a 2x2 (two input ports, two output ports) 50/50 polarization maintaining fibre optic beamsplitter (from Oz Optics). Each arm of the interferometer is terminated with a fibre optic Faraday mirror, which compensates for any polarization transformation that occurs in the arms of the interferometer, and results in the light exiting the arms of the interferometer being orthogonally polarized to the light entering the arms. The long arm is wrapped around

a piezoelectric tube actuator (from Physik Instrumente (PI)). This allows slow adjustments of the interferometer phase by applying a voltage to the piezo, which stretches the fibre and increases the path length difference of the interferometer by a fraction of a wavelength. This allows for adjustments to the phase of up to 10π at a resolution of 0.007π. Upon exiting the interferometer the polarization of the light is orthogonal to the polarization of the light at input, it is then rotated such that is the same as it was upon input.

The measurement interferometer was not required to output the same polarization as was input into it. It was built using a standard SMF28 50/50 beamsplitter from Oz Optics. The measurement interferometer is otherwise identical in design to the preparation interferometer.

Each interferometer is housed in a thermally insulated PVC box. The boxes contain a temperature stabilization system consisting of a heated metal plate with a temperature sensor (Thorlabs AD590) connected to an external PID temperature controller (Thorlabs TED200C), able to stabilize the temperature of the interferometer to 0.01° accuracy. This allows for passive stabilization of the interferometers, providing several minutes of phase stability. In order to enable long term phase stability, an active stabilization system is required. This is discussed in detail in Chapter 4.

3.2.2 Construction

The path-length difference of both QKD interferometers were matched to the path-length difference of another 1550 nm reference interferometer. The reference interferometer has the same path length difference as the majority of interferometers used in our lab.

The visibility, V, can be used to assess how well the path-lengths are matched.

$$V = \frac{P_{max} - P_{min}}{P_{max} + P_{min}} \tag{3.3}$$

P_{max} and P_{min} denote the maximum and minimum power of the observed interference fringes.

The QKD interferometers were initially built with a path-length difference of approximately 15.7 cm, 1 cm larger than desired. The difference in path-length difference between the reference interferometer and the QKD interferometers was precisely measured, as outlined below, and the excess fibre was removed from the QKD interferometer using a cleaver mounted on a translation stage, which has μm resolution.

To measure the difference in path-length difference between the reference interferometer and each of the QKD interferometers an unbalanced free-space Michelson interferometer was constructed out of bulk optics. The free-space interferometer was built with a translation stage in each arm such that it had an adjustable path-length difference of 1.4 cm. Light from a 1550 nm broadband Amplified Spontaneous Emission (ASE) source was sent through the reference interferometer and then through the free-space interferometer (connected in series), and detected at the output of the free space interferometer. The translation stages in the arms of the free-space interferometer were adjusted until maximum visibility was observed at the output. The bandwidth of the ASE source was about 20 nm allowing for a resolution of 5 μm to be achieved. At this position, x_0, the path-length difference in the free-space interferometer is equal to that of the reference interferometer. The reference interferometer was then swapped for one of the QKD interferometers and the process was repeated such that the free-space interferometer was equal in path-length difference to the QKD interferometer, yielding position x_1. The amount of fibre required to be cut from the QKD interferometer to match the path-length difference to that of the reference interferometer was calculated as:

$$L = \frac{|x_0 - x_1|}{n} \tag{3.4}$$

n is the index of refraction for SMF28, and $x_0 - x_1$ is the free-space difference in path-

length difference between the QKD interferometer and the reference interferometer.

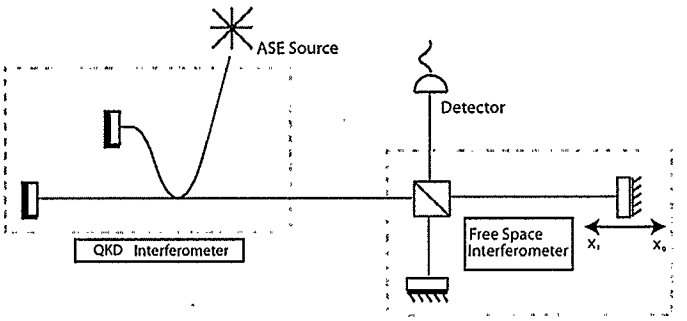

Figure 3.3: Measurement of Path Length: Setup for measuring the difference in path length difference.

Once both of the QKD interferometers were matched to the path-length difference of the reference interferometer, any slight discrepancies could be compensated by adjusting the temperatures of the QKD interferometers, allowing maximum visibility between the two interferometers to be achieved.

In order for QKD to be possible a visibility of at least 78% must be achieved between the states used. This corresponds to the 11% bound on the QBER for an optimal coherent attack. When sending classical light through the interferometers, the maximum visibility that can be observed is only 50% due to the non-interfering light contained with in the sidepeaks. As a result the 78% bound for QKD corresponds to a 39% bound, as observed with classical light.

Temperature tuning was able to achieve a maximum visibility of 48.5% by sending classical light through both interferometers. This was seen at a temperature of 30.08°C for the preparation interferometer and 38.08°C for the measurement interferometer. These were the final temperatures used in the experiments.

Chapter 4

Active Interferometer Stabilization with Quantum Frames

This chapter introduces the idea of Quantum Frames. An active stabilization system based on Quantum Frames was developed to stabilize phase drift between the preparation and measurement interferometers. The details of this system are covered in this chapter as well as results from testing of the system.

4.1 Quantum Frames

Quantum frames enable the transmission of classical data over a quantum channel used to transmit qubits [36]. Each quantum frame consists of a sequence of strong laser pulses, called the data header, followed by some quantum data, which is comprised of qubits used for a key distribution protocol. The strong pulses can be used as classical bits to encode digital information in the data header. Since it is sent over the quantum channel, the data header contains information about phase and polarization transformations during transmission through that channel that subsequent quantum data will be subjected to. This information can be used for stabilization tasks as discussed in detail in section 4.2. Another function of the data header is that it allows the qubits to be organized into subsets according to which frame number they are associated with, helping to facilitate time-tagging of the detection events.

There are several additional useful forms of digital information that can be encoded in the data header. One example is information about the sender and receiver, which allows qubit routing in network applications. It is also possible to include information about the encoding of the qubits (e.g. polarization or time-bin); this is useful in situations

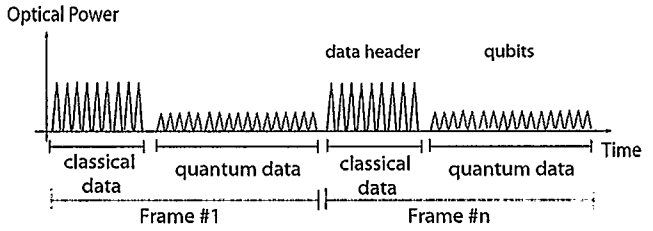

Figure 4.1: Quantum Frame

where the qubits are being received at a location that has the ability to measure multiple forms of encoding. Information about the key distribution protocol (e.g. BB84) or the specific bases being used with the protocol can also be included. Encoding this sort of information allows the classical data header to contain instructions for how to interpret the qubits contained within the frame.

Another requirement for a QKD system is keeping the system clocks in Alice's and Bob's devices synchronized. This is required so the detectors can be triggered at appropriate times and temporal modes, used with time-bin qubits, can be distinguished. Clock synchronization is also required to enable the association of detection events at Bob with their corresponding qubit emission from Alice. This clock synchronization is often done using a separate classical channel, but can instead be achieved with the data header.

Finally, the classical data header can contain information useful for stabilization tasks. As a result of traveling over the same channel as the qubits the data header experiences the same polarization and phase transformations. This information can be assessed using a classical detector and then used to compensate for the polarization transformations over a fibre optic link or to stabilize the phase between interferometers in a time-bin qubit system. Accomplishing these stabilization tasks is essential for the proper functioning and operation of a QKD system. The classical data header provides an nice solution to the problem by allowing the stabilization information to be sent over the quantum channel without requiring the actual qubits for the stabilization process.

4.2 Stabilization with Quantum Frames

The QKD system described in this work demonstrates the successful use of quantum frames to provide active stabilization of the phase between the preparation interferometer and the measurement interferometer. The two interferometers are required to be phase stabilized to each other because if the relative phase between the two interferometers drifts this changes the final state that is projected onto during the measurement.

4.2.1 Optical Setup

The optical setup for stabilization is shown in figure 4.2. The classical data header is produced by a 1550 nm pulsed laser diode (3S Photonics A1905LMI), with polarization maintaining output fibre. The laser diode is identical to the second laser diode used to produce the qubits (discussed further in chapter 5). The data header is sent once per second. It consists of a 100 μs burst of 500 ps wide pulses with a repetition rate of 100 MHz. For the remainder of the 1 s period the laser diode is turned off and it is during this time the quantum data is sent (see figure 4.3).

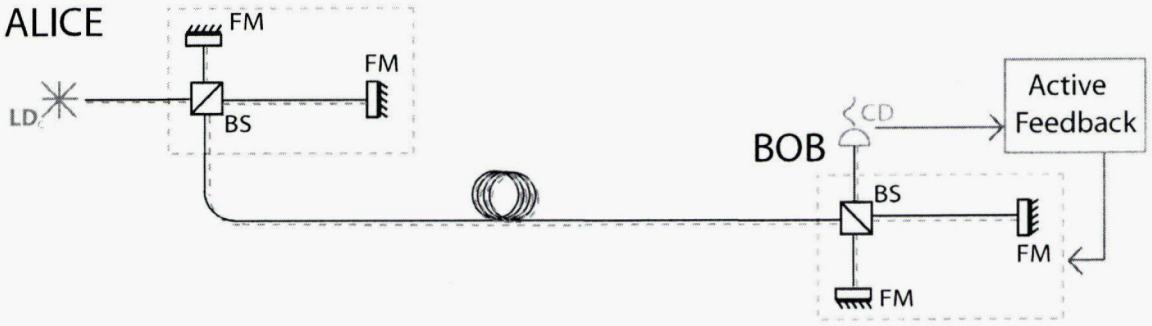

Figure 4.2: Optical Setup for Stabilization: LD_c is the laser diode used to produce the data header, and CD is a classical detector used for the detection of the data header.

The data header is sent through the preparation interferometer, across the link and finally through the measurement interferometer. It travels the same path as the qubits

and therefore picks up the same phase information. The interference observed at the output of the measurement interferometer is the same for classical pulses as it is for qubits, therefore classical pulses can be used to accurately assess the phase drift of the measurement interferometer with respect to the preparation interferometer. At the output of the measurement interferometer the optical pulses are detected by a low noise photoreceiver (New Focus 1811). The resultant electronic signal is fed into an active feedback system for processing.

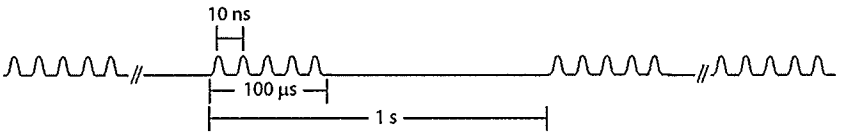

Figure 4.3: Data Header

4.2.2 Active Feedback System

Electronic processing generates an active feedback signal used to stabilize the phase between the interferometers. Details of the active feedback system are depicted in figure 4.4. The photo receiver used to detect the optical pulses has a maximum bandwidth of 125 MHz.

The amplitude of each electronic pulse contains phase information that is used for the active stabilization process. The amplitude of the electronic pulses varies between a maximum of 470 mV and a minimum of 330 mV, which corresponds to a π phase change between the interferometers.

Because the DAQ card only has a sampling rate of 1 MHz, in order to produce a signal that it can read, the signal output from the photo receiver is fed into a power detector (Mini-circuits ZX47-60S+). The power detector outputs a 100 μs long electrical pulse, with an amplitude proportional to that of the pulses from the data header. The signal is then read by a DAQ card (National Instruments NI USB-6361) for interfacing

with Labview software.

The Labview software processes the signal and then uses the DAQ card to drive a Piezo controller (Thor Labs MDT694A). Details of this software are discussed in section 4.2.3. The piezo controller outputs a voltage to the piezo contained within one arm of the measurement interferometer, which causes it to stretch or contract the fibre to compensate for phase drift in the system.

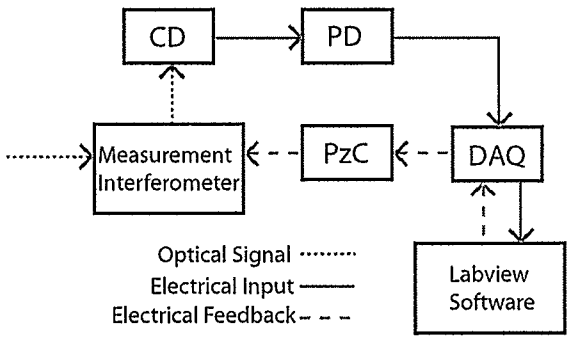

Figure 4.4: Active Feedback System: Schematic of the active feedback system. CD is the photo receiver, PD is the powerdetector, DAQ is the data acquisition card, and PzC is the piezo controller

4.2.3 Labview Software

The Labview software used for the stabilization makes use of a PID control feedback loop. The software was modified from software originally written by John Nguyen and later modified by Joshua A. Slater and Félix Bussières for use in other time-bin qubit experiments. Originally it was used to stabilize a free-space interferometer using a CW mode-locked laser. The laser was never turned off and the beam was sent through the interferometer with a beam path offset from that of qubits being sent through the same interferometer. The software constantly read the power off of a classical detector and used a PID controller to create a feedback signal to lock this power to a desired setting.

For this work, modifications to the software were required in order to enable the

software to compensate using the data header, consisting of a 100 μs burst of pulses instead of the constant CW signal. Some of the required modifications were integrated into the hardware by converting the 100 MHz data header pulses into a continuous 100 μs signal using the power detector. This was required to bring the signal within the frequency range of the DAQ card, which has a maximum sampling rate of 1 MHz. The DAQ card was triggered to begin measuring about 50 ms before the expected arrival time of the data header. The software ignores the first 10 μs of the data header as the data header pulses are irregular during this time and therefore contain no useful information. Over the next 70 μs the amplitude of the detected power was averaged. This averaged power is sent to the PID controller that creates a feedback signal used to drive the piezo controller.

4.3 Results

To test the stabilization, the relative phase drift between the interferometers was observed both with and without the active stabilization system on. The phase drift in the system was assessed by monitoring the change in detected power using Labview software. Figure 4.5a shows the natural phase drift in the system over the course of several hours with the active stabilization system turned off. Passive stabilization by means of temperature control was still maintained during this time. Figure 4.5b shows several hours with active stabilization turned on. To put this data into context a phase scan curve was produced by continually increasing the piezo voltage while monitoring the detected power from Labview. This curve is shown in Figure 4.6.

Statistical analysis of the data taken during the stabilization run was performed with Origin. This analysis reveals that the scatter of the points follows a Gaussian distribution centered at 0.9097 V with a standard deviation of 0.0018 V. From an analysis of the phase

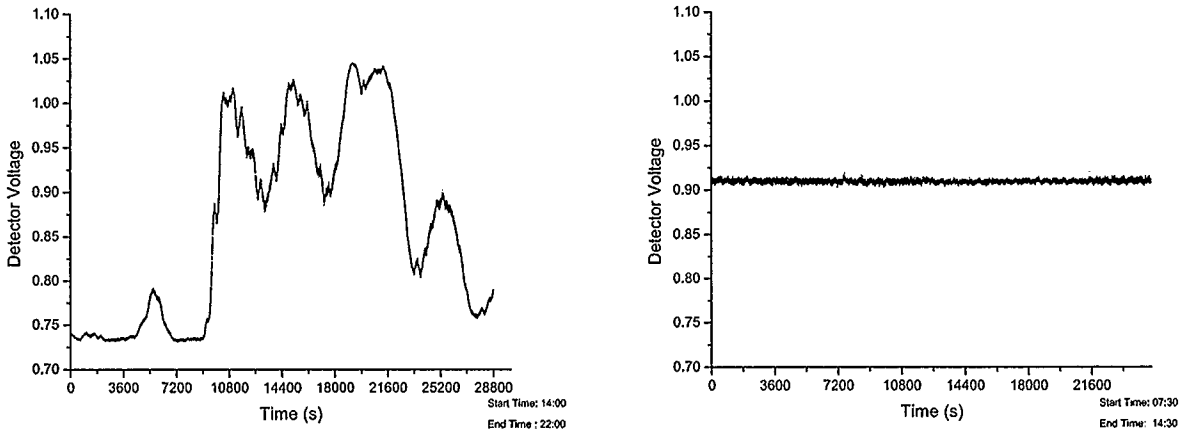

Figure 4.5: Stabilization Results: a)Drift in the system with the active stabilization turned off, collected over a period of 8 hours. b) Phase stabilization of the system over a period of 7 hours. The minimum and maximum voltages (corresponding to a π phase change between the interferometers) produced by the system as the phase changes are 0.75 V and 1.06 V respectively, as can be seen in the phase scan curve of figure 4.6. Both of the graphs displayed here are shown on the same scale.

scan curve a π voltage of 11.06 $\pm$ 0.34 V was found. Comparing the stabilization graph against the phase scan curve, the standard deviation in the stabilization data corresponds to an applied piezo voltage of 0.075 $\pm$ 0.014 V from the piezo controller. From this the phase drift is calculated as:

$$\phi = \frac{x\pi}{y} \tag{4.1}$$

where y is the π voltage and x is the applied voltage corresponding to the phase drift. From this, a phase drift of $(6.78 \pm 0.21)\pi$ x 10^{-4} is found, corresponding to the standard deviation in the stabilization curve. Hence, testing of the active stabilization system demonstrates successful phase stability over the course of several hours. The remaining phase drift in the system after stabilization only contributes a negligible increase to the QBER.

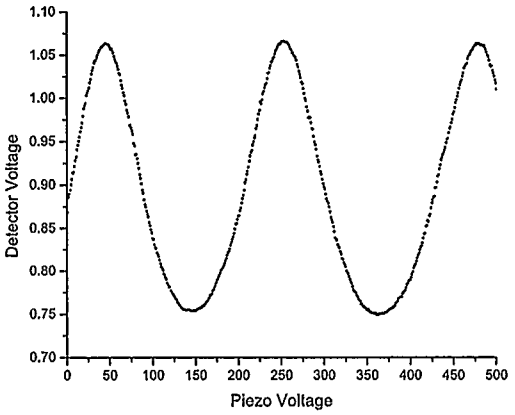

Figure 4.6: Phase Scan Curve: Continuous scanning of the piezo voltage to produce a phase scan. All conditions are the same as for the measurements done to produce figure 4.5, except that here the phase is continuously changed over a short amount of time by adjusting the piezo voltage.

The active stabilization system has been able to achieve up to 20 hours of phase stability, but periods of stability lasting around 8 hours are more common. The stability is lost when the piezo voltage required to correct the phase drift increases beyond the range of the piezo controller. However, stability is later recovered, generally after a couple of hours, once the system naturally drifts back into the range of the controller. It is possible to avoid these long periods of stability by modifying the software such that it could auto-reset itself and regain stability.

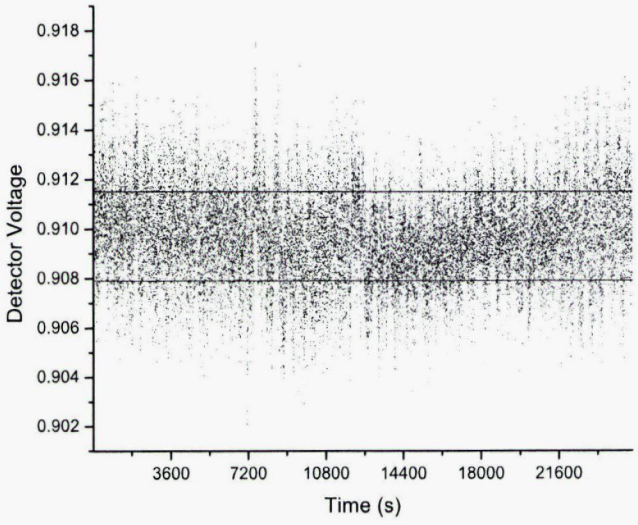

Figure 4.7: Scatter in Stabilization Data: The stabilization data zoomed in on the y-axis to show scatter. Horizontal lines show the standard deviation in the data.

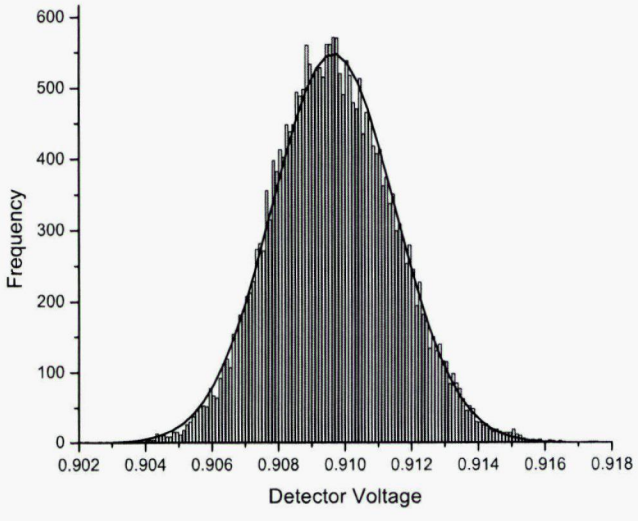

Figure 4.8: Gaussian Fit to Stabilization Data

Chapter 5

Experimental Quantum Key Distribution

The time-bin QKD systems developed for this work are described in detail in this chapter. Two different systems were developed, which are easily convertible to allow for a thorough comparison of the two. The first is called the active system, in which Bob must actively select a measurement basis for each incoming qubit. The second is called the passive system, in which measurement basis selection is done passively. Both systems (active and passive) use the same components and the same experimental setup, aside from minor changes required to switch between the two systems. This allows for a direct comparison between a time-bin QKD system based on active projection measurements and one based on passive projection measurements.

5.1 Experimental Setup

The experimental setup can be split into two main parts: optical and electronic.

5.1.1 Passive System - Optical Setup

In the passive system Alice prepares the four states:

$$\begin{aligned} |t_0\rangle &= |t_0\rangle \\ |t_1\rangle &= |t_1\rangle \\ |+\rangle &= \frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle) = \frac{1}{\sqrt{2}}(|t_0\rangle + e^0|t_1\rangle) \\ |-\rangle &= \frac{1}{\sqrt{2}}(|t_0\rangle - |t_1\rangle) = \frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\pi}|t_1\rangle) \end{aligned} \tag{5.1}$$

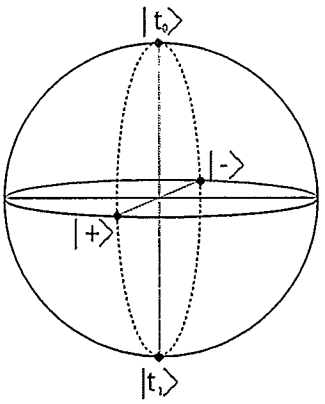

Figure 5.1: Passive System States on Bloch Sphere

These states are prepared using an intensity modulator and a phase modulator following the preparation interferometer. To prepare the states $|+\rangle$ and $|-\rangle$ the phase modulator is pulsed such that it acts on only one temporal mode. By doing this the relative phase between the two temporal modes is adjusted to select between the $|+\rangle$ and $|-\rangle$ states. To prepare the $|t_0\rangle$ and $|t_1\rangle$ states the intensity modulator is used. It is pulsed such that it maximally attenuates one of the two temporal modes (i.e. the one not corresponding to the state being prepared). Attenuating one of the two temporal modes effectively reduces the total energy of that qubit state by half (as half of the total energy is contained with in each temporal mode of the qubit). As a result, the mean number of photons for these states is attenuated by 3db. To keep the mean photon number constant across all four states, the intensity modulator is also used to attenuate the $|+\rangle$ and $|-\rangle$ states by 3 dB. In Bob's apparatus the measurement basis is passively determined by detecting the qubits at one of three possible arrival times, or time-bins (see section 3.1.3). A detection in the first or third arrival time projects the qubit state onto the $(|t_0\rangle, |t_1\rangle)$ basis, while a detection in the central arrival time projects the state onto the $(|+\rangle, |-\rangle)$ basis, with $|+\rangle$ or $|-\rangle$ determined by which detector the detection is received at.

The optical setup for the passive system is shown in figure 5.2. A 1550 nm pulsed

laser diode (3S Photonics A1905LMI) produces 500 ps wide pulses at a rate of 100 MHz. The pulses are sent through an optical attenuator (OzOptics RND-11-1550-8/125-P-40-3S3S-3-1-30-SP) for 50 dB attenuation. Ideally, the photons would then be sent through an intensity modulator to create the decoy states. However, as the decoy state protocol was not executed for this work, the intensity modulator was not included in the final experiments. The photons are then combined on a PBS with the data header, which is polarized orthogonally to the photons. The pulses are then sent through the preparation interferometer to generate the time-bin qubits. Following the preparation interferometer, the qubits pass through the intensity modulator (AVANEX IM10-P-13S-PP-FAFA-01) and the phase modulator (EOSpace PM-OKS-10-PFU-PFU-UL) used to create the desired quantum states. The qubits and data header are sent across the link to Bob. Upon entering Bob's system the pulses are sent through the measurement interferometer and detected at one of two InGaAs SPDs (IDQuantique id201). Immediately before the SPD the data header is split from the qubits at a PBS and sent to the active stabilization system.

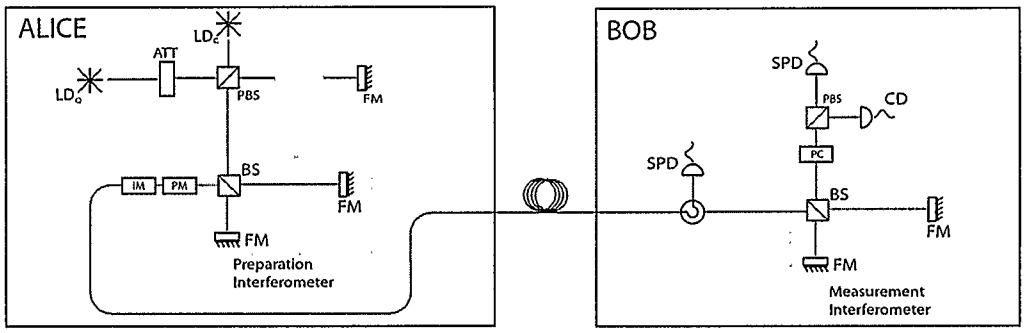

Figure 5.2: Experimental Setup - Passive System: LD_Q is the laser diode used for generation of the qubit states, LD_C is the laser diode used to generated the data header, CD is the classical detector used to detect the data header. Components shown here grayed out were not included in the final experiments.

5.1.2 Active System - Optical Setup

For the active system Alice prepares the states:

$$\begin{aligned}
|+\rangle &= \frac{1}{\sqrt{2}}(|t_0\rangle + |t_1\rangle) = \frac{1}{\sqrt{2}}(|t_0\rangle + e^0|t_1\rangle) \\
|-\rangle &= \frac{1}{\sqrt{2}}(|t_0\rangle - |t_1\rangle) = \frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\pi}|t_1\rangle) \\
|+i\rangle &= \frac{1}{\sqrt{2}}(|t_0\rangle + i|t_1\rangle) = \frac{1}{\sqrt{2}}(|t_0\rangle + e^{i\pi/2}|t_1\rangle) \\
|-i\rangle &= \frac{1}{\sqrt{2}}(|t_0\rangle - i|t_1\rangle) = \frac{1}{\sqrt{2}}(|t_0\rangle + e^{3i\pi/2}|t_1\rangle)
\end{aligned} \tag{5.2}$$

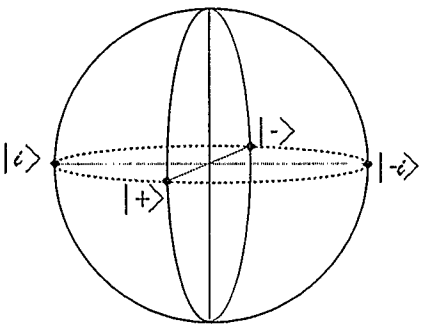

Figure 5.3: Active System States on Bloch Sphere

The states are prepared using a phase modulator. Again, it is pulsed to act on only one of the two temporal modes and different voltages must be applied to the phase modulator to create the different states. In Bob's system, before the qubits are detected, Bob actively selects the measurement basis using a phase modulator before the measurement interferometer. Pulsing the phase modulator such that it acts on only one of the two temporal modes allows him to select between the $(|+\rangle, |-\rangle)$ basis and the $(|+i\rangle, |-i\rangle)$ basis. Only detections within the central temporal window are considered and any detections in the first or third temporal window are discarded.

The optical setup for the active system is shown in figure 5.4. Except for a few small changes discussed below it is identical to the setup used for the passive system. A phase modulator (EOSpace PM-OKS-10-PFU-PFU-UL) is included in Bob's system directly before the measurement interferometer. As the phase modulator is a polarization dependent component, a polarization compensator is generally required before the phase modulator to compensate any polarization transformations that have occurred in the link. This was not included in the experiments preformed here as the link was polarization maintaining, but will be required for the system to be used over a real world link. Such polarization compensation over a real world link has been demonstrated in the polarization QKD system in the QC2 lab [36].

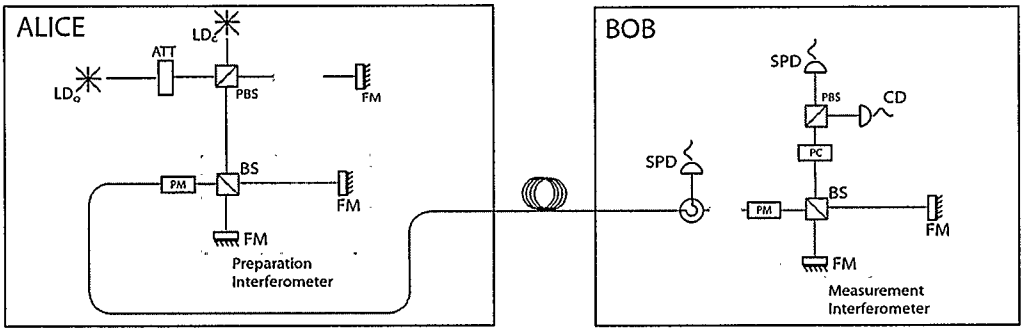

Figure 5.4: Experimental Setup - Active System: LD_Q is the laser diode used for generation of the qubit states, LD_C is the laser diode used to generated the data header, CD is the classical detector used to detect the data header. Components shown here grayed out were not included in the final experiments.

5.1.3 Electronics Setup

The electronic setup discussed here applies to both the passive and active systems. Five different signals are required to integrate the QKD system with the active stabilization system. These are depicted in figure 5.5. The digital signals to trigger the analog pulses required to generate the qubits and for the data header are provided by an arbitrary

function generator (Tektronix AFG 3252). The signal to create the qubits is an uninterrupted 100 MHz signal. The signal to create the data header is a burst signal, creating pulses at a rate of 100 MHz for 100 μs of every 1 s frame.

A second arbitrary function generator (Tektronix AFG 3012), synchronized to the first one, creates the signals to trigger the InGaAs SPDs. This signal has a repetition rate of 1 MHz and is sent for 999 500 μs out of every 1 s frame, leaving a 500 μs gap when the InGaAs detector is not triggered. This is required so that the InGaAs SPDs are not active during the arrival time of the data header to avoid flooding them with strong light pulses. There is a 200 μs window on either side of the data header. Furthermore, a disable signal is required to power down the classical laser diode during the time when the classical data header is not being produced. This suppresses the residual background light emitted from the diode. This disable signal is produced by a delay generator (Stanford DG 535) and it lasts for 999 700 μs out of every 1 s frame, leaving a window of 300 μs per frame during which the classical laser diode is powered.

The last required signal is a trigger for the stabilization software, which is produced by a second output of the delay generator. This signal is produced once per second and is timed to arrive at the DAQ card shortly before the arrival of the data header, triggering the software to begin reading the data header. Furthermore, a disable signal is required to power down the classical laser diode during the time when the classical data header is not being produced. This suppresses the residual background light emitted from the diode. This disable signal is produced by a delay generator (Stanford DG 535) and it lasts for 999 700 μs out of every 1 s frame, leaving a window of 300 μs per frame during which the classical laser diode is powered. The last required signal is a trigger for the stabilization software, which is produced by a second output of the delay generator. This signal is produced once per second and is timed to arrive at the DAQ card shortly before the arrival of the data header, triggering the software to begin reading the data header.

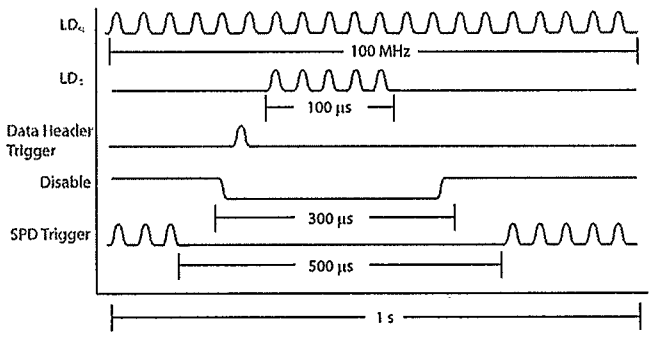

Figure 5.5: Experimental Setup Digital - Electronic Signals: Five signals used to integrate the QKD system with the active stabilization system.

The analog signals required for preparation and measurement of the qubits are generated using an arbitrary waveform generator (AWG) (Tektronix AWG 7102). The AWG has two independent output channels, each of which can operate at 10 Gs/s and generate output signals up to 1 V amplitude. Voltages exceeding 1 V are required, so amplifiers (AG-Berlin SHF 826H) are used for all signals coming from the AWG. A total of three amplifiers are used: one before Alice's intensity modulator, one before Alice's phase modulator, and one before Bob's phase modulator.

All signals in the system must be synchronized and so a third arbitrary waveform generator (Tektronix 3102) was used to produce dedicated timing signals to clock the entire system.

Detection and processing of the detection signal is done using two InGaAs SPDs and a Time-to-Digital-Converter (TDC). The InGaAs SPDs are gated at a frequency of 1 MHz with a gate width of 10 ns. There is a 10 μs dead time to avoid afterpulsing after any detection signal is received. The dark count probability is around 10^{-5} per gate and the detection efficiency is around 10%. The InGaAs SPDs output a signal upon each detection which is called the detection signal. They also output a signal every time the gate is activated which is called the gate-out signal. In order to distinguish between the three photon arrival times the detection signal is sent to a Time-Digital-Converter (TDC)

(ACAM ATMD-GPX). The TDC monitors nine channels (one start channel and eight stop channels) for electronic signals and it reports the time difference from the start pulse to each stop pulse with 80 ps resolution, sufficient to resolve the three arrival times that are each separated by 1.4 ns. This time difference is sent directly to a computer interfaced with the TDC for processing. The start signal for the TDC is produced by combining the two gate-out signals from the InGaAs SPDs on an AND gate. This produces a start signal only when both detectors have active gates and so detections that occur when either of the two detectors is in deadtime are not recorded. The detection times from the TDC are processed using C++ and Labview software originally developed for use in other experiments and modified for use with this QKD system.

5.1.4 Creation and Measurement of the Quantum States

While the system is running the relative phase between Alice's and Bob's interferometer is locked to a $\pi/2$ phase difference using the active stabilization system. Hence, at the locking point Alice is preparing the $|+i\rangle$ (ie $\phi = \pi/2$) state, and Bob is measuring in the $(|+\rangle, |-\rangle)$ basis.

To create the other states the phase modulator had to be calibrated to find three voltages corresponding to the phases 0, π, $3\pi/2$ (see equation 5.2), and the intensity modulator had to be calibrated to find two voltages corresponding to maximum attenuation and 3dB attenuation. Both were initially tested using strong pulses of light. Figure 5.6 displays the plots from this testing. Based on this data a voltage of 4.3 V on the phase modulator was estimated to correspond to a π phase shift. Further testing at the single photon level found a π voltage of 4.7 V. The voltages required to create the other states were estimated from the π voltage and tested with single photons. The final voltages used to create the states are summarized in table 5.1 and table 5.2.

Testing of the intensity modulator found a voltage of 4.6 V to correspond to maximum

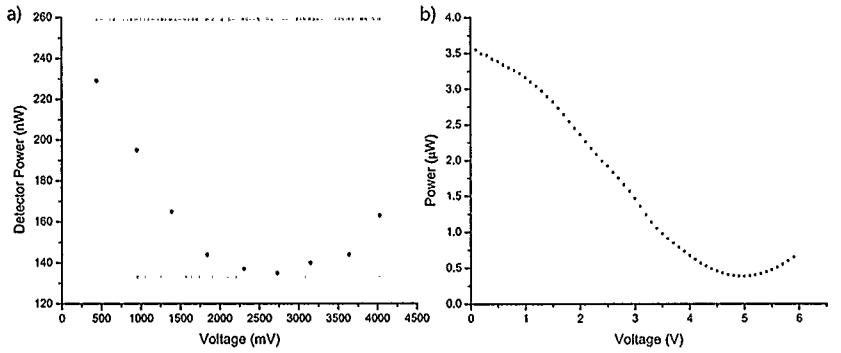

Figure 5.6: Testing of Phase and Intensity Modulators: a) Testing of the phase modulator was done by applying a series of increasing voltage pulses to the phase modulator and observing the output power, which produces an interference fringe. The horizontal lines represent the maximum and minimum expected powers. b) Testing of the intensity modulator was done by applying a series of increasing voltage pulses to the intensity modulator and observing the output power. Maximum power (about 3.5 μW) is at V = 0 and a minimum power, ideally 0 W, is found at V = 4.6 V.

attenuation, and 2.3 V to correspond to 3 dB. The voltages used to create the states are summarized in table 5.2.

Voltages required to be applied to the phase modulator for measurement of the states are summarized in table 5.3. These were found based on the voltages used to create the states.

Once all of the proper voltages required to create each of the states were found the next step was to find the precise timings in the system in order to ensure that all signals arrived exactly at the appropriate time. The arrival time of each signal was scanned over 10 ns at a resolution of 0.1 ns, to find the correct timings. The delay time of each of the signals are summarized in tables 5.1, 5.2 and 5.3.

Figure 5.7 shows a visual representation of how each of the states is created.

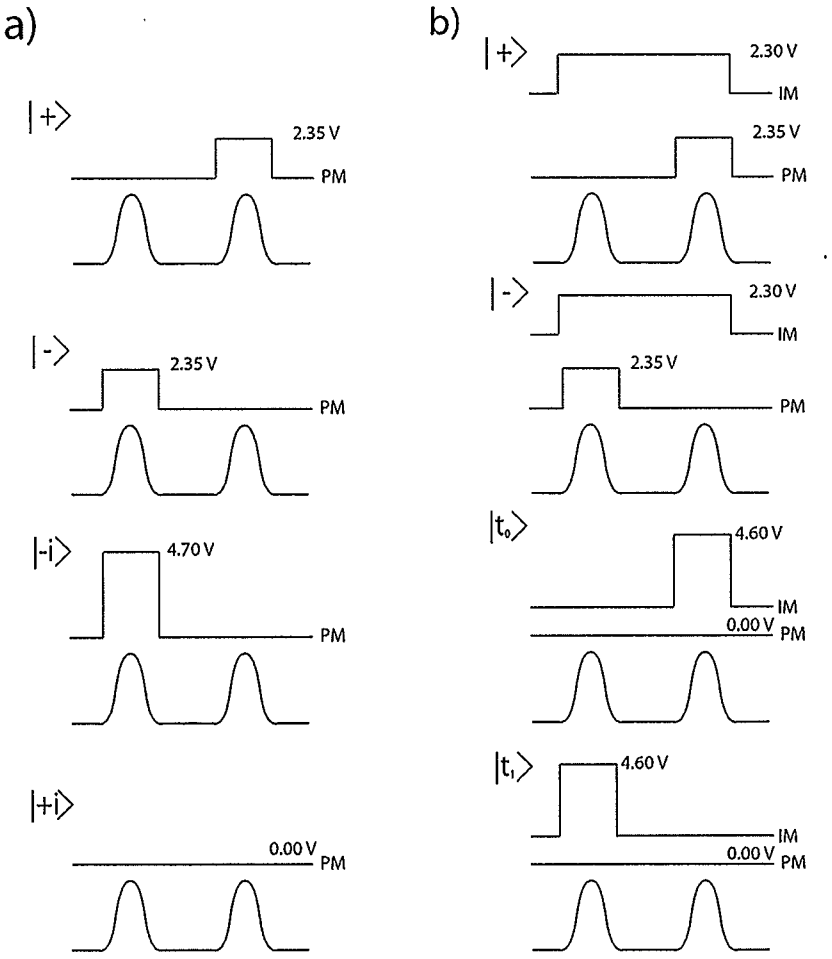

Figure 5.7: Creation of States: a) Visual representation of creation of states for the active system. b) Visual representation of creation of states for the passive system.

Table 5.1: Settings required to create the states for the Active System

	Phase modulator voltage	Temporal mode acted on
$\|+\rangle$	2.35 V	t_1
$\|-\rangle$	2.35 V	t_0
$\|+i\rangle$	0 V	-
$\|-i\rangle$	4.7 V	t_0

Table 5.2: Settings required to create the states for the Passive System

	Phase mod. voltage	Temporal mode acted on	Intensity mod. voltage	Temporal mode acted on
$\|+\rangle$	2.35 V	t_1	2.30 V	t_0, t_1
$\|-\rangle$	2.35 V	t_0	2.30 V	t_0, t_1
$\|t_0\rangle$	0 V	-	4.60 V	t_1
$\|t_1\rangle$	0 V	-	4.60 V	t_0

Table 5.3: Settings required for measurement basis selection

	Phase modulator voltage	Temporal mode acted on
$\|+\rangle, \|-\rangle$	0 V	-
$\|+i\rangle, \|-i\rangle$	2.35 V	t_1

5.2 Experimental Results

A proof-of-principle demonstration of each QKD system was conducted. Each version of the system was tested independently under the same conditions to provide a fair comparison. The mean photon number per qubit was kept at $\mu = 0.5$ for all of these experiments. This is the optimal signal state intensity for implementing the decoy state protocol [44]. The link between Alice and Bob consisted of 5 m of polarization maintaining fibre, which was approximated as having no transmission loss. This PM fibre was used for testing of the system; a real world link would not consist of PM fibre and would require compensation of the polarization over the link as has been demonstrated in [36]. Active stabilization of the QBER was also demonstrated. The results of the testing are summarized below.

5.2.1 Passive System

To test the passive system, first a sequence of qubits encoded with the $|+\rangle$ state was sent from Alice to Bob and the probability to project onto each state for a given basis was measured. This was repeated for each of the remaining states: $|-\rangle$, $|t_0\rangle$, and $|t_1\rangle$. These probabilities are summarized in table table 5.4. QBERs for each state based on this data are summarized in table 5.5. An overall sifted key rate of 13.4 kb/s was measured for the system.

Table 5.4: Passive System Results: For each state that Alice sends (rows), the probability (%) for Bob to detect each state (columns) is given.

	$\|+\rangle$	$\|-\rangle$	$\|t_0\rangle$	$\|t_1\rangle$
$\|+\rangle$	99.1 ± 0.033	0.9 ± 0.033	46.0 ± 0.018	53.4 ± 0.018
$\|-\rangle$	1.1 ± 0.035	98.9 ± 0.035	43.2 ± 0.017	56.8 ± 0.017
$\|t_0\rangle$	45.0 ± 0.014	55.0 ± 0.014	97.8 ± 0.029	2.2 ± 0.029
$\|t_1\rangle$	59.1 ± 0.006	40.9 ± 0.006	1.4 ± 0.008	98.6 ± 0.008

Table 5.5: Passive System QBERs

State	QBER (%)
$\|+\rangle$	0.9 ± 0.033
$\|-\rangle$	1.1 ± 0.035
$\|t_0\rangle$	2.2 ± 0.029
$\|t_1\rangle$	1.4 ± 0.008

5.2.2 Active System

The active system was tested in a similar manner to the passive system. First a sequence of qubits encoded with the $|+\rangle$ state was sent from Alice to Bob and Bob's measurement basis was set to the ($|+\rangle$, $|-\rangle$) basis. The probability to project onto each state was measured. The measurement was repeated for the ($|+i\rangle$, $|-i\rangle$) basis. This was repeated for each of the remaining states: $|-\rangle$, $|+i\rangle$, and $|-i\rangle$. These probabilities are summarized in table 5.6. QBERs for each of the states based on this data are summarized in table 5.7. An overall sifted key rate of 6.2 kb/s was measured for the system.

Table 5.6: Active System Results: For each state that Alice sends (rows), the probability (%) for Bob to detect each state (columns) is given.

	$\|+\rangle$	$\|-\rangle$	$\|+i\rangle$	$\|-i\rangle$
$\|+\rangle$	98.4 ± 0.035	1.6 ± 0.035	41.7 ± 0.034	58.3 ± 0.034
$\|-\rangle$	0.7 ± 0.040	99.3 ± 0.040	56.2 ± 0.039	43.8 ± 0.039
$\|+i\rangle$	50.0 ± 0.037	50.0 ± 0.037	98.7 ± 0.040	1.3 ± 0.040
$\|-i\rangle$	47.5 ± 0.037	52.4 ± 0.037	1.5 ± 0.038	98.5 ± 0.038

Table 5.7: Active System QBERs.

State	QBER (%)
$\|+\rangle$	1.6 ± 0.035
$\|-\rangle$	0.7 ± 0.040
$\|+i\rangle$	1.3 ± 0.040
$\|-i\rangle$	1.5 ± 0.038

5.2.3 Stability

To test the long term stability of the system (i.e. the ability to maintain a low QBER), the system was run for several hours with Alice sending the state $|+\rangle$, and Bob projecting onto the +/- basis. The QBER was calculated over this time using 5 minute intervals of

data. Figure 5.8 displays the results from this testing. Over a period of 5.8 hours the QBER was 1.15% with a standard deviation of 0.059%.

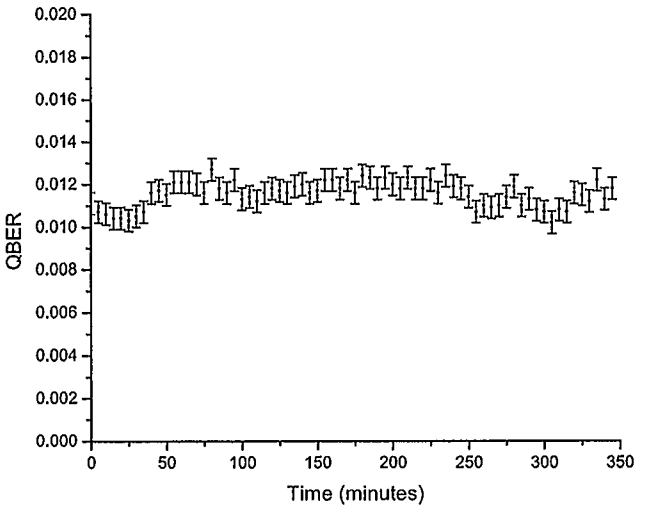

Figure 5.8: QBER Stability: Stability of the system over 5.8 hours.

As discussed in section 4.3 phase stability is periodically lost, this results in the system experiencing an increased QBER during these periods of lost stability and data collection would have to be stopped. However, some modifications to the software would enable the QKD system to run indefinitely even with these periods of lost stability. These modifications would require the stabilization software to alert the data collection software to stop collecting data when stability is lost, and later, when stability is regained, restart the data collection. Software allowing the stabilization system to auto-reset itself during this time would need to be added. With these modifications the QKD system could run continuously requiring only short pauses of the data collection during the reset time.

5.3 Estimation of Secret Key Rate

Using the decoy state method (see section 2.3.3), the secret key rate per faint pulse emitted, assuming no PNS attack, is given by:

$$s = \frac{1}{2}(Q_1 - Q_\mu f(e_\mu)h_2(e_\mu) - Q_1 h_2(e_1)) \tag{5.3}$$

Q_μ and e_μ are the signal state gain and error rate, as determined from experimental data. $f(e_\mu)$ is the error correction efficiency, assumed to be 1.22 [53]. Q_1 and e_1 are the single photon gain and error rate, which are bounded using the method and equations from [44]:

$$\begin{aligned} Q_1 &\geq \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \\ e_1 &\leq \frac{e_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1 \nu} \\ Y_1 &\geq \frac{\mu}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \end{aligned} \tag{5.4}$$

Y_0 is the experimenatlly measured backgroung count rate. Q_ν and e_ν are estimated for $\nu = 0.1$ using equations taken from [44]:

$$\begin{aligned} Q_\nu &= Y_0 + 1 - e^{-t\eta\nu} \\ e_\nu &= e_0 Y_0 + e_d(1 - e^{-t\eta\nu}) \end{aligned} \tag{5.5}$$

e_d is the temporal mode extinction ratio, t is the total loss over the link and in Bob's setup before the measurement, and η is the detector efficiancy.

Q_μ, e_μ, Q_ν, e_ν and Y_0 for both the active and passive systems are given in table 5.8. Based on this a secret key rate of 5471 kb/s is estimated for the passive system and 2545 kb/s is estimated for the active system.

Table 5.8: Decoy State Parameters

	Active	Passive
Q_μ	1.23×10^{-2}	2.67×10^{-2}
e_μ	1.26×10^{-2}	1.34×10^{-2}
Q_ν	2.48×10^{-3}	5.41×10^{-3}
e_ν	1.69×10^{-2}	1.48×10^{-2}
Y_0	2.0×10^{-5}	3.4×10^{-5}

5.4 Discussion

Using experimental data, there are three figures of merit that can be explored to compare the two modes of operation: QBER, sifted key rates and ease of implementation. The two systems exhibit similar QBERs, while the passive system sees higher key rates and enjoys greater simplicity of implementation. Overall the passive system seems to be a better option in most situations.

The QBERs between the two systems are very similar. The active system has a QBER of 1.26% averaged over the four states and the passive system has a QBER of 1.34% averaged over the four states. This difference is small and does not play a large role in overall secret key rates. The $|t_0\rangle$ state is seen to have a noticeably higher QBER than the other states in both the active and passive systems. This may be the result of non-uniform detection efficiency across the gate. Further evidence for this is that the $|t_0\rangle$ state has the lowest gain over all of the states, even though during testing of the states before measurement the $|t_0\rangle$ and $|t_1\rangle$ states were measured to have the same gain.

Key rates in the passive system are more than twice as high as those seen for the active system. A major factor is that in the passive system every detection is counted as a legitimate detection (although half of these will be detected in the wrong basis). In the active system half of the total detections, i.e. those contained within the first and third temporal window, are discarded outright. Another factor is that the passive system does

not require a phase modulator for measurement and thus less loss slightly improves key rates.

Finally, the passive system is easier to implement. First, the measurement apparatus is simpler. A phase modulator is not required for basis selection, which also eliminates the need to stabilize the polarization over the link, which would be required in any real world situation. Second, in the passive system all of the fast signals (those required for the creation of the states) are contained in one location and so synchronization of fast signals over a link would not be required.

Based on a theoretical calculation secret key rates in the passive system are seen to be slightly more than twice as high as those in the active system. This is the most important figure of merit in any QKD system, and backs up the superiority of the passive system over the active system.

In the active system any state on the equator of the Bloch sphere can be generated and measured, allowing for protocols that may require states in non-mutually orthogonal basis, for example coin flipping [17]. This is a major advantage of the active system as there is greater flexibility in the states that can be used. In the passive system only four states can be used and they must be in mutually unbiased basis.

Overall the passive system is better than the active system provided that the system is only going to be running the BB84 protocol or similar. This is based on projected higher secret key rates combined with greater ease of implementation. If flexibility of the possible states is required the active system is a better choice.

Chapter 6

Summary and Outlook

Quantum key distribution is capable of providing security beyond what any classical key disribution protocol is capable of. When used in conjunction with a one-time pad it can provide an unconditionally secure cryptosystem.

Investigations such as this one, which are aimed at learning more about different methods of implementation, are an essential part of improving the overall performance of QKD systems. With the exception of two entanglement-based QKD systems [26], [27], all other time-bin based QKD systems in use today are based on an active projection measurement system. This work demonstrates that a faint pulse system based on passive projection measurement could be capable of outperforming an analogous counterpart system based on active projection measurement and, furthermore, is potentially easier to implement.

Two time-bin encoding quantum key distribution systems based on the BB84 protocol were designed and constructed for this work: a passive measurement system and an active measurement system. This included building and characterizing two fiber-optic interferometers that were used for the preparation and measurement of the time-bin states.

Insulated boxes containing a heating system for passive stabilization were also designed to house the interferometers. An active stabilization system based on Quantum Frames was also designed and developed as part of this work. The system is used to stabilize the phase between the preparation and measurement interferometers. Several hours of phase and QBER stability were demonstrated. This is another step towards improved implementations as it allows for tight stability of the QBER to be maintained,

while only requiring hundreds of microseconds per second for the stabilization process.

The two systems use all of the same components and the same experimental setup aside for a few minor changes necessary to switch between them. Both systems were tested in a proof of principle demonstration that was conducted under the same conditions (i.e. identical link loss and mean number of photons per faint pulse). This allowed for a direct comparison and analysis of the two systems. The systems were compared based on QBER, key rates and ease of implementation. For the BB84 protocol, the passive system is able to outperform the active system due to its simpler implementation and key rates that are more than twice as high. However, any protocol requiring more than four states in two mutually unbiased bases would be required to use an active measurement system.

Improvements to the system would include replacing the measurement interferometer with a polarization maintaining interferometer, similar to the one used in preparation. The usefulness of a polarization maintaining interferometer for measurement only became apparent during the development of the active stabilization system when the decision was made to split the data header from the qubits using a PBS instead of a 90/10 beam splitter, as was originally intended. The PBS allowed for higher detected powers with the active stabilization system, which resulted in tighter stability. However, the addition of the PBS resulted in an additional polarization compensator to be required before the PBS, this would not be required if the measurement interferometer output the same polarization that was input to it.

Further testing of the system over a real world link, such as the one connecting the QC2 lab to our second lab at SAIT, should be conducted. This will require a means of active stabilization of the polarization over the link, which was not developed during this work, but exists in the QC2 lab polarization QKD system [36].

Further development is required to create a fully functional QKD system. This would require random state preparation and measurement, as well as incorporating a full post-

processing system consisting of error correction, privacy amplification and decoy state analysis, as well as proper authentication over the channel. Such a post processing system is already in place for the polarization based QKD system in our lab and could be easily adapted for this system. As well, the function generator that drives the phase and intensity modulators, to create and measure the states could be replaced by FPGAs and suitable drivers, which would result in a more integrated and less expensive system.

Currently, the detectors are the biggest bottle neck to higher key rates in this system. Alice prepares states at a rate of 100 MHz, but the current detectors can only be clocked at a maximum rate of 1 MHz and also experience a dead time of 10 μs between each detection resulting in a maximum possible key rate of 100 kHz. This means that faster detectors would greatly improve key rates. Faster detectors are already available, detection rates exceeding 100 MHz have been reported [54], [55], [56].

The system could also be incorporated into a QKD network with multiple senders and receivers of qubits. Quantum frames would need to be further developed for use in such a network for routing qubits between various senders and receivers. In addition, integrating this system with systems based on different encodings, such as the polarization based QKD system our lab has developed, in a network setting would also be possible.

Bibliography

[1] D. Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* Scribner, New York NY, (1996).

[2] Cornell Department of Mathematics. *http://www.math.cornell.edu/* **001** (2004).

[3] W.F. Friedman. *The index of coincidence and its applications in cryptology.* Department of Ciphers, Geneva, Illinois, USA: Riverbank Laboratories, (1922).

[4] B. Schneier. *Applied Cryptography - Second Edition.* John Wiley & Sons, New York NY, (1996).

[5] C.E. Shannon. *The Bell System Technical Journal* **27**, 379 (1948).

[6] National Institute for Standards and Technology. *Federal Information Processing Standards Publication* **46**, 1 (1977).

[7] W. Diffie, M.E. Hellmann. *IEEE Transactions on Information Theory* **6**, 664 (1976).

[8] R. Rivest, A. Shamir, L. Adleman. *Communications of the ACM* **21**, 120 (1978).

[9] Electronic Foundation. *Cracking DES - Secrets of Encryption Research, Wiretap Politics & Chip Design.* O'Reilly Media, Sebastopol, CA, (1998).

[10] National Institute for Standards and Technology. *Federal Information Processing Standards Publication* **197**, 1 (2001).

[11] S. Gueron. *Intel Advanced Encryption Standard (AES) Instructions Set.* Intel, Santa Clara, CA, (2010).

[12] P. W. Shor. *Proceedings of the 35^{th} Annual Symposium on Foundations of Computer Science* (1994).

[13] W. K. Wootters, W. H. Zurek. *Nature* **299**, 802 (1982).

[14] W. Tittel, G. Weihs. *Quantum Information and Computation* **1**, 3 (2001).

[15] J. F. Clauser, M. A. Horne, A. S. R. A. H. *Phys. Rev. Lett.* **23**, 880 (1969).

[16] C. H. Bennett, G. Brassard. *Proceedings of the IEEE International Conference on Çomputers, Systems and Signal Processing* , 175 (1984).

[17] G. Berlin, G. Brassard, F. Bussières, N. Godbout. *Phys. Rev. A* **80**, 062321 (2009).

[18] S. Schauer, M. Huber, B.C. Hiesmay. *Phys. Rev. A* **82**, 062311 (2010).

[19] M. Jakobi, C. Simon, N. Gisin, J.-D. Bancal, C. Branciard, N. Walenta, and H. Zbinden. *Phys. Rev. A* **83**, 022301 (2011).

[20] L. Yang, M. Liang, B. Li, L. Hu, D.-G. Feng. *arXiv:quant-ph/1012.5249* (2011).

[21] A.K. Ekert, J.G. Rarity, P.R. Tapster, G.M. Palma. *Phys. Rev. Lett.* **69**, 1293 (1992).

[22] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. *Appl. Phys. Lett.* **70**, 793 (1997).

[23] S. Fasel, N. Gisin,, G. Ribordy, and H. Zbinden. *Eur. Phys. J. D* **30**, 143 (2004).

[24] C. Gobby, Z.L. Yuan, and A.J. Shield. *Appl. Phys. Lett.* **84**, 3762 (2004).

[25] Z.L. Yuan, A.R. Dixon, J.F. Dynes, A.W. Sharpe, and A.J. Shields. *New Journal of Physics* **11**, 045019 (2009).

[26] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin . *Phys. Rev. Lett.* **84**, 4737 (2000).

[27] H. Takesue, K. Harada, K. Tamaki, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, S. Itabashi. *Optics Express* **18**, 16777 (2010).

[28] Z. Yuan, A. Shields. *Optics Express* **13**, 660 (2005).

[29] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, and A.J. Shields. *Appl. Phys. Lett.* **96**, 161102 (2010).

[30] F. Bussières, J.A. Slater, J. Jin, N. Godbout, W. Tittel. *Phys. Rev. A* **81**, 052106 (2010).

[31] A. K. Ekert. *Phys. Rev. Lett.* **67**, 661 (1991).

[32] C. H. Bennett, G. Brassard, N. D. Mermin. *Phys. Rev. Lett.* **68**, 557 (1992).

[33] K. Inoue, E. Waks, Y. Yamamoto. *Phys. Rev. A* **68**, 022317 (2003).

[34] C.H. Bennett, F. Bessette, G. Brassarad, L. Salvail and J. Simolin. *Journal of Cryptology* **5**, 3 (1992).

[35] Pearson, D. *Quantum Communication, Measurement and Computing. AIP Conference Proceedings* **734**, 299 (2004).

[36] I. Lucio Martinez, P. Chan, X. Mo, S. Hosier, W. Tittel. *New J. Phys.* **11**, 095001 (2009).

[37] D. Bruss, D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello1, and J.A. Smolin. *Phys. Rev. A* **57**, 2368 (1998).

[38] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A.Peres. *Phys. Rev. A* **56**, 1163 (1997).

[39] P. Shor, J. Preskill. *Phys. Rev. Lett.* **85**, 441 (2000).

[40] G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders. *Phys. Rev. Lett.* **85**, 1330 (2000).

[41] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill. *Quant. Inf. Comp.)* **4**, 325 (2004).

[42] W.-Y. Hwang. *Phys. Rev. Lett.* **91**, 057901 (2003).

[43] X. B. Wang. *Phys. Rev. Lett.* **94**, 230503 (2005).

[44] X. Ma, B. Qi, Y. Zhao and H.-K. Lo. *Phys. Rev. A* **72**, 012326 (2005).

[45] Y. Zhao, C.-H. Fred Fung, B. Qi, C. Chen, and H.-K. Lo. *Phys. Rev. A* **78**, 042333 (2008).

[46] V. Makarov and D.R. Hjelm. *J. Mod. Opt.* **52**, 691 (2005).

[47] V. Makarov, A. Anisimov, and J. Skaar. *Phys. Rev. A* **74**, 022313 (2006).

[48] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov. *Nature Photonics* **4**, 686 (2010).

[49] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. *Phys. Rev. A* **73**, 022320 (2006).

[50] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, V. Scarani. *New Journal of Physics* **11**, 045021 (2009).

[51] X. Mo, I. Lucio Martinez, P. Chan, C. Healey, S. Hosier, W. Tittel. *Optics Express* **19**, 17729 (2011).

[52] G. P. Agrawal. *Fiber-Optic Communication Systems.* John Wiley & Sons, New York NY, (1997).

[53] G. Brassard, L. Salvail. *Advances in Cryptology EURO-CRYPT* **765**, 410 (1994).

[54] C. Healey, I. Lucio Martinez, M.R.E. Lamont, X. Mo and W. Tittel. *arXiv:quant-ph/1105.3760* .

[55] Z.L. Yuan, A.W. Sharpe, J.F. Dynes, A.R. Dixon, and A.J. Shields. *Appl. Phys. Lett.* **96**, 071101 (2010).

[56] A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G. N. Gol'tsman, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Slysz, A. Pearlman, A. Verevkin, and R. Sobolewski. *Appl. Phys. Lett.* **84**, 5338 (2004).