On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source

by

Chris Erven

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Science
in
Physics

Waterloo, Ontario, Canada, 2007

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

C. Erven

I understand that my thesis may be made electronically available to the public.

C. Erven

Abstract

This thesis describes the deployment of a free-space quantum key distribution system across the University of Waterloo campus. The quantum key distribution system has the ability to provide unconditionally secure communication between two parties: Alice and Bob. The system exploits the quantum mechanical property of entanglement in order to generate a key. Security is then guaranteed by the No-Cloning theorem and the laws of quantum mechanics which prevent a quantum system from being measured without disturbing it. Polarization-entangled photon pairs are created using the non-linear optical process of type-II spontaneous parametric down-conversion. A free-space link of approximately 580 m is used to distribute one-half of the pairs to Alice at a distant location, while the other half of the pairs are locally detected by Bob. The details of the detection apparatus necessary to measure the polarization of the photons and the software used to process the measurement data according to the BBM92 protocol are described. An experimental violation of the CHSH inequality (a derivative of the original Bell inequality) is demonstrated to show that polarization-entangled photon pairs are in fact being distributed to the two parties. Finally, the full BBM92 protocol is performed using the entangled photon pairs to generate a secure key and transmit an encrypted message between Alice and Bob. Currently, the system can only be operated at night because background light saturates the detectors during the day; however, future work will focus on making daylight operation feasible.

Acknowledgements

First, I must thank Dr. Gregor Weihs for supervising and supporting my work over the course of my Masters program. His help and many insightful comments and suggestions have been a great aid to me in completing this project. In addition, I would like to thank Dr. Raymond Laflamme for co-supervising me during my Masters and using his directorial influence to speed along administrative permissions and requests necessary to complete this thesis. I must also thank the other members of my advisory committee; Dr. Norbert Lütkenhaus and Dr. Hamed Majedi, for their interest in my research and their helpful comments during committee meetings; and Dr. Kevin Resch for agreeing to be my external examiner for my Masters defence.

I am indebted to my parents, Jim and Sandy, and my sister, Lisa, for their love and support throughout my education. I want to thank Anne, for her patience, understanding, and moral support. She has on more then one occasion listened to complaints about optics and electronics that miraculously seemed to be conspiring against me during experiments.

I have to thank a number of undergraduate co-op students and research assistants for their help during the project including: Paul McGrath, Matt Peloso (detector boxes and free-space design), Jordan Thompson, Benjamin Schmidt (software and GPS), and Nikolina Ilic (many late nights aligning and testing the system). As well, I have to thank Christophe Couteau, a postdoc in our group, for all of his optics advice and help in the lab; and Rolf Horn for his help in the lab, commiseration on the many trials and tribulations of graduate student life, and exercise on the badminton court. I also owe a huge thank you to Devin Smith for proofreading this thesis and helping to make it a much more readable document. Any lingering mistakes are the sole responsibility of the author.

I am grateful for the financial support from the IQC and from the Bell family through their Bell Family Fund for Quantum Computing Scholarship program.

Last, but not least, I would like to thank all of my friends and colleagues including: Martin Laforest, Casey Myers, J.C. Boileau, Hauke Häseler, Georg Heinrich, Toby Moroder, Osama Moussa, Marcus Silva, and any others I might have missed for the many needed beers; volleyball, tennis, and hockey games; and general comaraderie. And for occasionally helping to lug shacks and entangled photon sources up to rooftops.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The development of the transistor heralded the launch of the new electronic information processing age. It has brought with it rapid technological advancements in society and science; yet, the current electronic age is now starting to run up against fundamental physical limitations which are slowing its progress. As things get smaller, the classical notions which have been used to develop the electronics industry have become inadequate because quantum effects are starting to dominate. Rather than being a problem, however, these quantum effects provide us with the possibility for the next technological revolution: the quantum information age. Many new ideas have formed out of the new quantum information paradigm, one of the most successful and notable of them is quantum key distribution.

1.1 Quantum Computing

Quantum computing exploits the features of quantum mechanics such as the superposition principle, entanglement, and quantum interference, in order to produce more efficient algorithms for computation and unconditionally secure protocols for communication [28]. While the entire subject of quantum information and computation is vast[1], this thesis will

[1]For a more complete description of the field of Quantum Information Processing, please refer to [32].

focus on developing a practical quantum key distribution system. For this, the pertinent concepts from quantum information are discussed in the following.

1.1.1 Qubits

In classical computing, the main fundamental computational unit is the bit. It can either have the value of 0 or 1. The analogous concept for quantum computing is the quantum bit or qubit. A qubit can be in one of two orthogonal states $|0\rangle$ or $|1\rangle$, or any coherent superposition of these two states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Any two level quantum system can be used to encode a qubit, such as, spins of electrons or nuclei, the polarization of photons, or superconductors and Josephson junctions arranged to form flux, phase, or charge qubits. Two qubits are represented by states of the form $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

All of the experiments in this work will use the polarization of photons as qubits with the two orthogonal states being $|H\rangle$ and $|V\rangle$ where H and V refer to the horizontal and vertical polarizations of a photon with respect to a suitable frame of reference. The $|H\rangle$ and $|V\rangle$ states correspond to the computational basis states $|0\rangle$ and $|1\rangle$ respectively. Photons are ideal qubits for quantum communication and cryptography schemes because of their weak interaction with each other and most matter. This weak interaction translates into low decoherence rates, so that the qubits maintain their quantum states for a long time [32]. Also, they move at the speed of light which makes it possible to transmit them very quickly over large distances.

1.1.2 Entanglement and Bell States

The principle of superposition can lead to states with uniquely quantum mechanical correlations, called entanglement, which cannot be represented as the product of independent states of each qubit [24]. Einstein, Podolsky, and Rosen (EPR) studied these states in 1935 [14] for purely philosophical concerns about the nonlocality and completeness of quantum mechanics. They were concerned with the nonlocality inherent in an entangled pair of space-like separated particles. Quantum mechanics predicted that a measurement on particle 1 could affect a subsequent measurement on particle 2 even though they were

space-like separated and thus could not interact in any way. More precisely, this meant that the two particles did not possess physical properties that existed independently of observation. EPR argued that quantum mechanics must therefore be an incomplete description of reality. David Bohm simplified EPR's work in 1957 [9] using a system of spin-$\frac{1}{2}$ particles in the anti-symmetric entangled state $|\psi\rangle = \frac{1}{2}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$. A state which leaves the individual particles in an undefined spin state, but which defines their joint property of always having orthogonal spins. John Bell continued this work and showed that the predictions of quantum mechanics deviate from those of a local realistic theory when measuring the Bell inequality which is discussed in Section 1.1.3. In other words, the measurement correlations in this entangled state are stronger than could ever exist between classical systems.

There have been many experiments performed which validate the predictions of quantum mechanics using various types of entangled particles, such as photons [3, 42], single ions [35], and more. More important though is the fact that entanglement is now understood as a quantum computing resource and that the stronger-than-classical correlations can be used to build secure quantum cryptographic protocols.

There are four maximally entangled two qubit states which can be used for quantum cryptography, known as the Bell states. They have the following form using the polarization of photons:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle) \tag{1.1}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \tag{1.2}$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \tag{1.3}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle). \tag{1.4}$$

These form a complete orthonormal basis for all polarization states of a two photon system. The Bell states have the property that measuring the polarization of one photon produces

one of two possible random results: H with a probability of $\frac{1}{2}$ or V with a probability $\frac{1}{2}$.[2] But upon measuring the polarization of the other photon a particular correlated result is always found. The correlation depends on the particular Bell state that is measured. In the case of the anti-symmetric, rotationally invariant $|\psi^-\rangle$ state, perfect anti-correlated results will always be observed. This anti-correlation of the entangled $|\psi^-\rangle$ state will be a key feature of quantum cryptographic protocols.

1.1.3 Bell Inequalities

In 1964 J.S. Bell [4] derived an inequality for correlation measurements which showed that the results for entangled states, which are predicted by quantum mechanics, could not be reproduced by a local realistic theory based on hidden variables. In other words, entangled particles could violate this inequality, while two particles that were assigned local hidden variables (parameters that the particles carry with them which determine their measurement results) and acted independently when measured could not. In order to reconcile this fact some of the assumptions used in the derivation of Bell's inequality have to be discarded, either locality or realism, or perhaps both.

There are many variants of Bell's inequality; one that is particularly suitable for experiments is the CHSH inequality derived by Clauser, Horne, Shimony, and Holt in 1969 [12]. A slightly modified version of their inequality is given by

$$S(\alpha, \beta, \alpha', \beta') = |E(\alpha, \beta) + E(\alpha', \beta) + E(\alpha, \beta') - E(\alpha', \beta')| \leq 2 \tag{1.5}$$

where $E(\alpha, \beta)$ is the expectation value of polarization correlation measurements made on a two photon system with the polarization measured at the angles α and β respectively.

The following short derivation of the CHSH inequality is due to a combination of A. Peres [33] and Neilsen and Chuang [32]. Suppose two observers, Alice and Bob, each get one photon from a two-photon system to measure. Alice can measure the polarization of her photon at the angles α and α', while Bob can measure his photon at the angles β and β'. For a particular choice of measurement angle, the measurement device can either tell

[2] Actually, a local polarization measurement in any basis produces locally random results with a probability of $\frac{1}{2}$ and a global correlation dependent upon which Bell state is being measured.

the observer that the photon was polarized parallel or perpendicular to the chosen angle. For example, Alice measuring a photon at an angle $\alpha = 0°$ (the H/V basis) can either get the result H or V. A measurement result parallel to the measurement angle is assigned a value of +1, while the orthogonal measurement result is assigned a value of -1. Let the corresponding measurement results for the angles α, α', β, and β' be represented by the variables a, a', b, and b'. These variables can have the values ± 1.

Now consider the equation

$$ab + a'b + ab' - a'b' = (a + a')b + (a - a')b' \tag{1.6}$$

since $a, a' = \pm 1$ it is easy to see that either $(a+a')b = 0$ or $(a-a')b' = 0$ which means that Equation 1.6 must equal ± 2. Now, if several photon pairs are tested, the jth pair yields

$$a_j b_j + a'_j b_j + a_j b'_j - a'_j b'_j = \pm 2. \tag{1.7}$$

Converting this to expectation values and taking the absolute value gives[3]

$$|\langle ab\rangle + \langle a'b\rangle + \langle ab'\rangle - \langle a'b'\rangle| \leq 2. \tag{1.8}$$

Writing the expectation value $\langle ab\rangle$ instead as $E(\alpha, \beta)$ and similarly for the other three terms results in the CHSH inequality of Equation 1.5.

The CHSH inequality can be violated, for instance, if the two photons are in any of the Bell states of Section 1.1.2. In particular, if the photons are in the entangled $|\psi^-\rangle$ state, the expectation value according to quantum mechanics is given by

$$E(\alpha, \beta) = -\cos(\alpha - \beta). \tag{1.9}$$

It can be shown that the Bell parameter, S, is maximized at $S = 2\sqrt{2}$ for the angles $\alpha = 0° + \phi$, $\beta = 22.5° + \phi$, $\alpha' = 45° + \phi$, and $\beta' = 67.5° + \phi$, for any constant offset ϕ. This violation can also be used to show entanglement since $S > 2$ can only be achieved with entangled states.

[3]The equality becomes an inequality because sometimes $a_j b_j + a'_j b_j + a_j b'_j - a'_j b'_j$ will equal +2 while other times it will equal -2, so the expectation value $|\langle ab\rangle + \langle a'b\rangle + \langle ab'\rangle - \langle a'b'\rangle|$ will generally be < 2. Equality will be fulfilled when every $a_j b_j + a'_j b_j + a_j b'_j - a'_j b'_j$ has the same measurement result.

The CHSH inequality has the advantage that it can allow for experimental deficiencies such as the loss of particles or imperfect state preparation. No perfect anti-correlation is needed for its derivation, and the particle detection efficiency does not have to be 100%. The only assumption it requires is the fair sampling assumption, which means that the probability of the joint detection of a pair of photons is independent of the measurement angles used.

In experiment, the expectation values $E(\alpha, \beta)$ are calculated from the number of events for each set of measurement angles as follows

$$E(\alpha, \beta) = \frac{C_{++}(\alpha, \beta) + C_{--}(\alpha, \beta) - C_{+-}(\alpha, \beta) - C_{-+}(\alpha, \beta)}{N} \tag{1.10}$$

where $C_{++}(\alpha, \beta)$ represents the number of events where both photons were measured to be parallel to the directions α and β and similarly for the other terms. Lastly, N is the total number of events given by

$$N = C_{++}(\alpha, \beta) + C_{--}(\alpha, \beta) + C_{+-}(\alpha, \beta) + C_{-+}(\alpha, \beta). \tag{1.11}$$

1.1.4 No Cloning Theorem

The No Cloning theorem is an important fact concerning the possibility of copying the unknown state of a qubit, first shown by Wootters and Zurek [43] and Dieks [13] in 1982. As will be seen in Section 1.2.4, the security of quantum cryptography relies on the fact that it is impossible to copy an unknown quantum state. Otherwise, an eavesdropper would be able to make a copy of the qubits used to generate the secure key. They would then be able to use the public information sent between Alice and Bob during the BBM92 protocol to produce a key identical to the one shared by Alice and Bob. Thus, they would be able to decrypt and read any information subsequently sent between Alice and Bob.

The impossibility of cloning a qubit is shown by the following argument. Suppose there exists a quantum machine which attempts to copy the state of an unknown data qubit (without disturbing it) onto a target qubit through some unitary operation U. The input starts out in the state

$$|\psi\rangle \otimes |s\rangle \tag{1.12}$$

where $|\psi\rangle$ is the data qubit attempting to be copied and $|s\rangle$ is the target qubit initialized in a pure state. The unitary evolution now performs the copying procedure

$$|\psi\rangle \otimes |s\rangle \longrightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle. \tag{1.13}$$

Now suppose that this procedure works for two particular pure states, $|\psi\rangle$ and $|\varphi\rangle$; this implies

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{1.14}$$

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle. \tag{1.15}$$

If the inner product of Equation 1.14 with Equation 1.15 is calculated, the following equality is arrived at

$$\langle\varphi|\psi\rangle = (\langle\varphi|\psi\rangle)^2 \tag{1.16}$$

But Equation 1.16 only has the two solutions $\langle\varphi|\psi\rangle = 0$ or $\langle\varphi|\psi\rangle = 1$, meaning either $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal. Thus, a quantum cloning device can only copy states which are orthogonal to one another, and therefore a general quantum cloning device is impossible [32].

While perfect quantum cloning is impossible an optimal procedure for approximate quantum cloning has been developed by Buzek and Hillery [10]. However, this procedure leaves the two identical output qubits in the mixed state ρ which has a maximum fidelity of $F = 0.82$ with the original state $|\psi\rangle$, where the fidelity is defined as $F \equiv \langle\psi|\rho|\psi\rangle$. This means that if an eavesdropper attempts to use this procedure to copy the qubits used to generate the secret key, she will inevitably disturb those qubits; this disturbance will be detectable, and indicate that the key is not secure.

1.2 Quantum Cryptography

The basic task of any cryptographic scheme is to provide two parties, typically called Alice and Bob, with secure communication so that data transmitted between them is indecipherable to any third party, commonly called Eve, who might be listening in.

1.2.1 Problems with Classical Cryptography

There is one provably secure cryptographic scheme: the Vernam Cypher or One-Time Pad [40], which requires a secret random key that Alice and Bob share. There are a number of problems with this, primarily that the keys have to be physically transported to Alice and Bob securely; which becomes increasingly cumbersome as the distance between them grows. Moreover, it is always in principle possible for Eve to intercept a classically distributed key and copy it without being detected since there is no analog of the No Cloning theorem for classical information. Another problem is that the key has to be as long as the data to be encrypted, meaning that large amounts of data require large amounts of key.

These key distribution problems led to the creation of public key cryptosystems. These systems usually have two keys: a public key and a private key. Data is encrypted by a user with the public key using a public algorithm. The security of the system is based on the fact that the encryption algorithm uses a one-way mathematical function (a function which is easy to compute in one direction, but who's inverse operation is computationally hard). Decrypting the data is hard, unless you have a special piece of information — the private key. This removes the need for key distribution since you can post the public key for all to see; however, it comes with a cost. The one-way function relies on the computational complexity of inverting the function in order to say that it is one-way. In other words, the most efficient algorithms that we currently know for a classical computer which can solve the inverse of the function (and thus decrypt the data) take an impractical amount of time to finish for a key of sufficient size. However, this assumption of computational complexity has already been shown to be invalid, if we have a quantum computer at our disposal, for many of the popular public key cryptosystems; such as, RSA and elliptic curve cryptography. Thus, there is an intrinsic need to develop new cryptographic systems which are provably secure for use in the future.

1.2.2 The Vernam Cypher

In the previous section, it was stated that there was one provably secure [37] encryption protocol known as the Vernam Cypher [40]. Since Quantum Key Distribution will rely on

this protocol, it is explained more fully here. The protocol relies on a secret random bit string (the secret key) known only to Alice and Bob. The secret key must be the same length as the data to encrypt. By using the secret key only once to encrypt and decrypt the data it is impossible for anyone who receives only the encrypted data to decrypt it without knowing the secret key. However, if the secret key is used more the once, there are statistical and numerical techniques that an eavesdropper can use to begin to discover the secret key and decypher the data.

A simple implementation of the Vernam cypher is using the bitwise XOR (exclusive-OR) operation of digital logic on the key and data to both encrypt and decrypt the message. An example of encrypting and decrypting a short ASCII message is given in Table 1.1. The requirement of only using the key once to encrypt and decrypt can be illustrated with a simple attack on two different messages that were encrypted using the same key as in Table 1.1. If the two encrypted messages are combined with the XOR operation, the result will be the XOR of the two original messages with the key removed. Since the message bit strings are no longer random without the key, statistical techniques can then be used to rapidly recover the two original messages.

Message (Alice)	1001000 1101001	$\Longleftarrow$ "Hi"
Key (Alice)	0010111 0100101	
Encrypted Message (Alice)	1011111 1001100	$\Longrightarrow$ "-L"
Coded Message Received (Bob)	1011111 1001100	$\Longleftarrow$ "-L"
Key (Bob)	0010111 0100101	
Decrypted Message (Bob)	1001000 1101001	$\Longrightarrow$ "Hi"

Table 1.1: Implementation of the Vernam Cypher with the XOR operation. Alice encrypts the message she wishes to send to Bob using her key and the XOR operation as the encrypting operation. Bob receives the encrypted message and performs the inverse operation (the XOR again) with his secret key in order to decrypt and recover Alice's original message.

The security of the Vernam cypher relies on the following:

- The key must be random to avoid statistical attacks

- The key must be securely transported to Alice and Bob so that its secrecy is assured

Classically, both of these requirements are hard to accomplish securely. For the first requirement, generating truly random numbers is hard, and any patterns in the key can lead to successful statistical attacks. The second requirement is even more difficult, since transported keys can in principle always be intercepted, copied by Eve, and sent on to Alice and Bob without their knowledge. Eve would then be able to listen to any communication between Alice and Bob which used those keys. Quantum key distribution provides a solution to these problems, allowing one to have a proveably secure encryption/decryption protocol.

1.2.3 Quantum Key Distribution

Quantum cryptography, or perhaps more properly quantum key distribution, began with the BB84 protocol proposed by C.H. Bennett and G. Brassard in 1984 [6] which showed how one could distribute a random secret key between Alice and Bob using single qubits along a quantum channel. The security of quantum key distribution is due to random measurements of the qubits in one of two complementary, non-orthogonal bases, and the fact that quantum mechanics prohibits an eavesdropper from gaining information on the state of an unknown qubit without disturbing it. Thus, any subsequent measurement of a complementary observable on the same qubit becomes random. Alice and Bob need only start with a small amount of shared secret key to initially authenticate each other and then can use quantum key distribution to distribute as large a key as needed between themselves.

There are many different protocols for quantum key distribution, a good overview of several QKD schemes can be found in a review paper by Gisin *et al* [17]. Quantum cryptography with the BB84 protocol can be performed ideally with single photons [8] or, more practically, with weak coherent laser pulses [5]. However, the weak coherent laser pulse schemes are open to the photon number splitting attack since more than one photon is sometimes created in a pulse. Eve could then split off one photon for her to measure from each multi-pair event and gain information about the key. A method for

overcoming the photon-number-splitting attack for the weak laser pulse implementations has been developed using decoy states [20]. Quantum key distribution protocols have also been extended to use entangled qubit pairs as in the Ekert91 protocol proposed by Ekert in 1991 [15] or the BBM92 protocol by Bennett, Brassard, and Mermin in 1992 [7]. This work implements quantum key distribution with the BBM92 protocol using pairs of polarization-entangled photons.

A range of experiments have demonstrated the feasibility of quantum key distribution [42, 30, 19, 34, 25, 39]. There are a number of advantages of the entanglement based QKD schemes over the single photon and weak laser pulse schemes. The entangled photon source can also be viewed as a conditional single photon source [18], which is an important criterion for the security of the QKD system. Also, the probability of having two photon pairs within a coincidence window is sometimes lower then the probability of having two photons per pulse when using weak laser pulses [28]. Moreover, it is not clear that multi-pair emission in a parametric down-conversion source necessarily leaks any information to Eve in the way that it does for BB84 implemented with weak laser pulses. This reduces the possibility of the photon-number splitting attack. Also, the inherent objective randomness of the entangled photon source[4] leads to purely random keys, which are very hard to create classically but are an important ingredient for secure communication. [22]

1.2.4 BBM92 Protocol

The BBM92 protocol using polarization-entangled photon pairs is a very elegant variation of the BB84 protocol. An overview of the BBM92 protocol is shown in Figure 1.1. A source produces polarization-entangled photon pairs in the $|\psi^-\rangle$ state. These pairs are then split up with one photon from each pair being sent to Alice and one to Bob. Alice and Bob each randomly choose to measure each photon they receive in one of two non-orthogonal complementary bases, the horizontal/vertical basis ($H = 0°$ and $V = 90°$) or the +/- basis ($+ = +45°$ and $- = -45°$). After a measurement run, where Alice and Bob have

[4]Since each of Alice's and Bob's measurement results are random due to quantum mechanics, their key bit strings which are formed from these measurements are also random. Globally, the measurement results are correlated, by individually each measurement and thus each bit in the key is random.

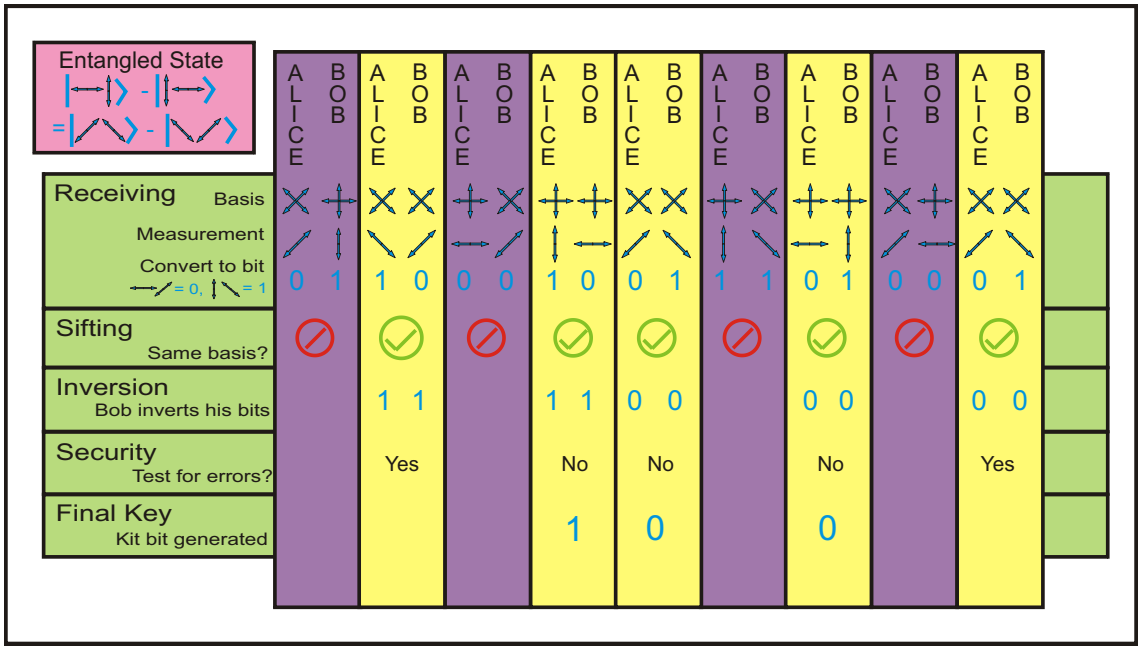

Figure 1.1: The complete BBM92 protocol. Alice and Bob each receive one photon from a stream of entangled photon pairs, they randomly pick a basis to measure each photon in, get a measurement result, convert their result to a classical bit, sift their results down to only those where they measured in the same basis, use 10% of their measurements to estimate the quantum bit error rate (QBER), and generate a final secure key from the rest of their measurement results.

been measuring incoming photons for a certain time, they communicate publically over a classical channel which basis they measured in for each photon they received.[5] Whenever they measured in the same basis they each save their measurement result, since it should be anti-correlated and they will be able to form a secret key from it. The rotational invariance of the $|\psi^-\rangle$ state means that Alice and Bob will observe perfect anti-correlation not only

[5]It is important to note that publically disclosing which basis they measured each photon in does not give Eve any information about the eventual secret key since it is generated from the measurement results, and disclosing the measurement basis does not reveal anything about their measurement results.

in the H/V basis, but also in the +/- basis as shown in Equation 1.17.

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \tag{1.17}$$

Alice and Bob discard any measurement results where they measured in different bases since the results will be uncorrelated. This process is called sifting because Alice and Bob are reducing their measurements to only those where they measured in the same basis and thus will have anti-correlated measurement results.

Next Alice and Bob convert their measurement results to bit values by assigning the measurement results H and + to the bit value 0 and V and - to the bit value 1. Since the $|\psi^-\rangle$ state produces anti-correlated results, Bob inverts his bit string so that he and Alice arrive at an identical, random, secret key shared between them. This is also called the raw key.

The security of the protocol is based on Alice's and Bob's use of two non-orthogonal complementary measurement bases, which makes the result of a second measurement in the complementary basis random. This can be seen as a result of Heisenberg's uncertainty principle, or equivalently due to the No-Cloning Theorem of Section 1.1.4 which prevents Eve from making copies of the qubits and then delaying her measurements until Alice and Bob have publically disclosed their measurement basis for each qubit. Thus, any eavesdropper attempting to gain information on the photons being sent to Alice or Bob inevitably will disturb the entangled state and introduce errors into the raw key. Therefore, Alice's and Bob's verification of the security of their raw key consists of comparing a small random subset of the bits from their raw key over the public classical channel in order to estimate the quantum bit error rate (QBER). Then using information theoretic arguments concerning the mutual information between Alice, Bob, and Eve, an upper bound of $\sim 14.6\%$ [17] can be found on the tolerable error rate for key distribution secure against individual attacks. A more detailed description of the important security thresholds can be found in Section 1.2.5.

This security argument can be illustrated with a simple eavesdropping approach (as shown in Figure 1.2) where Eve intercepts and measures the photons, meant to reach Bob, in one of the two polarization bases. Eve then resends another photon, polarized

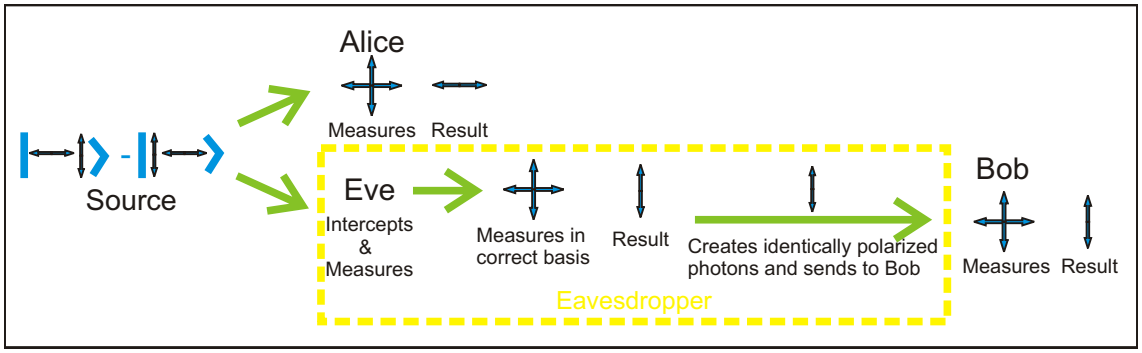

Figure 1.2: A simple intercept-resend attack. Eve intercepts each photon meant for Bob, randomly picks a basis to measure in, gets a result, and sends an identical photon to Bob. Eve's measurement collapses the superposition of the $|\psi^-\rangle$ state and ruins the quantum coherence responsible for the perfect anti-correlations in any basis. The final result is an increased error rate which Alice and Bob can detect and use to determine that their key is insecure.

according to the measurement outcome of the intercepted photon, to Bob. Alice and Bob only keep results where they measure in the same basis, and Eve now has a 50% chance of measuring in either basis. If Eve measures in the same basis as Bob, then she does not introduce any errors and Alice and Bob get the anti-correlated measurement results which they expect. However, 50% of the time Eve measures in the complementary basis and now will introduce an error into Bob's key due to his subsequent complimentary measurement and the Heisenberg uncertainy principle. Thus, Bob will get an error with a probability of 50%. Therefore, the total error rate that Eve induces will be 25%. This is well above the tolerable QBER of $\sim 14.6\%$ for individual attacks and will be detected by Alice and Bob, alerting them to the presence of an eavesdropper.

After the QBER estimation, the raw key then goes through two more processing steps before it is turned into the final secure secret key. While theoretically Alice and Bob should measure a completely anti-correlated raw key, in a practical real life set-up (without an eavesdropper) there will be small imperfections which contribute to a non-zero error rate. Thus, it is necessary to perform classical error correction (Section 5.4.3) on the raw key to

remove these errors. Lastly, Eve might have employed a strategy where she only measured a certain percentage of the qubits in order to keep Alice's and Bob's measured QBER under the acceptable threshold. Alice and Bob therefore perform a classical privacy amplification protocol (Section 5.4.4) on their error-corrected key to reduce the maximum potential information Eve might have gained about the key to an arbitrarily small value. Alice and Bob now possess a secure, random, secret key which they can use with the Vernam One-Time Pad to communicate securely between themselves.

1.2.5 Security of QKD Protocols

The subject of security proofs for quantum key distribution protocols is an extremely active area of research with frequently changing methods and thresholds. This section limits its discussion to two thresholds for specific attacks which have been established: symmetric individual attacks and coherent attacks. In both cases the thresholds examined are limited to one-way quantum key distribution protocols which is what is implemented in this thesis.[6] One-way quantum key distribution refers to protocols that only allow Alice and Bob one-way communication. In other words, they receive their qubits and do not perform any other quantum operations on them which depend on communication between Alice and Bob. There is another class of more general protocols which use two-way communication between Alice and Bob to perform a process called advantage distillation. These protocols can guarantee security for higher quantum bit error rates than one-way protocols as long as Eve's actions do not disentangle Alice's and Bob's qubits. However, in practice the one-way protocols are more realistic since the advantage distillation algorithms are much less efficient then classical privacy amplification algorithms [17].

The first threshold is for symmetric individual attacks which means Eve is restricted to attacks on a single qubit at a time. Gisin *et al* [17] show in their paper that Eve's maximal

[6]The Cascade error correction protocol used in this thesis is actually two-way. However, two-way communication is used only as a trick to approach the Shannon limit for efficient error correction which is impractical to reach with a one-way protocol. The two-way communication in the Cascade algorithm does not allow advantage distillation. Therefore, the protocol implemented in this thesis is in fact a one-way protocol.

information for her optimum measurement strategy is given by

$$I^{max}(A,E) = \frac{2}{\ln 2}e + O(e^2) \approx \frac{2}{\ln 2}e \tag{1.18}$$

where $I^{max}(A,E)$ is the maximum Shannon information between Alice and Eve, and e is the error rate. After Alice, Bob, and Eve have measured their quantum systems, secret key agreement between Alice and Bob will only be possible if their mutual Shannon information $I(A,B)$ is greater than the Alice-Eve $I(A,E)$ or Bob-Eve $I(B,E)$ mutual information. Gisin *et al* show that Alice's and Bob's mutual information is given by

$$I(A,B) = 1 + e\log_2(e) + (1-e)\log_2(1-e). \tag{1.19}$$

Figure 1.3, from Gisin *et al* [17], plots Bob's and Eve's Shannon information versus the error rate. As the error rate increases, Eve's information increases while Bob's decreases. Eventually the two curves intersect at the specific error rate

$$e = \frac{1 - \frac{1}{\sqrt{2}}}{2} \approx 14.6\%. \tag{1.20}$$

This is the error threshold for individual attacks whereby no (one-way communication) error correction and privacy amplification protocol can produce a secure secret key for Alice and Bob.

Interestingly enough, there appears to be a connection between the threshold found in Equation 1.20 and the ability to violate the CHSH inequality of Section 1.1.3 [17]. With an imperfect quantum channel, the ability to violate the CHSH inequality is reduced to

$$S_{max}(e) = (1-2e)2\sqrt{2}. \tag{1.21}$$

The critical error rate for which the CHSH inequality can be violated is precisely that which was found to allow Alice and Bob to generate a secure key. The exact relationship of this connection remains an interesting open problem.

The second threshold deals with coherent attacks which means that Eve can manipulate several qubits coherently together. The proofs of this threshold are much less transparent then for the case of individual attacks, so only the results will be quoted. In 1998 Dominic

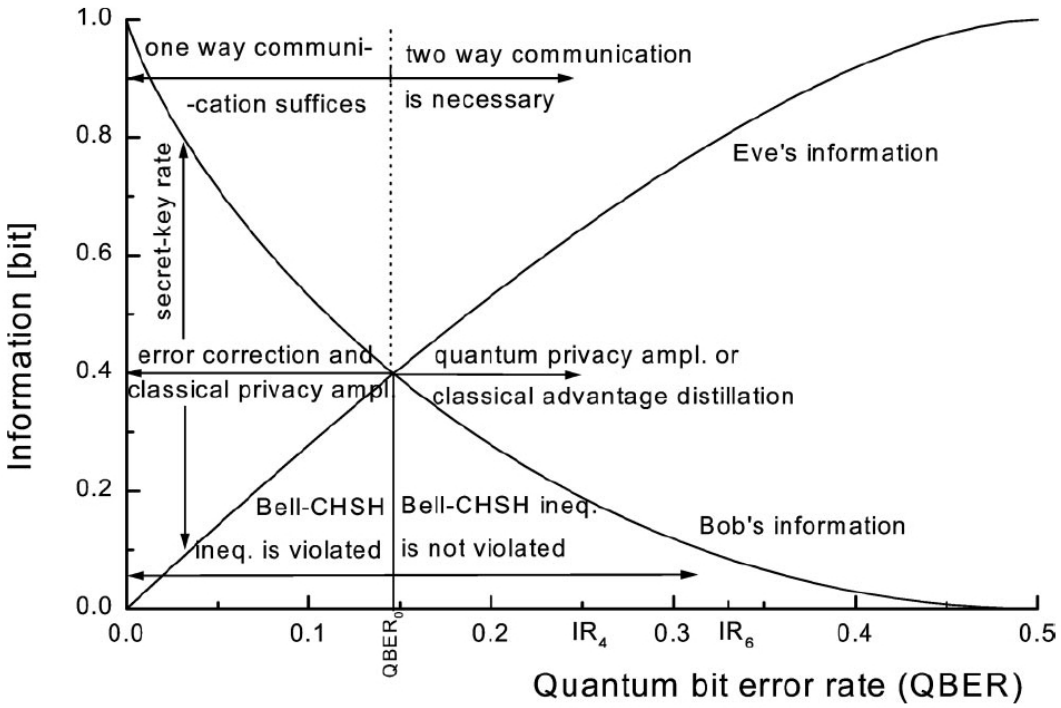

Figure 1.3: Error Thresholds. The error thresholds for one-way and two-way quantum key distribution protocols.

Mayers [31] and Hoi-Kwong Lo and H.F. Chau [29] developed a proof of security for these attacks which was improved by Shor and Preskill in 2000 [38]. These proofs found the following sufficient condition on the error rate in order to generate a secure key:

$$e \log_2(e) + (1-e) \log_2(1-e) \leq \frac{1}{2}. \tag{1.22}$$

This equation is solved for a threshold of

$$e \leq 11\% \tag{1.23}$$

below which a generated key is provably secure against the worst possible attack allowed by quantum mechanics.

These two thresholds provide the ability to say whether a particular generated key was secure or not. While the threshold of Equation 1.23 provides complete security, the technology needed to perform the coherent attack has not yet been developed. Thus, the threshold of Equation 1.20 is the practical threshold below which a key can be said to be secure against attacks using present day technology.

1.3 General Experimental Setup

A map of the overall setup of the QKD system that is described in this thesis can be seen in Figure 1.4.[7] Entangled photon pairs are distributed over the University of Waterloo (UW) campus. The source of polarization-entangled photon pairs is located on the sixth floor of the Centre for Environmental and Information Technology (CEIT) building in the middle of the UW campus. Single mode fibre optic cable carries one half of the entangled photon pairs to a sender telescope on the roof of the CEIT building; they then travel over a free space link to Alice's receiver telescope situated in a second floor office in the B.F. Goodrich (BFG) building at the northeast corner of the UW campus. The other half of the photons are locally detected by Bob on the sixth floor of the CEIT building. Alice and Bob use these photon pairs and a public channel (the internet) to build up two secure, secret keys which they can use to encrypt and decrypt data sent between them.

[7] The map actually shows two links, one from CEIT to BFG and another from CEIT to PI. Future work on the project includes getting a second link to PI working and moving Bob to an office located at PI. However, for the experiments detailed in this thesis, only the CEIT to BFG link is used.

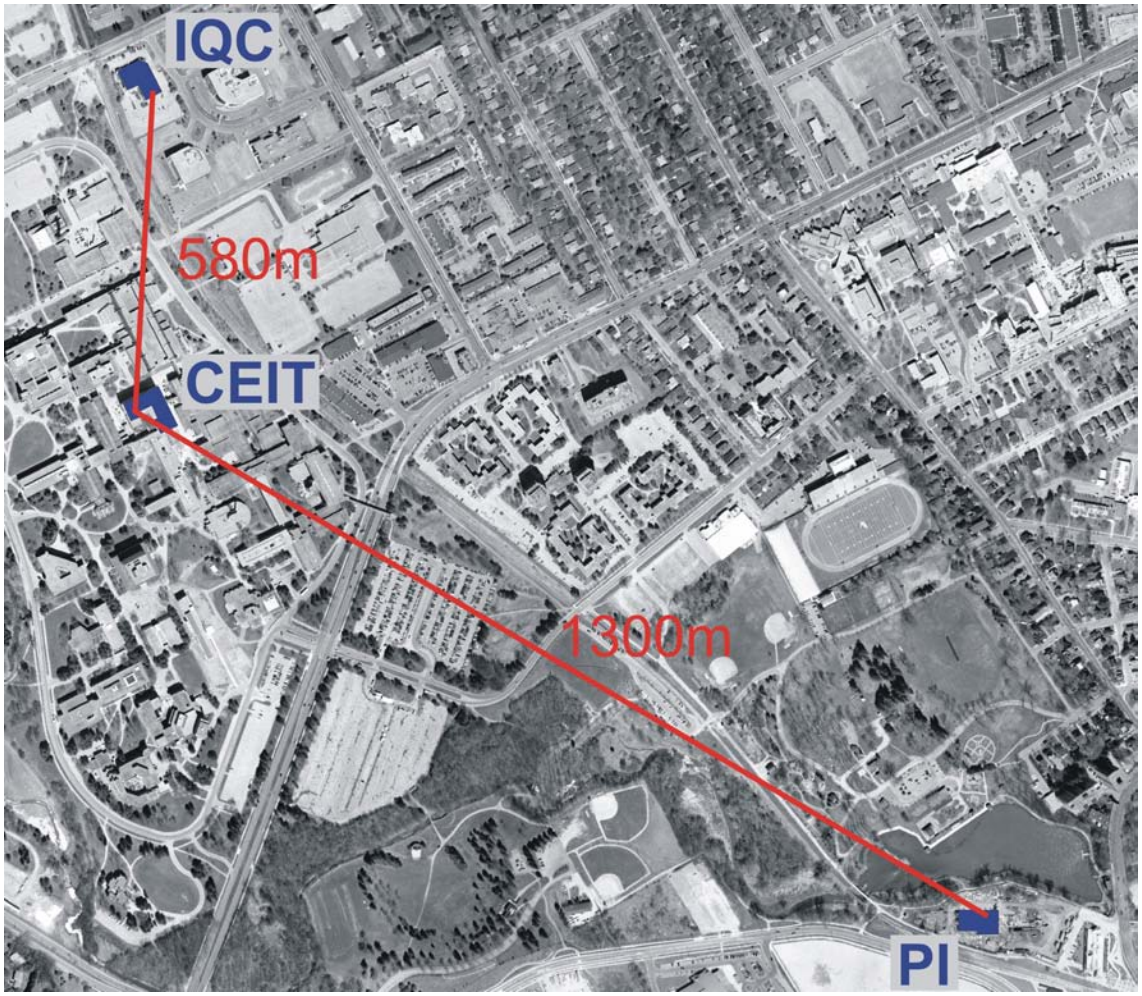

Figure 1.4: Map of the QKD setup. The experiments in this thesis use one free-space link: the CEIT to BFG link. Future work includes setting up a second link from CEIT to PI and moving Bob to an office at PI.

Chapter 2

Entangled Photon Source

The first piece required to implement Quantum Key Distribution is a source of entangled photon pairs that can be distributed to Alice and Bob. For the experiments described in this thesis, the polarization-entangled photon pairs are created with a non-linear optical process called type-II spontaneous parametric down-conversion. The original scheme using parametric down-conversion was developed by Kwiat *et al.* in 1995 [26] as a high efficiency source of entangled photon pairs. This chapter describes the theory and experimental setup of the photon source used herein.

2.1 Spontaneous Parametric Down Conversion

Parametric down-conversion is a non-linear optical process which relies on the $\chi^{(2)}$ optical non-linearity of certain media; for example, KDP, $LiIO_3$, $KNbO_3$, $LiNbO_3$, and BBO. For the source used in this thesis, a violet (407.5nm) pump laser beam is mixed with two vacuum infra-red (815nm) fields, known as the signal and idler beams, inside a BBO ($\beta - BaB_2O_4$) crystal. The non-linearity of the crystal leads to photon-pair production through spontaneous parametric down-conversion. Spontaneous parametric down-conversion is a distinctly quantum mechanical phenomenon, as it involves mixing vacuum fields with the pump field and classically one would never see light creation in those fields. Type II refers to the fact that for the emerging photon pairs, the signal photon has ex-

traordinary polarization while the idler photon has ordinary polarization.[1]

Two conservation laws have to be obeyed during the down-conversion process. The first law is the conservation of energy which requires the frequency of a pump photon to equal the sum of the frequencies of the two generated photons, ie.

$$h\nu_{pump} = h\nu_{signal} + h\nu_{idler}. \tag{2.1}$$

This process can be considered the splitting of a pump photon into two daughter photons.

The second law is the conservation of momentum which requires the wavevector of a pump photon to equal the sum of the wavevectors of the two generated photons, ie.

$$\hbar\vec{k}_{pump} = \hbar\vec{k}_{signal} + \hbar\vec{k}_{idler}. \tag{2.2}$$

Due to momentum conservation and the cut of the BBO crystal, the down-conversion photons are emitted on two cones as can be seen in Figure 2.1. Furthermore, the photons are emitted diametrically opposite to one another around the pump wavevector, with the extraordinary (signal) photon being vertically polarized and the ordinary (idler) photon being horizontally polarized.

Polarization entangled photons can be obtained by spatially and spectrally filtering the photons emerging on the intersection lines of the two cones. Energy conservation coupled with the crystal being cut for degenerate wavelength production guarantees that the photons will be indistinguishable according to their frequency. Momentum conservation guarantees that one photon will emerge from each side, but it will be impossible to distinguish which cone each photon came from. However, each of the two photons must be from a different cone, and thus they will always have opposite polarizations. Therefore, two photons will be emitted into two different spatial modes and they will have opposite polarizations but individually will have no definite polarization.

Due to the birefringence of the BBO crystal the propagation directions and velocities of horizontally and vertically polarized light are slightly different as they travel through the crystal. This leads to a transverse walk-off (spatial displacement) and longitudinal walk-off

[1]The polarization of a photon is defined as the direction of its electric field vector.

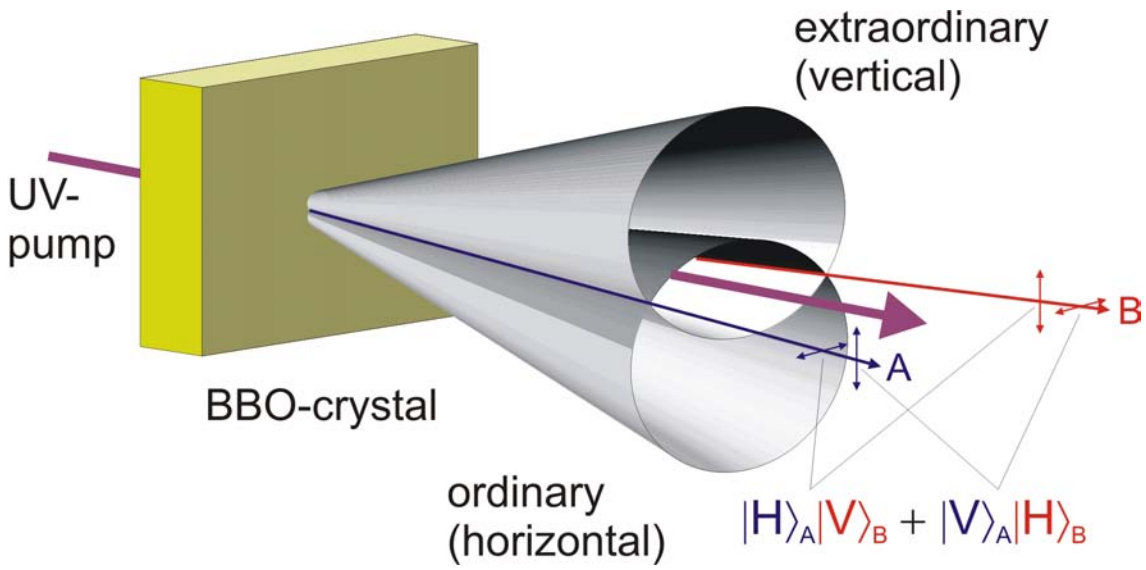

Figure 2.1: Type II spontaneous parametric down-conversion [41] produces photon pairs which emerge on two cones where the vertically polarized photon is on the upper cone and the horizontally polarized photon is on the lower cone. Polarization-entangled photons are observed at the two intersection lines of the cones.

(temporal displacement) of the horizontally polarized photons from the vertically polarized photons, thus the photons can be distinguished by their position and time-correlation relative to one another. While the walk-off effects cannot be truly compensated, the distinguishability of the photons can be washed out by the use of compensator BBO crystals. First, the down-converted photons have their polarizations rotated by 90° using a half-wave plate so that H is exchanged with V and vice versa. Each photon is then passed through a compensator BBO crystal which is half as thick as the original crystal that performs down-conversion. In this fashion, the walk-off effects are reversed by half, which consequently erases all temporal distinguishability and reduces the effects of the transverse walk-off. The temporal compensation can be seen in Figure 2.2. A schematic drawing for the complete setup necessary to generate polarization-entangled photon pairs is shown in Figure 2.3.

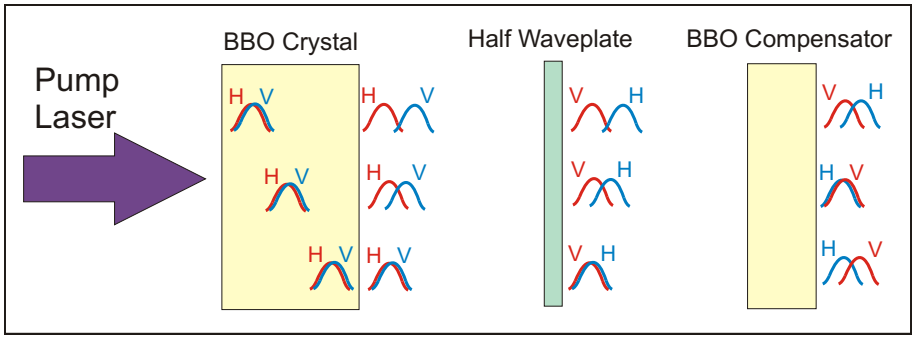

Figure 2.2: Longitudinal walk-off of the horizontally polarized photon from the vertically polarized photon occurs due to birefringence of the BBO crystal. It leads to a temporal distinguishability of the two photons, since their polarizations can now be determined by their time-correlation relative to one another. A half wave-plate and a compensator crystal are used to wash out this distinguishability and return the photons to an entangled state.

The states produced in the down-conversion process are a good approximation to the ideal state given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + e^{i\varphi}|VH\rangle). \tag{2.3}$$

The phase φ in the equation can be set to any desired angle by tilting one of the compensator crystals and thereby altering the phase between the two photons; tilting one of the compensator crystals so as to set $\varphi = \pi$, produces the $|\psi^-\rangle$ state as desired for the BBM92 protocol.

In any practical realization of quantum key distribution there will always be some errors due to imperfect alignment and compensation. In this case, the state produced in the down-conversion process will not be exactly that given by Equation 2.3. Instead, assuming a simplified white noise model, the partially decohered $|\psi^-\rangle$ state can be approximated by the density operator

$$\rho = V|\psi^-\rangle\langle\psi^-| + \frac{1-V}{4}I \tag{2.4}$$

where V is the visiblity and I is the identity operator used to represent the maximally

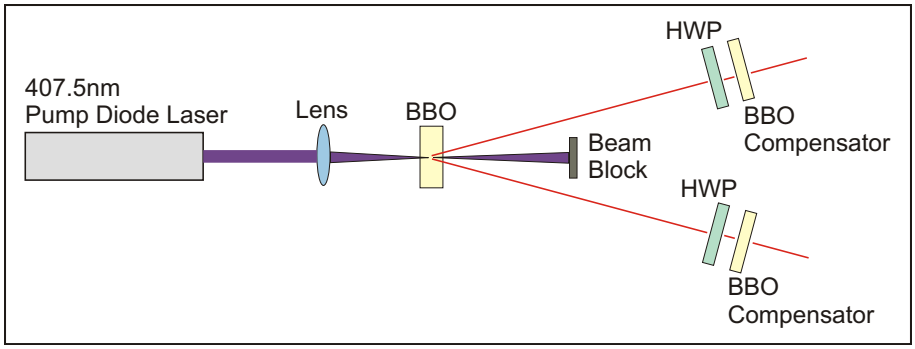

Figure 2.3: Schematic diagram of the setup needed to generate entangled photon pairs.

mixed state [28]. The visibility is defined by

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{2.5}$$

where I_{max} and I_{min} correspond to the expected and unexpected coincidence rates for the particular state being produced.[2] While the identity operator representing the maximally mixed state has the usual definition

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.6}$$

2.2 Experimental Setup of the Source

The source of polarization-entangled photon pairs is placed on the 6th floor of the CEIT building, as shown in Figure 2.4, under a plexiglass shield to protect it and reduce the amount of dust which builds up on the optics. The source is pumped by a 50 mW, 407.5 nm violet ChromaLase diode laser from Blue Sky Research, which can be seen along with the other components which comprise the source in Figure 2.5. This produces entangled photon

[2]For the $|\psi^-\rangle$ state, the expected coincidences are for the anti-correlated measurements (HV, VH, +-, -+) while the unexpected rates are for the correlated measurements (HH, VV, ++, - -). The names I_{max} and I_{min} are fairly intuitive since I_{max} should be a maximum and I_{min} should theoretically be zero for a perfect $|\psi^-\rangle$ source. A visibility of 100% is desired.

Figure 2.4: Portable entangled photon source sitting on the 6th floor of the CEIT building.

pairs at 815 nm which first pass through a half-wave plate and compensator crystal to wash out the transverse and longitudinal walk-off effects, and are then coupled into short single-mode optical fibres. The short optical fibres pass through polarization controllers necessary to correct the random polarization rotation which the fibres induce on the photons. One of the fibres is then connected to the detection equipment described in Chapter 4 so that Bob can measure it locally. While the other fibre is attached to a long single-mode fibre that guides the other photon from the pair to a sender telescope on the roof of the CEIT building where it will be sent over the free-space link, described in Chapter 3, to Alice.

The source is first aligned by locally maximizing the single photon count rates emerging

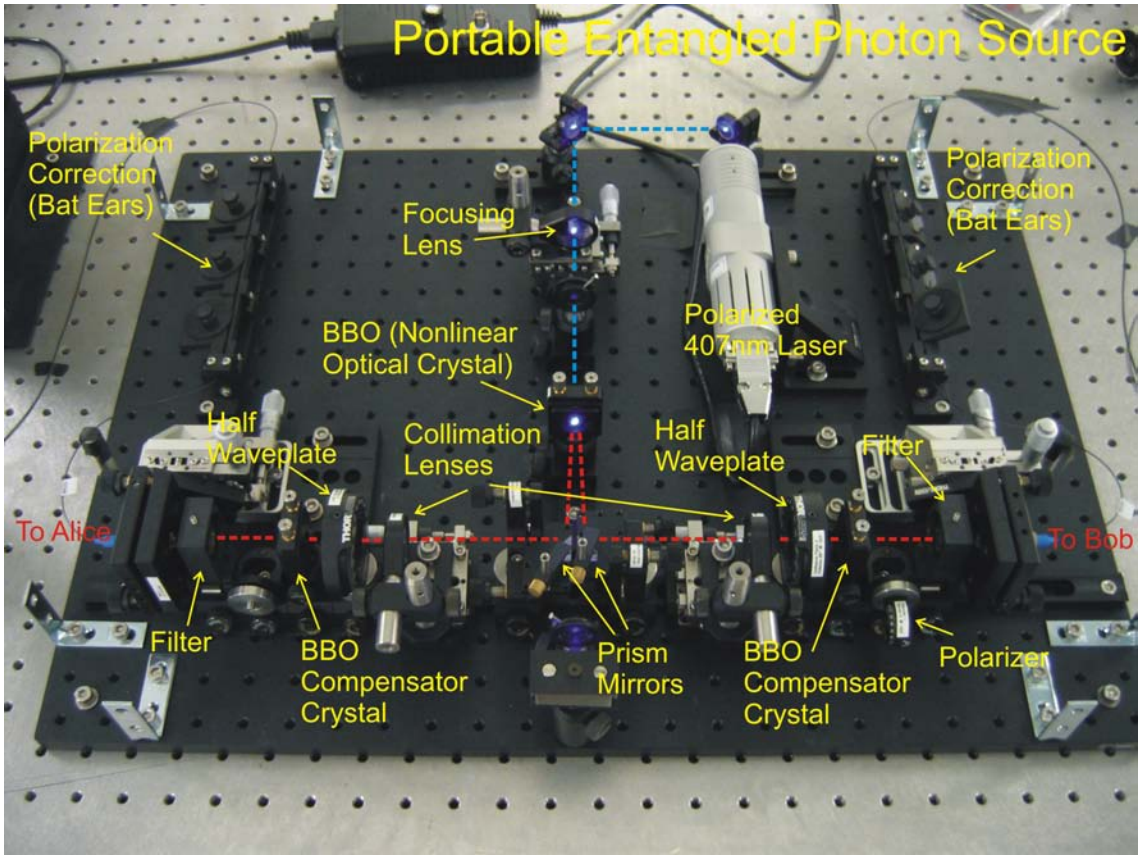

Figure 2.5: Detailed picture of the optics comprising the portable entangled photon source.

from either side. When properly aligned, the source has around 130,000 cps (counts-per-second) on Alice's side and around 120,000 cps on Bob's side. Besides being used to align the source, knowing the local single photon count rates will also allow the calculation of the transmission efficiency of the free-space optics by comparing the transmitted single photon count rates with the local single photon count rates. Next, the source is fine tuned to locally maximize the coincident photon count rate produced by the source. Coincident photons are defined as two photons which are detected in a narrow coincidence window of ten nanoseconds. These coincident events are attributed to detection of both photons from an entangled photon pair. A coincidence rate of about 18,000 cps is seen when the source

is fine tuned. Lastly, the visibility of the source in the H/V and +/- bases is maximized. The visibility in the H/V basis is adjusted by further fine tuning the alignment of the collimators, which couple the down-converted photons into the thin fibres, to select the correct spots on the down-converted cones. While the visibility in the +/- basis is adjusted by tilting one of the compensator crystals in order to set $\varphi = \pi$ in Equation 2.3.

A high visibility means that the coincident events which are expected from proper $|\psi^-\rangle$ states are high, while those that should not be possible are low. Simultaneously high visibilities in both bases are desired[3], since this corresponds to a high degree of anti-correlation in both bases and this is what the key generation protocol is relying on to form two identical secret shared keys for Alice and Bob. The visibility of the source in the H/V basis is around 98% while in the +/- basis it is around 92% when it is properly aligned.[4] The visibilities are less then the desired 100% due to imperfect alignment of the optics, imperfect compensation of the random polarization rotation induced on the photons by the single-mode fibres, and the coarse control over the precise tilt of the compensator crystal. These important characteristics of the source are summarized in Table 2.1.

[3]It is the simultaneous high visibility in two non-orthogonal bases which is the signature that this is a quantum mechanical state of light. This is evident by the fact that someone could easily devise a source which (classically) probabilistically emitted an HV pair of photons or a VH pair of photons; however, if these pairs were examined in any other basis, a high degree of anti-correlation would not be observed (all four possible states would be produced, say ++, +-, -+, and - -) and thus the visibility in a second basis would be low.

[4]Much better visibilities have been seen in previous experiments; however, work in this thesis primarily focused on developing an entire working QKD system. To that end, the source was aligned well enough to allow quantum key distribution and then work moved on to other aspects of the system. For future experimental results, the source will be fine tuned to generate better visibilities.

Singles Rates		Coincidence Rates (window = 10ns)
Alice Bob	130000 cps 120000 cps	18000 ccps
Visiblity		
H/V +/-	98% 92%	

Table 2.1: Important characteristics of the source.

Chapter 3

Free Space Communication

After polarization-entangled photon pairs have been generated they must be distributed to Alice and Bob. As described in Section 1.3, Bob is located next to the source and locally measures a photon from each pair; however, Alice is located at a distant location and thus the other half of the photons from each pair are sent over a free-space optical link to her. This chapter describes the theory of free-space communication, and the experimental setup of the free-space optics used in this thesis.

3.1 Theory

There are two main general problems with sending photons over a free-space link: transmission losses and background light. Since the signal is not transmitted in a guiding medium (such as a fibre optic cable) the energy can spread out leading to transmission losses. Additionally, extraneous background light can also couple into the receiver telescope leading to more background noise and an increased error rate. The errors induced by the background light can be reduced to a reasonable level by using spectral filtering, spatial filtering, and temporal discrimination with a coincidence window of a few nanoseconds [17].

For the transmission losses, there are a number of effects due to the atmosphere which play a role in the transmission efficiency of the free-space link. The atmosphere itself has a particular transmission efficiency for light due to atmospheric extinction of the photons

as they travel through the air. Atmospheric extinction refers to the process of photons interacting with air molecules, aerosol particles, and water droplets through scattering and absorption. These processes lead to the loss of some photons and an overall extinction of the light [28]. Fortunately, the atmosphere has a high transmission window ($\sim 85\%$) at a wavelength of about 800 nm where commercial, high-efficiency photon detection modules exist [17].

Atmospheric turbulence also has an effect on the photons as they pass over the free-space link. The turbulence leads to refractive index inhomogeneities in the air which can cause beam spreading and beam wander. Turbulent eddies which are large compared to the beam diameter can deflect the beam and lead to beam wander, while turbulent eddies which are small compared to the beam diameter can lead to scattering and produce beam spreading [17]. The use of larger receiver optics can somewhat compensate for these effects.

Lastly, the divergence of the Gaussian beam which emerges from the single-mode fibre and sender lens can limit the spot size at the receiver telescope. Again, the use of bigger optics and a larger beam diameter can compensate quite well for these effects.

3.2 Experimental Setup of the Free Space Optics

A schematic of the free space optics is shown in Figure 3.1. [1] A long single-mode optical

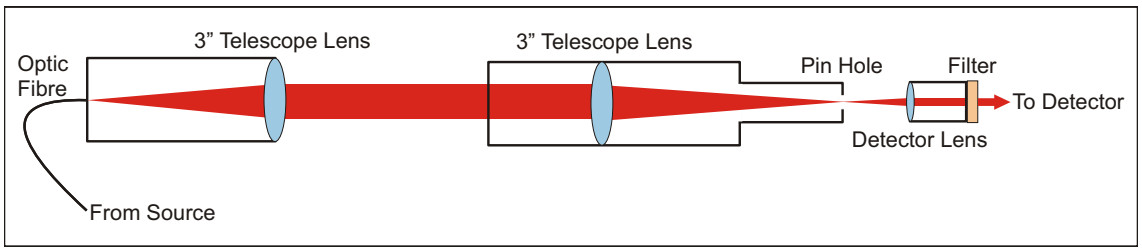

Figure 3.1: Schematic diagram of the free space optics.

[1] There are actually two complete free-space links available for future experiments; however, only one will be used with the experiments described in this thesis. For completeness, efficiencies for both links are included in Table 3.1.

fibre (45 m FiberCore SM800 5.6/125 μm, Fiber Instrument Sales Inc.) is used to guide one photon from each down-converted pair to a sender telescope on the rooftop of the CEIT building. The efficiency of the single mode fibre and fibre coupler used to get the photons to the roof is $\sim 87\%$.[2] The sender telescope consists of an FC connector mount for the bare single-mode fibre and an achromatic lens (NT45-417, 75 mm diameter, 200 mm focal length, Edmund Optics) which is matched as closely as possible to the NA of the optical fibre. The efficiency of the lens was experimentally measured, using a Titanium:Sapphire laser tuned to a wavelength of 815 nm, to be 93%. This lens collimates the photons into an approximately three inch Gaussian beam which is then transmitted through free-space to the receiving telescope at the BFG building. The photons are expanded into a three inch beam to reduce the effects of Gaussian beam divergence (or equivalently to avoid high diffraction losses due to the sender telescope aperature). The linear approximation for the beam divergence gives the equation

$$\theta = \frac{\lambda}{\pi W_o} \tag{3.1}$$

where λ is the wavelength of the light and W_o is the waist radius [36]. Using Equation 3.1 with a three inch Gaussian beam yields a divergence angle of $\theta = 1.02 \times 10^{-5}$ rad which corresponds to the beam diameter being broadened by ~ 12 mm over the 580 m link. If instead the ~ 3 mm beam produced in the down-conversion process had been used, a divergence angle of $\theta = 2.59 \times 10^{-4}$ rad corresponding to a beam diameter broadening of ~ 770 mm would have been produced at the receiver telescope. A beam of this size would have almost none of its photons captured by the three inch receiver telescope lens and resulted in a very poor transmission efficiency.

Figure 3.2 shows the sender telescope sitting in a protective enclosure on top of the CEIT building. The sender telescope is fixed to a custom built mount made out of aluminum extrusion pieces from 80/20 Inc. Figure 3.3 shows the coarse and fine alignment mechanism used to align the sender telescope with the receiver telescope at the BFG building. The coarse alignment consists of 80/20 Inc. pivot pieces which can be locked firmly in place

[2]For all of the transmission efficiencies measured in this section, there is about a $\pm 2\%$ error in their values due to fluctuations in the lasers used to measure them and fluctuations in the power meter readings. The $\pm 2\%$ is understood and suppressed for clarity.

Figure 3.2: Sender telescope on top of the CEIT building.

with screws once the telescope is coarsely aligned. Fine alignment is accomplished with a mirror mount (KS3, Thorlabs). For finer control the adjustment screws are replaced with differential adjuster micrometers (DM22, Thorlabs).

The photons are then sent over the free-space link to Alice in the BFG building. Since the free-space link is not that long (580 m), it is still possible to focus the beam to less than its original three inch diameter at the sending telescope. Thus, beam spreading is not a major problem for the experiments in this thesis. The sender telescope is adjusted so that

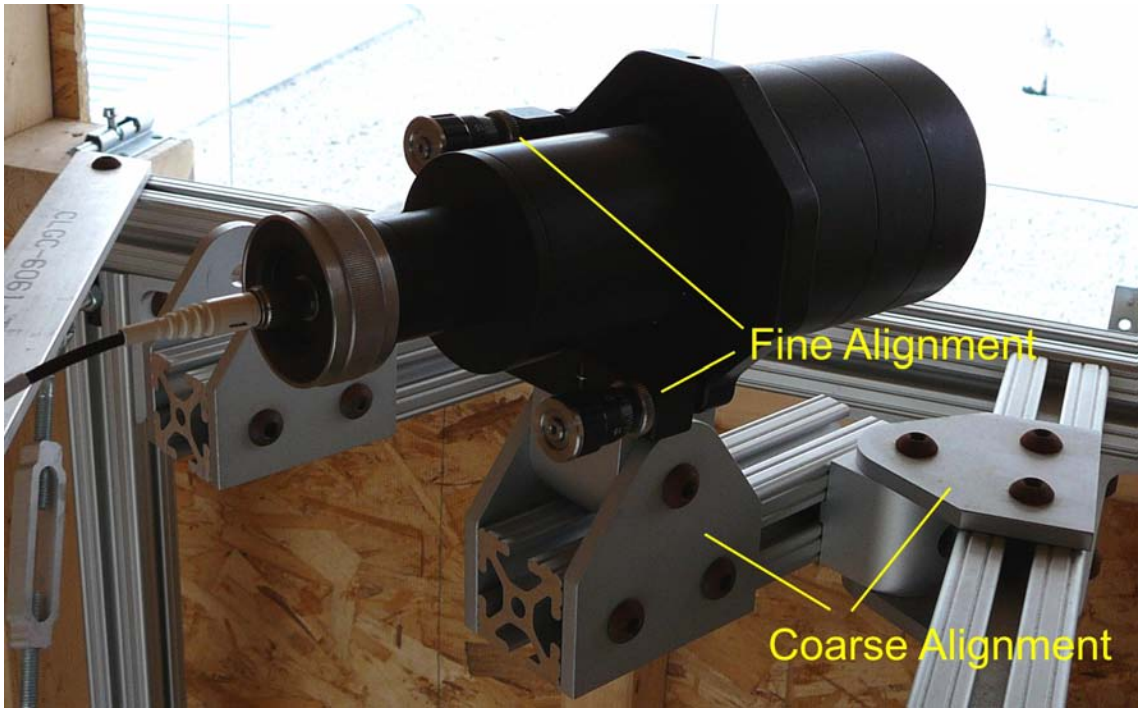

Figure 3.3: Sender telescope alignment mechanism. The coarse aligment is done with the pivot pieces, while the fine alignment is performed with the mirror mount and micrometers.

the beam diameter at the receiver telescope is the same size as at the sender telescope. However, beam wander is a problem for the experiments. Typically, the beam center wanders around its average position by 2 centimeters on the time scale of 0.1 s. This can degrade the transmission efficiency of the link if the beam wanders off the receiver lens for short periods of time causing photons to be lost. Overall, the link efficiency when measured with an 820 nm IR diode laser and a power meter is usually found to be between 5% and 7%. The total link efficiency is given by

$$\eta_{tot} = \eta_{fib} \times \eta_{sl} \times \eta_{fs} \times \eta_{win} \times \eta_{rl1} \times \eta_{rl2} \times \eta_{det} \tag{3.2}$$

where η_{fib}, η_{sl}, η_{fs}, η_{win}, η_{rl1}, η_{rl2}, and η_{det} are the transmissions of the single-mode fibre, sender telescope lens, free-space link, window, big receiver lens, small receiver lens, and

filter and detector box respectively. Working backwards from the total link efficiency by dividing out the efficiencies of the sender and receiver optics, the transmission of the free-space link plus window is estimated to be between 10.6% and 15%. The efficiency of the window in Alice's office also has to be divided out, using a transmission of 56% measured at normal incidence to a similar window. Taking this into account gives a free-space transmission efficiency between 19% and 27%.[3] In practice, the transmission of the window is probably closer to 30% or worse since it consists of 4 panes of glass and the photons are hitting it at an oblique angle.[4] The variation of the free-space link efficiency depends on the particular atmospheric conditions during an experiment.

After the photons are sent over the free-space link, they are collected with a receiver telescope which compresses and collimates the photons back into a three millimeter beam. The receiver telescope consists of an achromatic doublet lens (PAC095, 76.2 mm diameter, 250 mm focal length, Newport) to focus the beam and a small lens to collimate the photons into the three millimeter beam expected by the detection units. The transmission efficiency of these lenses was measured using the same Titanium:Sapphire laser mentioned above. The large lens was found to have an efficiency of 94% while the smaller collimation lens was found to have an efficiency of 96%. The beam of photons them passes through an interference filter (central wavelength 818.1 nm, FWHM 10.6 nm, Chesire Optical), tilted by 7° to shift the passpand center to 815 nm, which is used to suppress background light and has a transmission efficiency of 84%. The transmission characteristics of the sender and receiver telescopes are summarized in Table 3.1. At this point the photons are sent into the detection units to be measured and turned into a secret key.

[3]The η_{fs} is actually composed of a number of terms including telescope coupling, beam wander, and pure free-space link efficiency. The pure free-space link efficiency should be much better than the lumped 27% estimated here. A more accurate grouping of the efficiencies is perhaps $\eta_{tot} = \eta_{fib} \times \eta_{tc} \times \eta_{fs} \times \eta_{win} \times \eta_{det}$ where η_{tc} is now the lumped coupling efficiency of the telescope system as measured in the lab. The reason an η_{tc} is more desirable is that the coupling efficiency of the telescope system will in general be less than the individual efficiencies of the telescope elements multiplied together due to imperfect alignment. This efficiency breakdown will be measured and used in future work.

[4]These windows will soon be removed in the setup so as to improve the efficiency of the system. At that time, a much better estimate of the actual window efficiency for the experiments presented in this thesis will be possible.

The receiver telescope sitting on its mount in Alice's office in the BFG building is shown in Figure 3.4. The telescope is mounted to a custom built stand made from aluminum

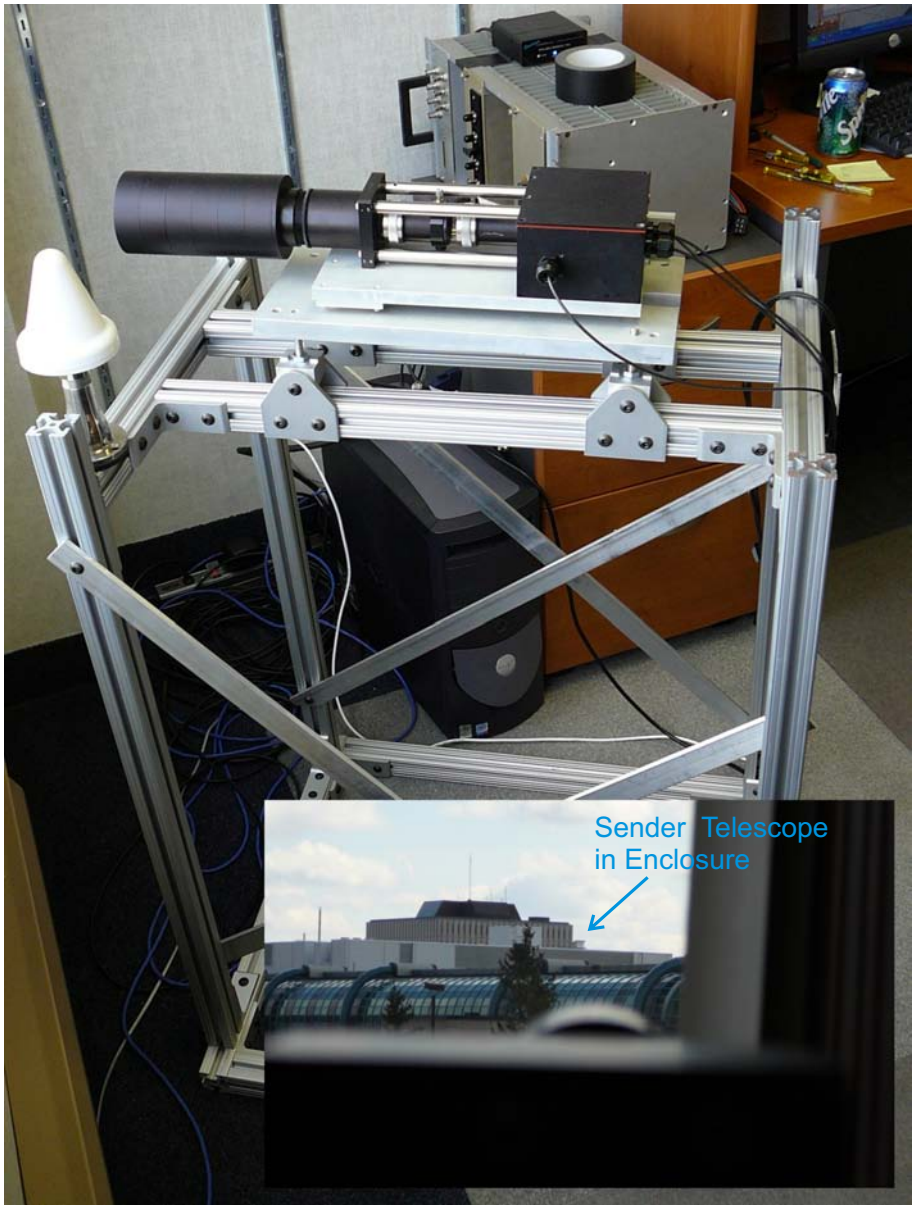

Figure 3.4: Receiver telescope sitting in Alice's office in the BFG building.

extrusion pieces from 80/20 Inc. Figure 3.5 shows the coarse and fine alignment mechanism used to align the receiver telescope with the sender telescope. The coarse vertical tilt

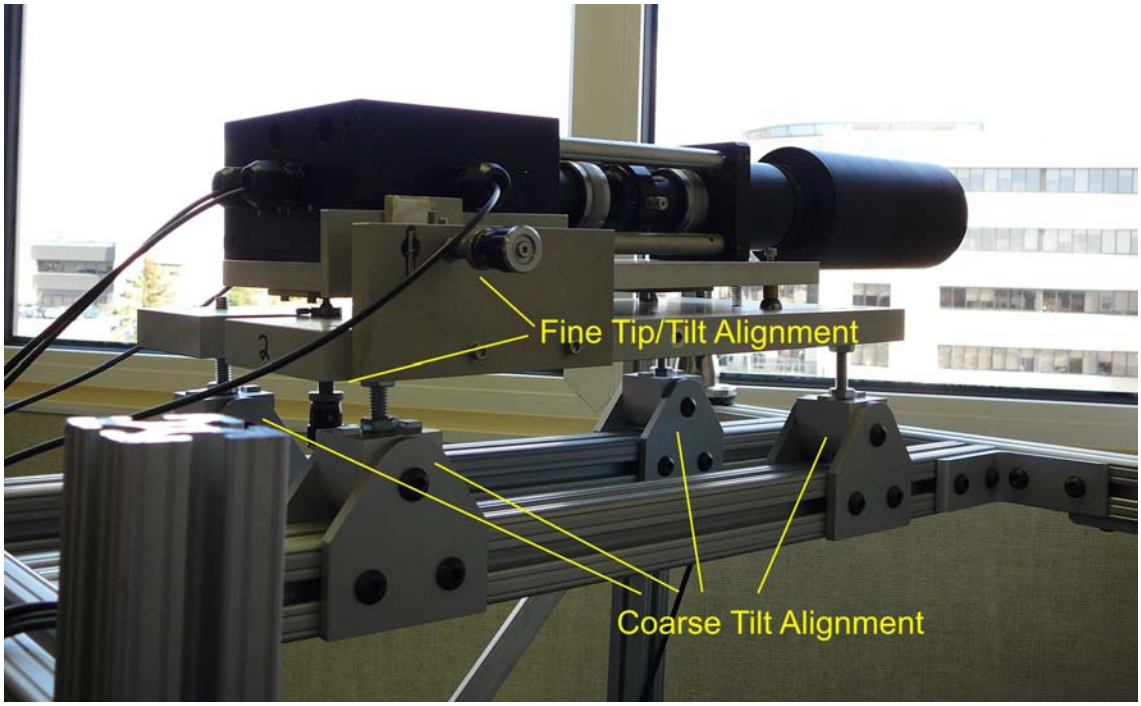

Figure 3.5: Receiver telescope alignment mechanism. The coarse vertical alignment is done with the pivot pieces and the coarse horizontal alignment is done by physically turning the stand. The fine alignment is performed with the custom tip/tilt stage sitting atop the coarse alignment pivot pieces.

alignment is done with 80/20 Inc. pivot pieces which are locked firmly in place once the receiver's vertical tilt has been coarsely aligned. The coarse horizontal tilt alignment is accomplished by physically turning the stand to align it to the sender telescope. Fine alignment is then performed with a custom tip/tilt stage that was built for the experiment. The tip/tilt stage has two micrometers (DM12, Thorlabs) which allow the fine adjustment of the vertical and horizontal angles.

Free-Space Optics Efficiencies			
Sender Optics			
Fibre 1	87.0%		
Fibre 2	86.0%		
Sender Lens 1	92.8%		
Sender Lens 2	92.4%		
Free Space Transmission			
Free Space	19% - 27%		
Window (dirty)	55.9%	Window (clean)	57.4%
Receiver Optics			
Receiver Lens 1 (big)	94.3%	Receiver Lens 1 (small)	96.0%
Receiver Lens 2 (big)	95.8%	Receiver Lens 2 (small)	96.6%
Filter 1	82.1%		
Filter 2	80.6%		

Table 3.1: Experimentally measured transmission efficiencies of the free space optics.

Chapter 4

Detection

Once entangled photon pairs have been created and sent to Alice and Bob over the free space link they need to be detected. The detection method needs to randomly choose a basis to measure in, measure the polarization, and record enough information to match each photon Alice detects with the corresponding photon Bob detects. This chapter describes the optics used to make the basis choice and polarization measurement, the detectors used to detect single photons, the timing hardware used to allow identification of entangled photon pairs, and the hardware used to transfer this information into computer memory.

4.1 Detector Modules

A compact detection module, shown schematically in Figure 4.1, was built to perform the random basis choice and polarization analysis. The photons pass first through a non-polarizing beam splitter (BS) which has an equal 50% probability of either transmitting or reflecting the photons by 90°; thus, ensuring a random measurement basis choice. In the reflected arm, the photons are projected into the H/V basis with a polarizing beam splitter (PBS) which transmits horizontally polarized photons while reflecting vertically polarized photons 90°.[1] In the transmitted arm, the photons first pass through a half-wave

[1]The H/V measurement is done in the reflected arm since the reflected beam in general experiences a phase shift between the horizontal and vertical polarizations. By doing the H/V measurement in the

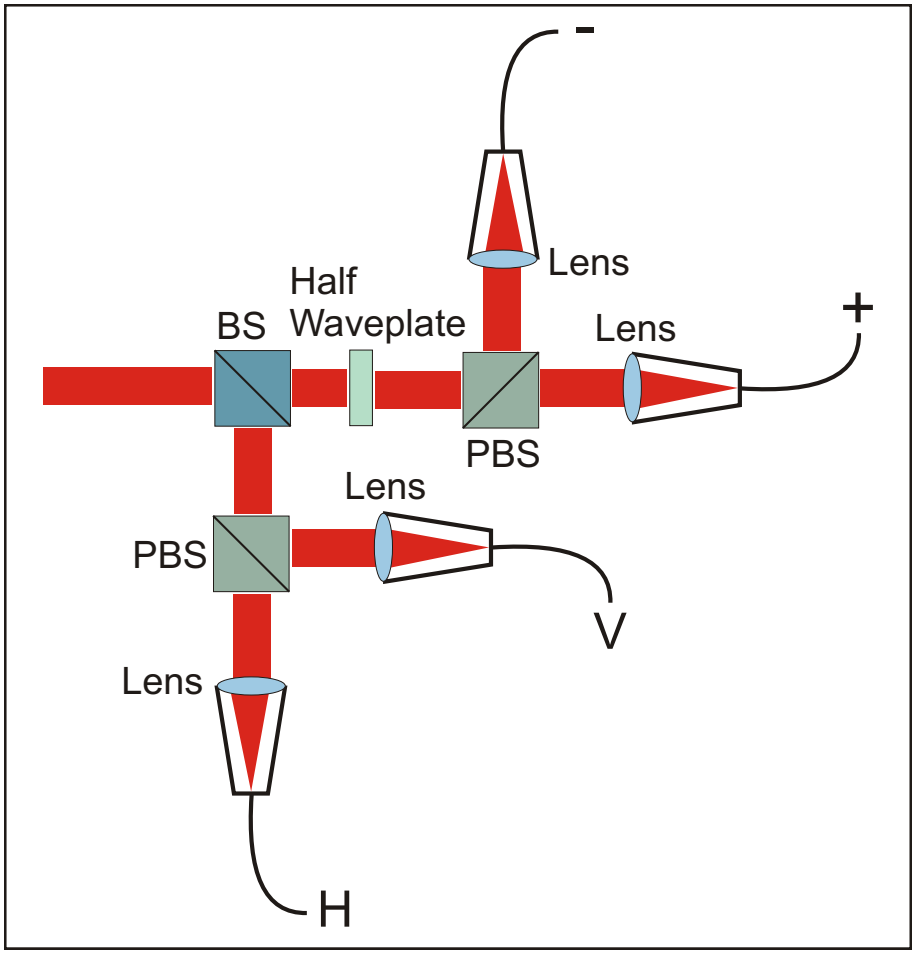

Figure 4.1: Schematic of the polarization analysis optics.

plate (HWP) angled so as to rotate the photons by 45° and then through a polarizing beam splitter. The combination of the two effectively projects the photons into the +/- basis, with the +45° photons transmitted and the −45° photons reflected by 90°. Finally, the photons are collimated into multimode fibre optic cables and transported to the single photon detectors.

reflected arm, this phase shift does not affect detection; whereas, it would alter the detection in the +/- basis.[28]

The detector boxes built for the experiments in this thesis can be seen in Figure 4.2. The

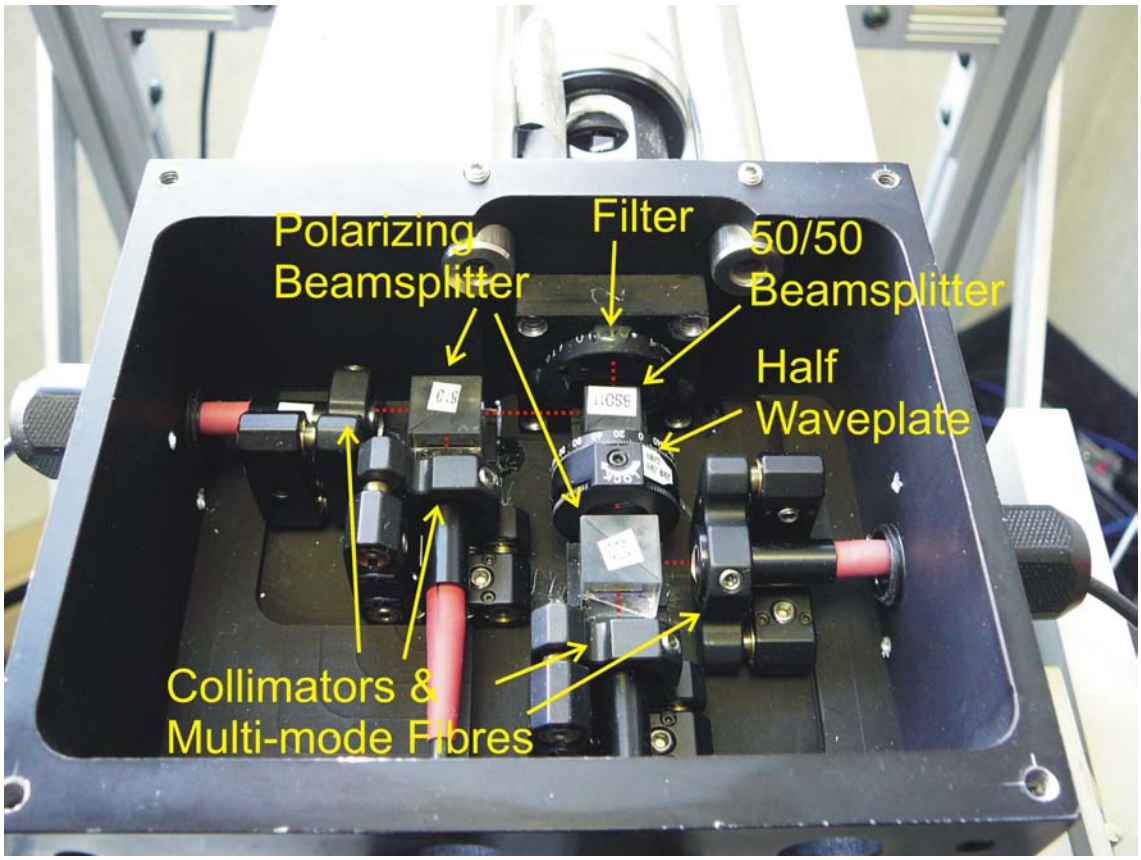

Figure 4.2: Detailed picture of the detector box.

efficiencies of the detector boxes were experimentally measured using a Titanium:Sapphire laser tuned to a wavelength of 815 nm. The laser's optical power was measured before and after entering the filter or the filter plus detector box. The detection efficiency of Detector Box 1 with Filter 1 is $\sim 64.20\%$ and the detection efficiency of Detector Box 2 with Filter 2 is $\sim 60.28\%$, as shown in Table 4.1.

Efficiencies	
Filter 1	82.05%
Filter 2	80.56%
Detector Box 1 + Filter 1	64.20%
Detector Box 2 + Filter 2	60.28%

Table 4.1: Experimentally measured transmission efficiencies of the detector boxes.

4.2 Single Photon Detectors

Once a photon is directed into one of four different fibres depending on its polarization in the detector modules, it still needs to actually be detected and turned into an electronic signal which a computer can process. The photons exit the detector boxes coupled into four multi-mode fibres which are connected to single photon detectors. The single photon detectors used are four channel SPCM-AQ4C modules made by PerkinElmer; inside are silicon avalanche photo-diodes operated in geiger counter mode. These are pn photo-diodes operated with a reverse bias voltage in excess of their breakdown voltage; when a photon strikes the diode, an electron-hole pair is created, which induces a charge avalanche that is electronically transformed into a 25 ns wide TTL pulse output from the detectors [28]. These detectors have an efficiency of $\sim 45\%$ at a wavelength of 830 nm, and a dead time of about 50 ns after each detection, as the avalanche must be quenched and the detector reset. The detectors also have a dark count rate[2] of ~ 500 cps since they are heavily reversed biased so that the thermal excitation of any impurities can cause a charge avalanche and false detection [1].

[2]The dark count rate is defined as the number of false detection events generated by the detectors when their optical inputs are blocked and thus no events should be seen.

4.3 Time Stamping

After the photons have been detected and transformed into an electronic signal, additional timing information needs to be saved so that Alice and Bob can identify entangled photon pairs in their incoming stream of photons. To do so, the TTL signal is fed into a six channel time stamping unit developed by Dotfast Inc [21], which has a resolution of 156.25 ps. The time stamper requires an accurate and stable 10 MHz clock signal which it uses to produce the highly accurate timing information. Each TTL signal is stamped with a detection time and input channel (which contains the polarization measurement information) and saved to on-board memory. A National Instruments PCI-6533 digital IO card is then used to transfer the measurements from the time stamping units to computer memory so that it can be processed with the QKD software.

4.4 GPS Receiver and Quartz Oscillator

In order for the time stamping units to produce accurate timing information, they require a highly stable and accurate 10 MHz clock signal as input. This signal is provided by a Spectrum Instruments' Intelligent Reference/TM-4 GPS receiver which provides disciplined precise timing, synchronization, and frequency referencing. It contains a high performance Oven Controlled Crystal Oscillator (OCXO) which provides Rubidium-like stability even in periods of GPS unavailability using Intelligent Holdover technology. It provides a 10 MHz clock signal with a long-term stability of 1×10^{-12} (over twenty-four hours of tracking), and a short-term stability of 1×10^{-11} (over an interval of one second). The GPS units also provide a 1 pulse-per-second (PPS) output which is fed to the sixth channel of the time stamping unit to provide the QKD software with additional information to maintain its signal lock. The 1PPS signal has an accuracy of 25 ns RMS (referenced to UTC).

Chapter 5

Software

After the detection units have measured the polarization of the incoming entangled photon-pairs and converted this information, along with timing data, into digital format computer software is needed to process this data. There are a number of applications that were developed in C# for the system outlined in this thesis: a channel rates utility designed to show a real-time 4x4 coincidence matrix of the incoming photons, a Bell inequality application designed to calculate the Bell parameter in real-time, and a QKD application designed to perform the BBM92 protocol to generate secure keys which can be used to encrypt and decrypt data. The Bell inequality and QKD applications also provided the option to save the data and statistics generated for further analysis. This chapter outlines the development of these software applications.

5.1 General Outline of the Software

There are a number of different software applications one would like to have available to be used with the QKD system described in this thesis. First, in order to correct for the random polarization rotation induced by the single mode fibres connecting the source to Alice and Bob, a real-time application displaying Alice's and Bob's single count rates (for H, V, +, and - measurements) and coincident measurement correlation matrix is required. This application is also needed to determine what angle to tilt one of the compensator

crystals at in order to produce the $|\psi^-\rangle$ state. Second, since the QKD system described in this thesis actually distributes entangled photon pairs, it can be used to check Bell inequality violations as described in Section 1.1.3.[1] Last, an application to perform the BBM92 protocol of Section 1.2.4 is needed to actually generate secure secret keys between Alice and Bob.

The software is a multi-threaded program, which performs a number of operations simultaneously. Since all three applications rely on a lot of the same underlying routines, they were created as sub-applications that could be opened to analyze the measurement data in a larger main program. All three sub-applications use a measurement thread to continuously measure the stream of incoming photons, and a coincidence thread to extract coincident measurement events corresponding to entangled photon pairs being detected. The QKD sub-application also employs a key generation thread to perform the BBM92 protocol continuously on the measurement data being generated. The shared routines are described here, while the specific sub-applications are described in the following sections.

5.1.1 Computer Clock Synchronization

Before starting the program, Alice's and Bob's computer clocks have to be synchronized to within a few hundred milliseconds ($\sim$ 300 ms). For this, a small TCP/IP NIST application is used to synchronize the computer clocks with the NIST time servers [2]. The software expects that Alice's and Bob's photon measurements will start within the same second (*i.e.* between say 12:00:45 and 12:00:46). After that, the software program then uses the 1PPS signal from the GPS receiver to calculate the offset between their start times and compensate for it in the timing measurements. Eventually, it is planned to use the GPS receiver to synchronize the computer clocks.

[1] Conversely, the Bell Inequality application can be used to verify that polarization-entangled photon pairs are in fact being distributed to Alice and Bob.

5.1.2 Communication Connection

When the program is first started, a standard TCP/IP connection is established between Alice's and Bob's computers over the internet to allow them to communicate classically. This is needed for: the Channel Rates utility to calculate the coincident measurement correlation matrix; the Bell inequality application to calculate the Bell parameter; and for the QKD application to sift the measurement data, estimate the bit error rate, perform error correction and privacy amplification, and send encrypted data between Alice and Bob.

5.1.3 Measurement Algorithm

Once a communication connection has been established, the measurement thread is called from one of the sub-applications. It waits until both Alice and Bob have chosen to start measuring their incoming photons, and then synchronizes the start of these measurements using the 1PPS signal from the GPS receiver. It accumulates data in one second data packets until the next 1PPS signal is received before passing the whole data packet along to the coincidence algorithm. This reduces the problem experienced by other experiments where the timing information slowly became invalid over the course of the experiment because the clocks (typically Rubidium clocks) slowly drifted off one another. In the case of the system described in this thesis, this would mean the 10 MHz signals sent to Alice's and Bob's time stamping units slowly drifted off one another, because their frequencies were not exactly 10 MHz, causing the timing information from the time stampers to slowly become erroneous. The measurement algorithm reduces this problem by saving the time of each 1PPS pulse and including it with each data packet so that each packet can be referenced to the 1PPS signal. This means that the 10 MHz clock only has to be accurate over the course of the second when the data is measured for the software to maintain a lock on the coincident events. In theory, this means that the software should be able to maintain a lock indefinitely.[2]

[2]Sunlight saturating the detectors might prevent a maintainable lock during the day, since the accidental coincidence rate can become quite high. Future versions of the system will include spatial filtering and

5.1.4 Coincidence Algorithm

Once incoming photons have been detected and measured, the time-tag data is passed along to the coincidence thread responsible for identifying the entangled photon-pair detection events among the continuous streams of photons that Alice and Bob receive. A coincidence algorithm was necessary because both Alice and Bob see a background rate of photon detections from both of their detectors even without the source turned on. Also, as was discussed in Section 2.2, while the source produces singles rates of about 120,000 cps, the local coincident entangled pair rate was only about 18,000 cps. In other words, Alice registers a lot of detection events for one half of a photon pair which Bob fails to detect and vice versa. Lastly, the software also needs to compensate for the optical path length difference for photons travelling to Alice and photons travelling to Bob. There is an overall large fixed offset the software has to compensate for as well as small random fluctuations due to evolving atmospheric disturbances which the photons experience as they cross the free-space link.

The coincidence algorithm is responsible for finding the time offset between Alice's and Bob's time-tags. Once this offset is found the coincidence algorithm can then sift the data down to only coincident events using a coincidence window. There were two coincidence algorithms developed to identify entangled photon pairs. The first algorithm was based on shifting the time-tag lists of photon events from Alice and Bob relative to one another until a maximum coincidence rate was found. The second was based on calculating a histogram for different time shifts to identify the shift that produced the maximum coincidence rate. For both methods, Alice transmits her time-tag data to Bob publically over the internet. The coincidence algorithm then uses Alice's and Bob's lists of time-tags to find the coincident events which correspond to entangled photon pairs. Both methods are detailed in the following sections.

---

more refined spectral filtering to allow the operation of the system during the day.

Shifting Coincidence Algorithm

The basic idea behind the shifting algorithm is that when Alice and Bob each measure a photon from an entangled photon pair, they will do so simultaneously since the photons were created at the same time. Thus, coincident events should indicate the detection of an entangled photon pair. This is an effective entangled pair discrimination mechanism since the accidental coincidence rate is only about 7 coincidences per second[3], which is much lower then the real coincidence rates experimentally measured in Section 6.2. The accidental coincidence rate can be calculated from

$$C_{accidental} = C_{Alice} \times C_{Bob} \times \Delta t_{cw} \tag{5.1}$$

where $C_{accidental}$ is the accidental coincidence rate (in cps), C_{Alice} and C_{Bob} are Alice's and Bob's single photon rates (in cps), and Δt_{cw} is the coincidence window.

The shifting coincidence algorithm begins by first coarsely correcting for the optical path length difference between Alice and Bob.[4] The coarse optical path length difference is about 1.933 μs according to the following equation

$$\Delta t = \frac{580 \text{ m}}{3 \times 10^9 \text{ m/s}} = 1.933 \ \mu\text{s}. \tag{5.2}$$

It then runs through Alice's and Bob's time-tag lists, recording an entangled photon pair registration every time a detection event occurs for both Alice and Bob within a certain coincidence window, typically 10 ns. It then fine tunes this offset by looping through this procedure multiple times with different small offsets added to Alice's time-tags each time. Typically, it tries offsets ranging from -100 ns to 100 ns in step sizes of 10 ns, but this range can be set by the user. By trying different offsets between the two time-tag lists and keeping track of the number of coincident events found for each offset, it can search for the offset which maximizes the coincidence rate. Once this offset found, it is used to correct Alice's time-tags and sift the data down to coincident detection events corresponding to entangled photon pair detections.

[3]This is calculated with the experimental data from Section 6.1 with $C_{Alice} = 7800$ cps, $C_{Bob} = 85,000$ cps, and $\Delta t_{coinwindow} = 10$ ns.

[4]Since they won't actually register photons simultaneously because it takes longer for the photon to travel over the 580 m free space link to Alice's detector then for it to travel to Bob's detector.

Histogram Coincidence Algorithm

The histogram coincidence algorithm relies on the same basic idea as the shifting algorithm: coincident events indicate detected entangled-photon pairs. The histogram algorithm corrects for the optical path length difference between Alice and Bob. After that the histogram algorithm calculates a histogram of different small offsets. Once the histogram has been generated, it finds the maximum value of coincident events in the histogram and the corresponding offset. The coincidence window used in the histogram can be dynamically changed from one data package to the next to optimize its size. Once the offset has been found, it is used just as in the shifting algorithm to sift the data down to only entangled photon pair measurements. The histogram algorithm is the algorithm used for the experiments described in this thesis.

5.2 Channel Rates Utility

When the Channel Rates Utility is used, the coincidence algorithm first determines the offset which maximizes the coincidence rate on a data block. Alice's time-tag data is then corrected using this offset. Next, the coincidence algorithm runs through both Alice's and Bob's time-tag lists identifying detection events which occurred within the coincidence window. Every time corresponding events are found for Alice and Bob, their indices in the time-tag lists are saved to two lists. Since this application is just used to help align the system and no key is generated from it, the measurement results for each data block are also sent from Alice to Bob at the same time she sends her time-tag data. With the two lists, the coincidence algorithm then sifts Alice's and Bob's measurement data down to only those measurements where the photons were detected by Alice and Bob within the coincidence window. The coincidence algorithm then goes through Alice's and Bob's measurement results to create a correlation matrix from their measurements. This shows the number of times each particular measurement combination occurred within a block of data. The total number of coincidences is also calculated along with the visiblities in both bases. All of this information is then passed back to the main Channel Rates Utility and displayed to the user.

The Channel Rates Utility can be seen in Figure 5.1 updating its statistics every second. The singles count rates appear along the left hand side of the screen, while the correlation

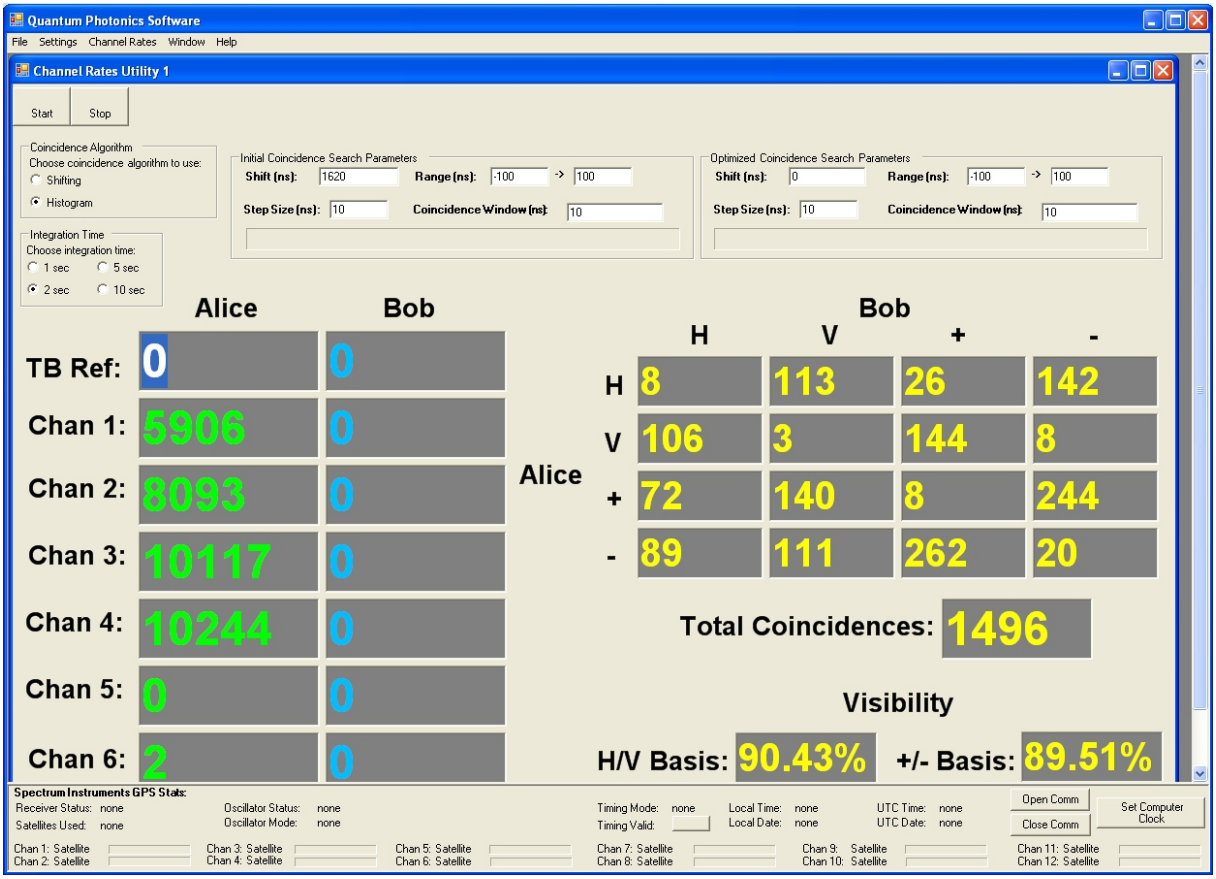

Figure 5.1: Screen shot of the Channel Rates Utility.

matrix is on the right. The total number of coincidences is also displayed along with the visibilities in both bases at the bottom of the screen. When compensating for the random polarization rotation induced by the fibres, a polarizer is put into each arm of the source to only allow vertically polarized photons through. The singles count rate for the corresponding channel for detecting vertically polarized photons is then maximized while minimizing the singles count for the horizontally polarized photons by adjusting the polarization controllers. Once the random rotation is corrected, the polarizers are removed

and a strong anti-correlation in the upper left quadrant of the correlation matrix (the correlations in the H/V basis) should be observed. The correlation matrix is then used to adjust the tilt of one of the compensator crystals to produce the $|\psi^-\rangle$ state. This is done by slowly varying the tilt of the crystal while watching the bottom right quadrant of the correlation matrix which becomes maximally anti-correlated when the crystal is tilted at the proper angle to produce the $|\psi^-\rangle$ state. There should not be any correlations between measurements that were done in different bases, so the rates in the upper right and lower left quadrants should be random and evenly distributed.[5] Strong anti-correlations observed in the H/V and +/- bases are evidence that the system is aligned correctly and that Alice and Bob and measuring entangled photon pairs.

5.3 Bell Inequality Application

The Bell Inequality application works very similarly to the Channel Rates Utility. There is one optics difference, a half wave-plate is inserted before Bob's detector module in order to rotate his photons by 22.5°. This causes Bob to measure in the 22.5°/112.5° and 67.5°/157.5° bases and should allow Alice and Bob to measure a maximally violated Bell parameter close to $2\sqrt{2}$. When the Bell Inequality application is being run, the coincidence utility again sifts Alice's and Bob's measurement data down to only entangled photon events, calculates the singles rates, and sends this information back to the main Bell Inequality application to display to the user. Also, following the procedure in Section 1.1.3, the Bell Inequality application uses Alice's and Bob's measurement data to calculate the correlation matrix (for the angles $\{0°, 90°, 45°, 135°\}$ and $\{22.5°, 112.5°, 67.5°, 137.5°\}$), the four expected values, and finally the Bell parameter. These results also displayed to the user.

A screen shot of the Bell Inequality application is shown in Figure 6.3. Again, the singles count rates appear along the left hand side of the screen, while the correlation

[5]Unfortunately, a strong correlation in the upper right quadrant of the coincident matrix is clearly visible. We are currently in the process of identifying the error in the system, for more comments on this see Section 6.4.

matrix is on the right. The total number of coincidences is also displayed at the bottom of the screen along with the four expected values and the Bell parameter. All of these numbers are updated every second. The user also has the option to choose to save the correlation matrix, expectation values, and Bell parameter to memory for further analysis later. For instance, the Bell parameter can be tracked to see whether its value changes appreciably over the duration of the experiment.

5.4 QKD Application

The QKD application requires a number of other algorithms not present in the Channel Rates utility or Bell Inequality application, in order to perform the BBM92 protocol. A screen shot of the QKD application is shown in Figure 6.5. The singles rates are again displayed to the user along the left side of the screen. The rest of the elements on the screen are generated from the algorithms described in the following sections. The user also has the option to choose to save the singles rates, the raw key and the raw key length, the quantum bit error rate (QBER), the error corrected key and the error corrected key length, and the final privacy amplified key and its length to memory for further analysis later. For instance, as before the key rate can be graphed and tracked over the course of an experiment to see how its value changes with time.

5.4.1 Basis Reconciliation and Sifting

The QKD application begins by using the coincidence algorithm to identify entangled photon pair measurements. It also receives Alice's and Bob's measurement basis choices for each measurement and sifts the data down to only those coincident events where Alice and Bob measured in the same basis.[6] At the end of the coincidence algorithm, Alice and Bob each get an index list which identifies entangled photon pair events measured in identical bases in their measurement data. Alice's and Bob's programs then use these

[6] Alice and Bob are only revealing their measurement basis, which does not leak any information about the key bits to Eve, since that is contained in their measurement results only.

index lists to locally extract the measurement results sitting in their original lists that can be used to form a secure key. After this sifting, Alice and Bob should each be left with a list of measurement results due only to entangled photon pairs which were measured in the same basis. In other words, they should have two lists of measurement results which are completely anti-correlated.

5.4.2 Quantum Bit Error Rate Estimation

After the measurement results have been sifted down to only those that were produced from an entangled photon pair measured in the same basis, the measurement data is passed along to the key generation thread responsible for performing the BBM92 key generation protocol. First, the measurement results are converted into a string of bits by $\{H, +\} \mapsto 0$ and $\{V, -\} \mapsto 1$, and Bob inverts his string of bits. Alice and Bob should now share an identical, random, bit string referred to as the raw key. The most important part of the QKD protocol is then performed — namely, the security of the entangled photon pairs measured by Alice and Bob is verified. The quantum bit error rate (QBER) must be accurately estimated to make sure that it is below the acceptable threshold of 14.6% as detailed in Section 1.2.5. To do so, the software randomly chooses a subset of the raw key, usually around 10% of the raw key. The bit values of this subset are then publically disclosed allowing Alice and Bob estimate the bit error rate in the measurements. This random subset must then be removed from the raw key, since the bit values have been publically disclosed. [7] If the bit error rate is found to be less then the acceptable threshold, the the software can move to generating a secure key. However if the bit error is too high, it must be attributed to the presence of an eavesdropper and the data must be discarded and the protocol started again. If the bit error rate continues to be too high, then the source of the errors must be found and eliminated.

[7] The measurement results used to calculate the QBER can instead be used to populate a correlation matrix and approximate the visibilities of the entangled photons.

5.4.3 Error Correction

In a practical quantum key distribution system, Alice and Bob will always find some non-zero error rate due to slight imperfections in the system (imperfect alignment of some optics, non-ideal polarizing beam splitters, etc). Due to this, the keys which they generate will not be perfectly correlated and will have some errors in them. Error correction is the process of correcting errors between Alice's and Bob's version of the key. This is done by public discussion, which can leak some information about the key to any eavesdropper listening in. The experiments in this thesis use the Cascade algorithm, developed by G. Brassard and L. Salvail in 1994 [16], to perform error correction. This is an efficient protocol that leaks an amount of information acceptably close to the minimum possible for sufficiently reliable secret channels. The BINARY primitive used in the Cascade algorithm is described below, followed by the actual Cascade algorithm.

BINARY

The BINARY algorithm is able to find an error between Alice's and Bob's bit strings represented by A and B, in the case where A and B have an odd number of errors. It performs an interactive binary search to find an error by exchanging fewer than $\lceil \log n \rceil$ bits over the public channel. It works in the following manner:

1. Alice sends Bob the parity of the first half of her bit string A
2. Bob determines whether an odd number of errors occurred in the first or second half by testing the parity of the first half of his bit string B and comparing it to the parity sent by Alice
3. This process is repeatedly applied to the half determined in step 2, until an error is eventually found

Cascade

The Cascade algorithm uses the BINARY primitive to correct all of the errors between Alice and Bob's raw keys with a high probability. It performs a number of passes through

the keys in order to correct the errors. The number of passes was chosen to be four for the error correction algorithm by interpolating the Cascade benchmark data in Table 1 of Brassard and Salvail's original paper [16].

In pass 1, Alice and Bob choose k_1 and break their raw key up into blocks of k_1 bits. Alice then computes the parities of her blocks and sends them to Bob. Bob uses the BINARY primitive described above to correct an error in each block where the parity of his block differs from the parity of Alice's corresponding block. At this point, all of Alice's and Bob's blocks have an even number of errors in them (possibly zero). Other protocols usually then remove one bit from each block since the publically communicated parities essentially revealed one bit from each block to an eavesdropper. Instead, all the bits are kept which allows more errors to be corrected for a certain number of passes. The information leakage is then dealt with by the privacy amplification protocol of Section 5.4.4.

For each subsequent pass $i > 1$, Alice and Bob choose a new block size k_i and a random function $f_i : [1..n] \rightarrow [1..\frac{n}{k_i}]$ which is used to randomly break their raw key up into new blocks of size k_i. Alice again computes her parities, sends them to Bob, and Bob uses BINARY to correct any errors where the parities differ. If any errors are found, this means that there must have been two errors in an earlier step (an even number of errors). Since one of them has now been corrected, going back to a previous step will now find an error (since there is now an odd number of errors in the key). In the actual Cascade algorithm, it goes iteratively back through all previous passes. Instead, the error correction algorithm here only goes back to the first pass to find the error, since the software only uses four passes. Having interpolated the number of passes to use from the Cascade benchmark data in [16], Alice's and Bob's keys should now be identical with a very high probability.

5.4.4 Privacy Amplification

The information that was leaked during error correction along with any information the eavesdropper might have gained from interacting with some of the photon pairs now has to be eliminated using a privacy amplification protocol at the cost of reducing the secret key size. For this purpose, the software uses a universal hash function developed by J.L.

Carter and M.N. Wegman in 1979 [11] on the error corrected key. This shortens the key by approximately the number of bits that were revealed during the error correction procedure; however, any information about the key which an eavesdropper had should now have been reduced to an exponentially small amount.

5.4.5 Encryption/Decryption

Once Alice and Bob have validated the security of their key by calculating the QBER, corrected any errors in their key, and performed privacy amplification to eliminate any information an eavesdropper might have gained about the key, they now have a secure key which they can use to send data securely between themselves. At the bottom of Figure 6.5 there is space for either Alice or Bob to type in a message to send. In this case Alice types in a messages and clicks on the encrypt/decrypt button causing the message to be encrypted using the XOR operation of Section 1.2.2 and her key. The encrypted message can be seen by Alice below her original unencrypted message. The encrypted message is then sent publically over the internet to Bob. Bob can also see the encrypted message that Alice sent. He then uses his secret key and performs the inverse encryption operation, in this case the XOR operation[8], to decrypt the message. Bob can then see the decrypted message below the original encrypted message which Alice sent. Functionality to encrypt and decrypt images can also be seen in Figure 6.5.

[8]The XOR operation is its own inverse, as shown in Section 1.2.2

Chapter 6

Experimental Results

The main goal of this Masters thesis has been to develop a complete, working, system for Quantum Key Distribution. Chapters 1 to 5 focused on the development of the components needed for the system. Once the system was finished a number of experiments were performed to test its operation. All of the experiments were performed during the night when background light was minimized.

6.1 Link Efficiency

The total link efficiency was estimated from Alice's single photon count rates. Figure 6.1 shows Alice's singles rates when the entangled photon pairs are blocked from entering the single-mode optical fibre which takes them to the sender telescope. Figure 6.2 shows Alice's singles rates when the source is unblocked. Both figures show the statistics for two seconds of data collection. The non-zero single photon count rates when the source is blocked are due to background light and the dark count rates of the photon detectors. The sum of the dark count rates for the four photon channels was measured to be 2500 cps, leaving a background photon count rate of $5,482$ cps. For this particular two second interval, Alice received 8556 photons per second from the source. Locally, the source emits about $120,000$ photons per second. This means that during this experiment the total link efficiency from the source to the detector modules was $\sim 7.1\%$.

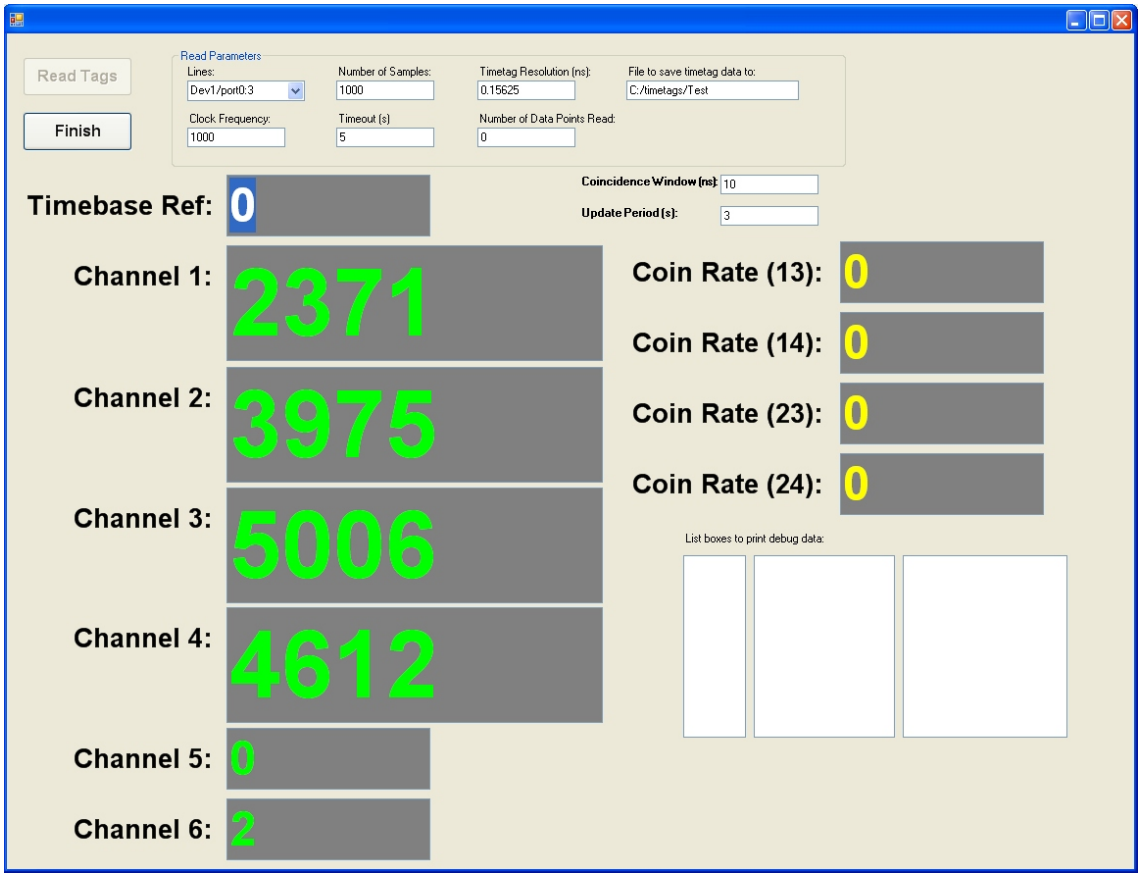

Figure 6.1: Alice's singles rates when the source is blocked.

6.2 Bell Inequality Violation

When the parametric down-conversion source was originally set up, a Bell inequality experiment was performed to verify that the source was indeed producing entangled photon pairs. Table 6.1 summarizes the data taken for this experiment. The data for each entry was generated over the course of one second. Using Equation 1.5 the Bell parameter S is calculated to be 2.74 ± 0.0091, which corresponds to a violation of the CHSH inequality by more then 81 standard deviations assuming Poissonian errors. The source was measured to have a visibility of 98% in the H/V basis and 90% in the +/- basis at the start of this

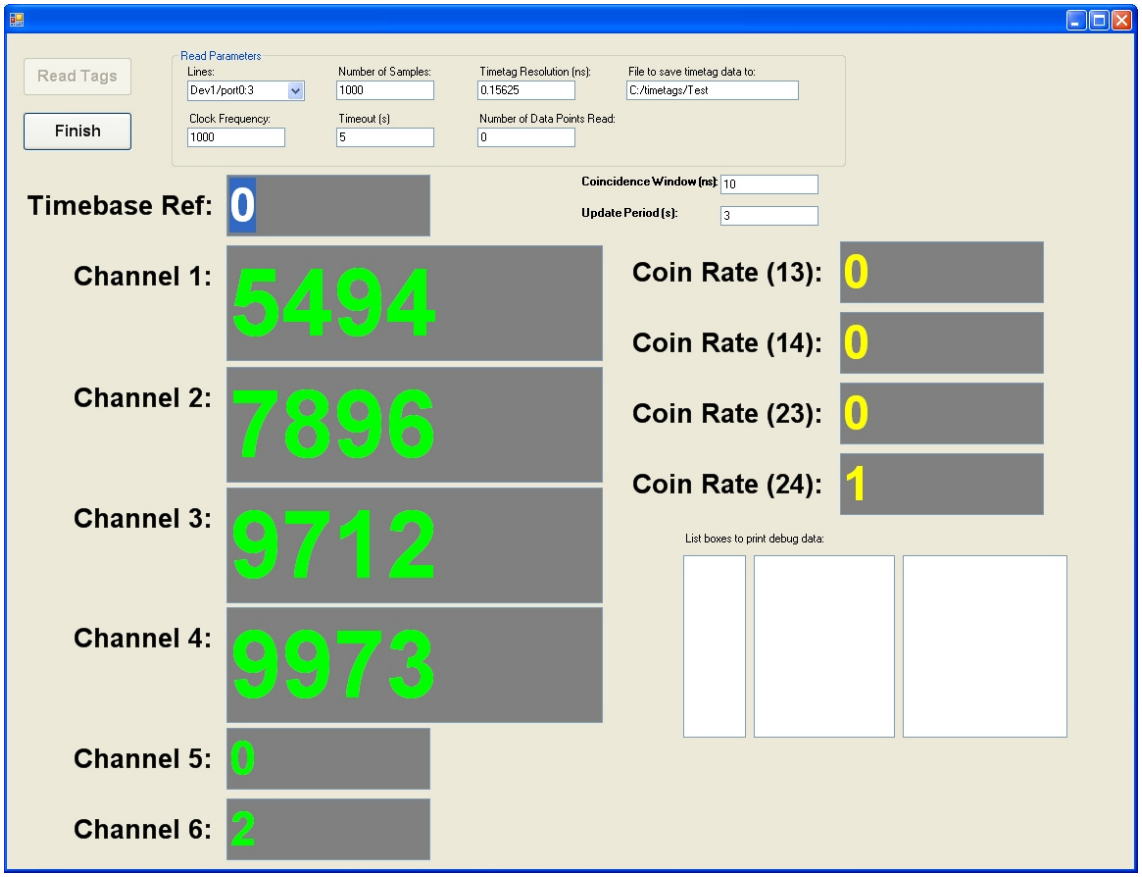

Figure 6.2: Alice's singles rates when the source is unblocked.

experiment.

After a working (non-zero) link efficiency has been measured the distribution of entangled photon pairs has to be verified. Figure 6.3 shows the measurement results for two seconds worth of data during a particular experimental run. A singles rate of 5876 cps with a coincidence rate of 390 cps and a background rate of 7982 cps was observed on Alice's side during this experiment. The local visibility of the source at the start of this experiment was measured to be 97% in the H/V basis and 90% in the +/- basis. The coincidence matrix used to calculate the four expectation values in Equation 1.5 can be seen on the right. The four expectation values and the calculated Bell parameter can be seen below

	++	- -	+-	-+
(0,22.5)	5284	1673	35612	30105
(0,67.5)	32365	28829	6276	5691
(45,22.5)	6816	8430	28830	27491
(45,67.5)	6317	4739	28793	30331

Table 6.1: Coincidences used to calculate a Bell inequality for the source after it was first setup.

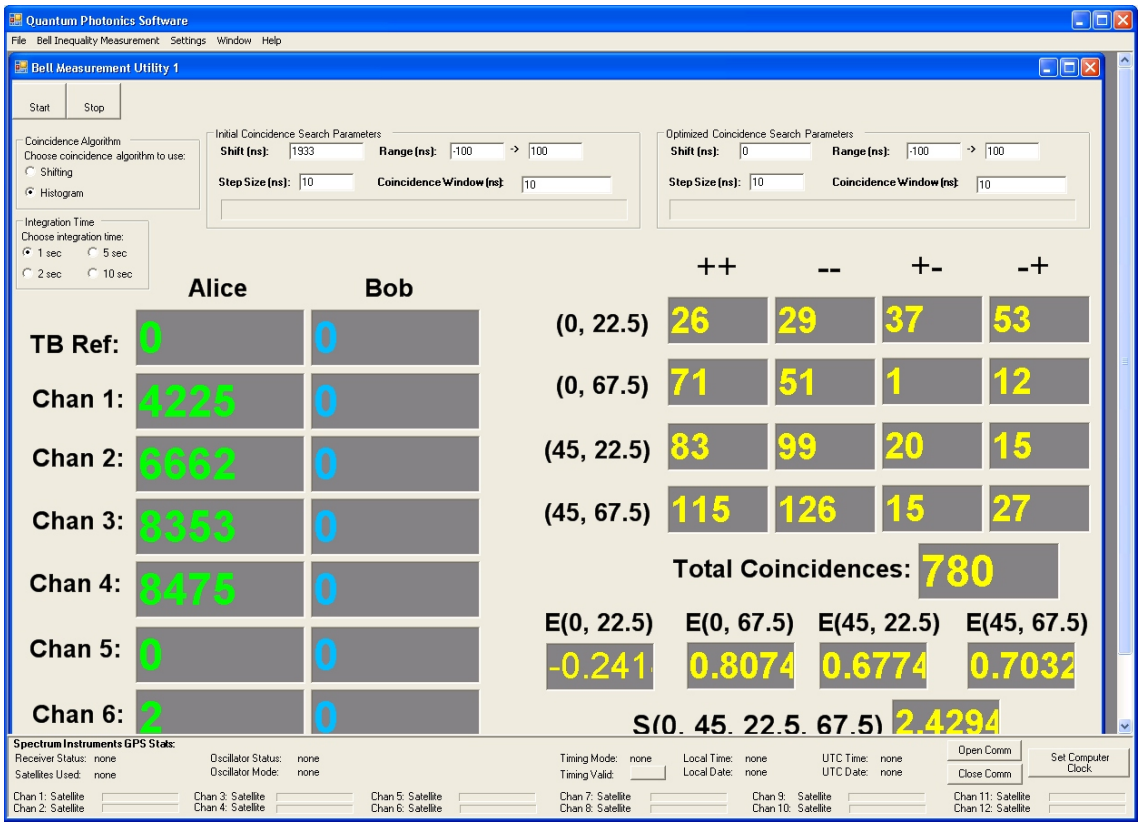

Figure 6.3: Screen shot of the Bell Inequality Application

that. For this measurement data, the Bell parameter is calculated to be $S = 2.43 \pm 0.18$ which is violation of more then 2 standard deviations. This verifies that entangled photons are being distributed over the free-space link.

The ability to save the Bell experimental data over the course of an experiment was also used to track the Bell parameter over time. Figure 6.4 shows a graph of the Bell parameter over the course of two minutes. It shows that the Bell parameter fluctuates around the

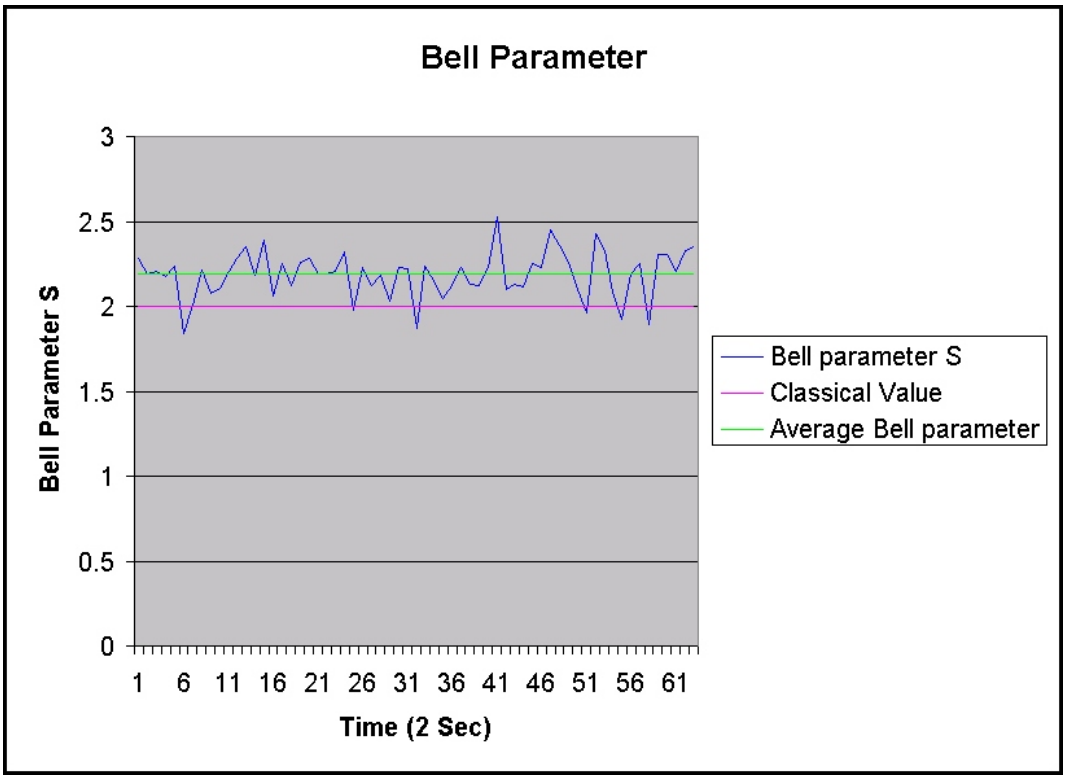

Figure 6.4: The Bell parameter tracked over the course of a long experiment.

average value of $S = 2.19 \pm 0.017$ which is well over the classical value of 2. The rather large fluctuation in the Bell parameter over time was not expected and is currently under investigation, see Section 6.4 for more comments. This shows that the QKD system is indeed distributing entangled photon pairs over the course of an experiment.

6.3 QKD

Finally, a QKD experiment was performed to test the key generation of the system. The experiment was first used to test whether the system could generate a secure key and send an encrypted message from Alice to Bob. During this experiment a singles rate of 8741 cps and a background rate of 7982 cps was seen by Alice, and a singles rate of 76175 cps and a background rate of 2500 cps was seen by Bob with a coincidence rate of 811 cps seen by both of them. The local visibility of the source was measured to be 97% in the H/V basis and 90% in the +/- basis. Figure 6.5 shows a screen shot of Alice's QKD application. A key

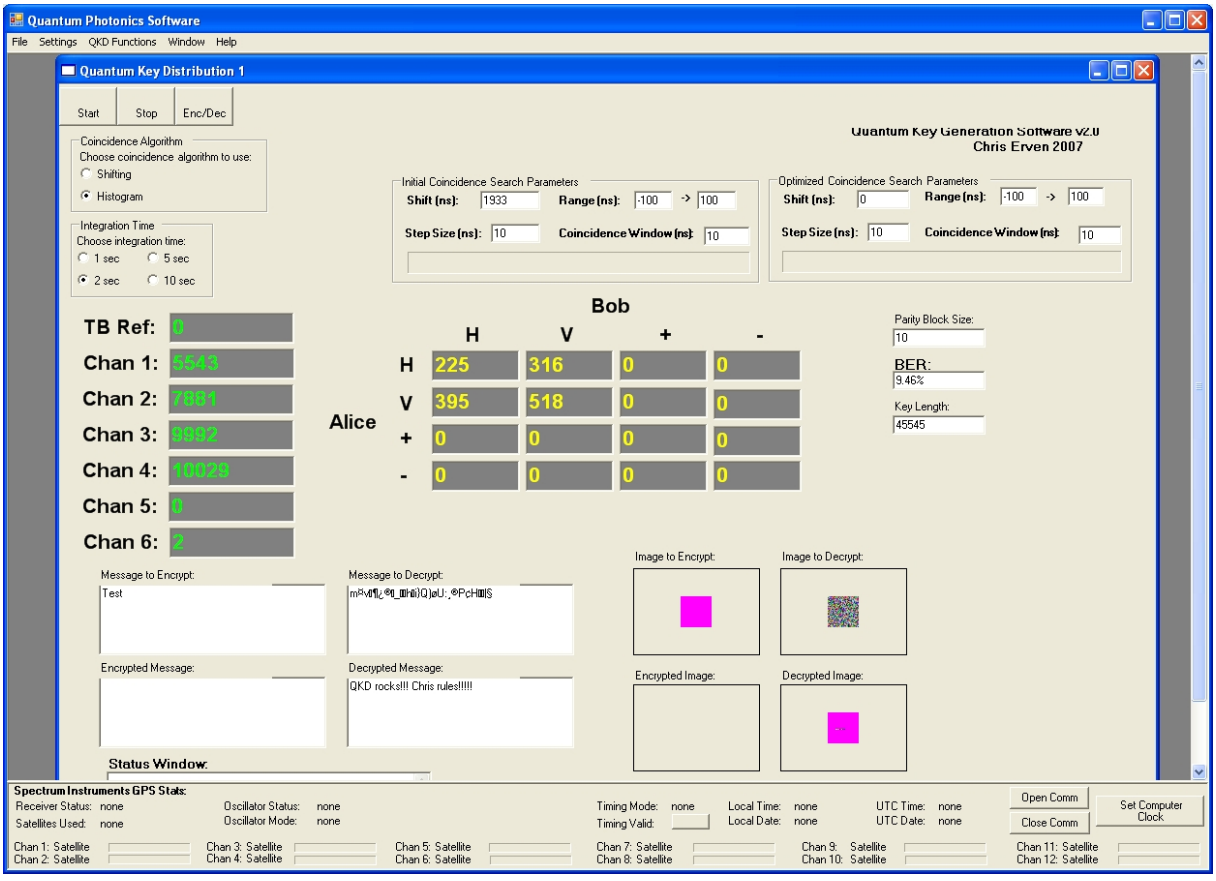

Figure 6.5: Screen shot of the Alice's QKD application for the QKD experiment.

was generated from measurement data collected over three minutes and twenty seconds. The size of the raw key generated from the data was 75478 bits. The QBER was estimated to be $9.3\% \pm 0.33\%$ and a final key of 45545 bits was generated after error correction and privacy amplification. Figure 6.6 shows a screen shot of Bob's QKD application during the same experiment. Bob encrypted the message "QKD rocks!!! Chris rules!!!!!" with his key,

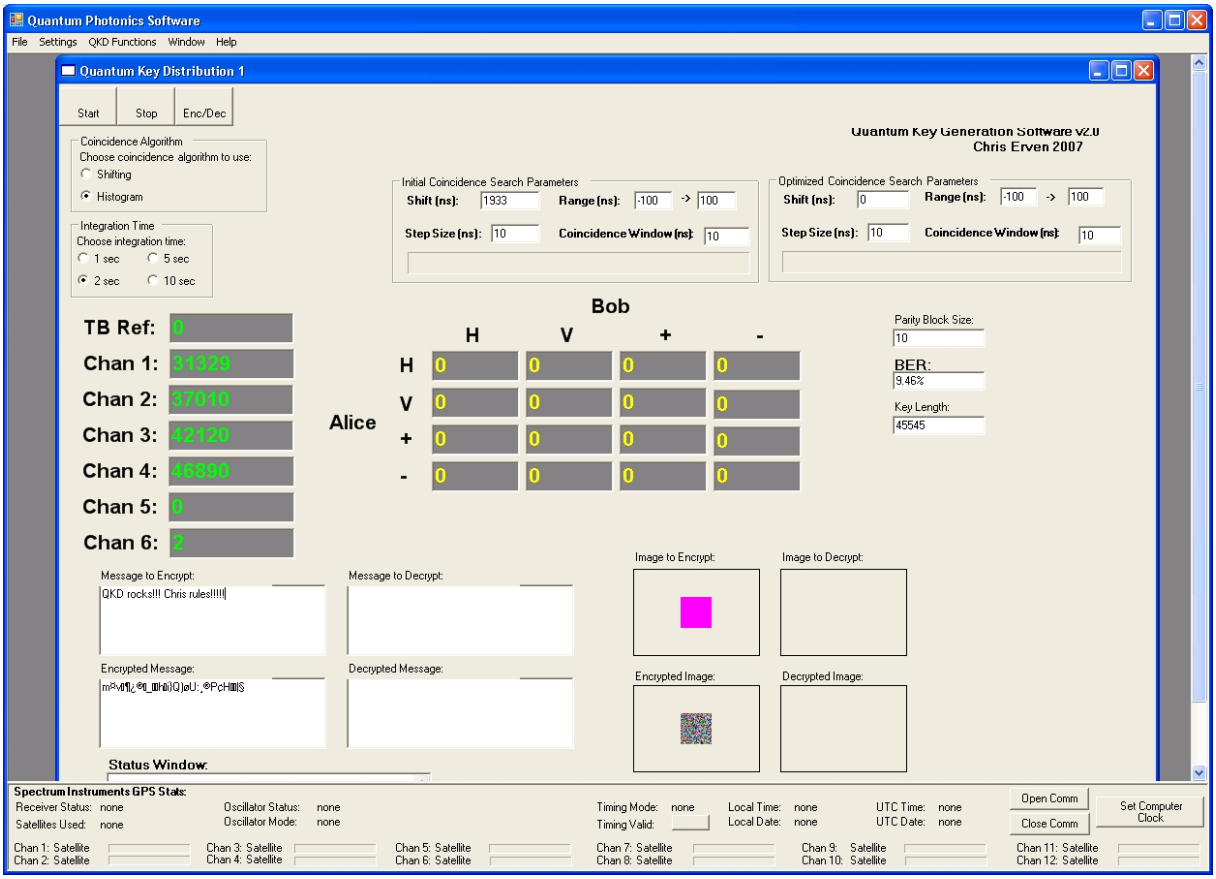

Figure 6.6: Screen shot of the Bob's QKD application for the QKD experiment.

as can be seen in the bottom left of his screen in Figure 6.6. The encrypted message sent to Alice can be seen at the bottom of her screen in Figure 6.5. Alice's QKD application then used her independently generated key to decrypt the message and recover what Bob sent. As the figures show, Alice was able to faithfully decrypt the message which Bob sent.

Thus, the successful operation of the QKD system was demonstrated.

Tables 6.2 and 6.3 show a portion of Alice's and Bob's raw keys from this experiment before error correction has occurred. Tables 6.4 and 6.5 show the corresponding portion of Alice's and Bob's final keys after error correction and privacy amplification, which were used to encrypt and decrypt the message sent in the above experiment. As can be seen from the figures, error correction removed all of the errors from the two keys, while privacy amplification shortened the keys by $\sim 33\%$.

10100011100000011111 11001100001**0**11000100 0110**0**010000011110110
0000**0**110111110010011 11110010011000101000 0100011010**1**10110000
1010**0**101010**1**11011011 00010101001**0**00001000 1101111**1**100111101**1**0
00001011001010110110 01000**0**11010000011110 11111101**1**00100010110

Table 6.2: A portion of Alice's raw key before error correction.

10100011100000011111 11001100001**1**11000100 0110**1**010000011110110
0000**1**110111110010011 11110010011000101000 0100011010**0**0110000
1010**1**101010**0**11011010 00010101001**1**00001000 1101110**1**100111101**0**0
00001011001010110110 01000**1**11010000011110 11111101**1**10100010111

Table 6.3: A portion of Bob's raw key before error correction.

11011111100010010101 10100001010000100111 11101101110100101111
01110001010010101010 11110110001101111111 00010101011110111010
00100000011100010000 11110111010001111001 10100101111110010101

Table 6.4: A portion of Alice's final key after error correction and privacy amplification.

Next, the experimental data gathered in Alice's and Bob's experiment above was analyzed to track the performance of the system over time by using the ability to save the

1101111110001001010 1010000101000010011 1110110111010010111
0111000101001010101 1111011000110111111 0001010101111011010
0010000001110001000 1111011101000111100 1010010111111001010

Table 6.5: A portion of Bob's final key after error correction and privacy amplification.

statistics of the QKD algorithm to memory during their experiment. The experimental rates are the same as above. Figure 6.7 shows a graph of the quantum bit error rate (QBER) over the course of the three minutes and twenty seconds when Alice and Bob were measuring data. It shows the QBER fluctuating around its average value of 9.3%.

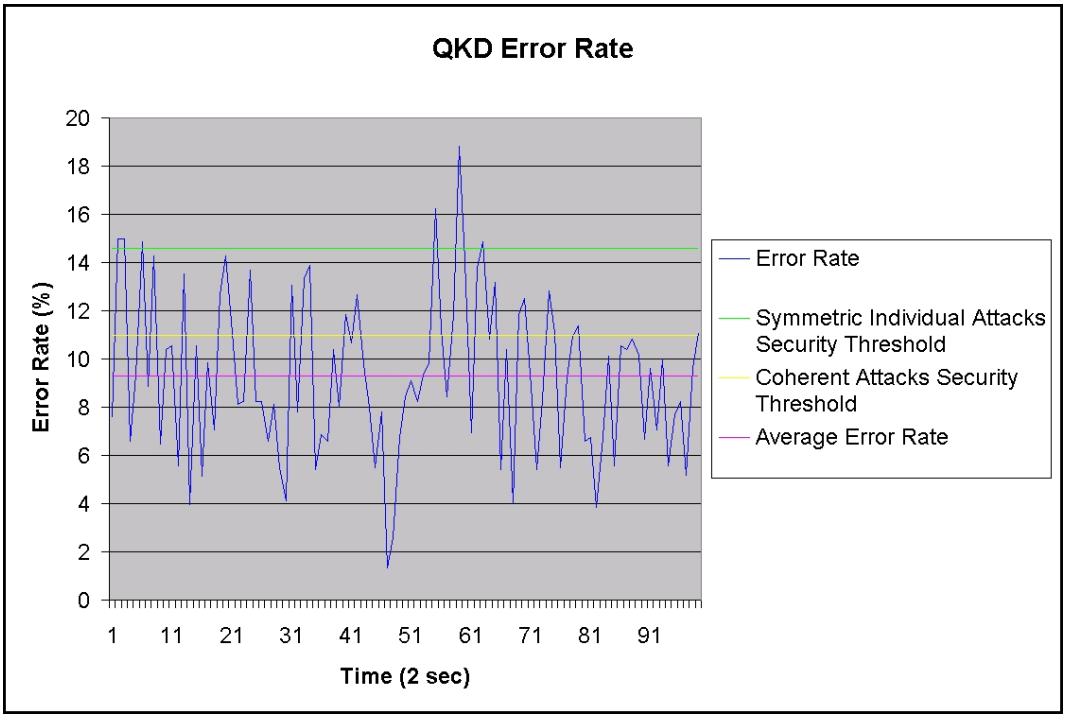

Figure 6.7: The QKD parameters tracked over the course of a long experiment.

The same large fluctuations that were present in the Bell parameter experiment are also visible here, see Section 6.4 for more comments.

6.4 Investigation of Errors in the System

The results of the previous sections indicate two potential errors in the system: the large fluctuations of the Bell parameter (Section 6.2) and QKD error rate (Section 6.3), and the strong correlations observed in different bases with the Channel Rates utility (Section 5.2). The large fluctuations of the Bell parameter and QKD error rates might simply be due to the small sample size being used to calculate their values. The QKD error rate is calculated using 10% of a key being produced at a rate of ~ 350 Hz. The experiments shown in Section 6.3 used 2 second intervals of data collection, thus each datum was generated using ~ 70 bits which is a sample size small enough that it could produce fairly large fluctuations ($\sim 12\%$). Further evidence of this is Section 6.2 used ~ 750 values to estimate the Bell parameter, based on a collection rate of ~ 750 Hz and 1 second intervals of data collection, and it showed less drastic fluctuations than the QKD error rate. The second possible cause of the large fluctuations could be the stability of the polarization in the long single-mode fibre which guides Alice's half of the photon pairs up to the rooftop. Any movement of the fibre could change the random polarization rotation that was originally compensated for and produce some of the fluctuations seen. Also, the fibre could exhibit a slower polarization drift due to temperature changes and other slower factors over the course of an experiment. Experiments are currently being conducted to measure the polarization stability in the long single-mode fibre and to determine the source of the large fluctuations seen in the data.

The strong correlations observed in different bases with the Channel Rates utility could be due to a number of causes. The correlation could indicate an error in one of the detector boxes which means that it is not measuring in the correct basis in each arm. Section 6.2 seems to corroborate this since one of the expectation values is always much lower than the other three. An improper setting of the half-wave plate could cause this. Also, the non-polarizing beam splitter could be slightly polarizing the photons which exit it. Finally, the polarizing beam splitters leaking any horizontally polarized photons into the fibre meant to collect vertically polarized photons and vice versa could also contribute to the problem. Experiments are currently underway to check each of the optical elements in the detector

modules. Improper alignment of the source so that $\varphi \neq \pi$ could also cause different statistics; however, local measurements of the source have always indicated that $\varphi = \pi$. The larger problem is trying to compensate for the random polarization rotation of the long single-mode fibre which takes Alice's half of the photon pairs to the rooftop. The rotation is corrected by observing single photon count rates from the source which are already low and fluctuate from one second to the next after travelling over the free space link. This makes it particularly difficult to accurately correct for the polarization rotation. Any imperfections in the polarization compensation will then lead to problems when the phase due to the long single-mode fibre is compensated for. This could produce $\varphi \neq \pi$ in the state which Alice and Bob receive. Strong alignment lasers at 658 nm and 808 nm are currently being installed on the source board which will travel the same path as the entangled photons and be coupled into the long single-mode fibre without needing to be attached via separate fibres. In addition to aiding initial alignment, the 808 nm laser will provide a much stronger reference signal which should allow the random polarization rotation to be compensated for more accurately. Once the random polarization is accurately compensated for, it should also be possible to compensate for the phase induced by the fibre much more accurately.

Chapter 7

Conclusions and Future Work

Quantum key distribution has the potential to be the next generation cryptographic solution. It does not rely on the assumptions of most cryptographic protocols in use today: namely, the computational complexity of certain mathematical problems. Assumptions that are going to be increasingly challenged as the field of quantum computing matures and quantum computers with increasing numbers of qubits are built.

This thesis has illustrated the development of a quantum key distribution system using polarization-entangled photon pairs to generate a secure key shared by two parties: Alice and Bob. Entanglement distribution with this system has been demonstrated along with successful secret key distribution over a single free-space link.

Now that a working quantum key distribution system has been developed, there are a number of exciting new things planned. The first improvement planned is to automate as much of the system as possible. Currently, all of the alignment of the source and the free-space optics is performed by hand; thus, the first task is to automate many of the alignment mechanisms so that a single person can operate the system. Much of the automation work is already well underway. Also, the system was designed with the intent of implementing two free-space links: one at the BFG building and one in an office at the Perimeter Institute. This shows the true power of quantum key distribution since the entangled photon source never has to be controlled by Alice or Bob. It also mimics the eventual deployment of the entangled photon source onto a low earth orbit satellite.

The system was built in a modular fashion so that various components could be improved and replaced as they were developed. The next improvement planned is to investigate how to increase the key generation rate of the system. Some of the potential solutions are: the replacement of the parametric down-conversion source with a brighter Sagnac interferometric source [23], the development of more efficient detector modules, and the investigation of using adaptive optics to correct some of the wavefront distortion induced on the photons by the free-space link.

There are a number of possible software improvements that can be incorporated as well. Currently Alice and Bob have to perform a Bell inequality experiment (which requires a slightly modified source) in order to demonstrate that the photons they are measuring at that particular moment are entangled. The notion of entanglement witnesses [27] makes it possible to demonstrate that the photons being distributed to Alice and Bob are entangled by analyzing the QKD data directly without any changes to the setup. Thus, an entanglement witness will be a future addition to the software. Additionally, improved error correction and privacy amplification protocols will also be investigated.

The ultimate goal of the project is to create an autonomous system capable of running twenty-four hours a day undisturbed. To this end, automated alignment hardware and control algorithms will be implemented in the system. This will allow it to continuously track and align the free-space link for continuous operation. Also, in order for the operation of the system to be possible during daylight a spatial filter (a variable pinhole designed by Biomedical Photometrics Inc.) will be built and added to the receiver telescope in order to reduce the increased background light experienced during the day.

Bibliography

[1] SPCM-AQ4C datasheet, 2005. http://optoelectronics.perkinelmer.com/content/DataSheets/DTS_SPCMAQ4C.pdf.

[2] Nist internet time service, 2007. http://tf.nist.gov/service/its.htm.

[3] A. Aspect, P. Grangier, and G. Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, 1982.

[4] J.S. Bell. On the einstein podolsky and rosen paradox. *Physics*, 1:195–200, 1964.

[5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3, 1992.

[6] C.H. Bennett and G. Brassard. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, New York, 1984.

[7] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992.

[8] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.P. Poizat, and P. Grangier. Single photon quantum cryptography. *Phys. Rev. Lett.*, 89:187901, 2002.

[9] D. Bohm. *Quantum Theory*. Prentice-Hall, Englewood Cliffs, N.J., 1957.

[10] V. Buzek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844, 1996.

[11] J.L. Carter and M.N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143, 1979.

[12] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880, 1969.

[13] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92:271–272, 1982.

[14] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete. *Phys. Rev.*, 47:777–780, 1935.

[15] A.K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[16] G.Brassard and L. Salvail. Secret-key reconciliation by public discussion. *Lect. Notes Comput. Sci.*, 765:410, 1994.

[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 75:145–195, 2002.

[18] C.K. Hong and L. Mandel. Experimental realization of a localized one-photon state. *Phys. Rev. Lett.*, 56:58, 1986.

[19] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Petersonn. Practical free-space quantum key distribution over 10km in daylight and at night. *New Journal of Physics*, 4:43.1, 2002.

[20] W.Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, 2003.

[21] T. Jennewein. Time stamping units, 2006. Dotfast Inc.

[22] T.D. Jennewein. *Quantum Communication and Teleportation Experiments Using Entangled Photon Pairs*. PhD thesis, University of Vienna, 2002.

[23] T. Kim, M. Fiorentino, and F.N.C. Wong. Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer. *Phys. Rev. A*, 73:012316, 2006.

[24] E. Knill, R. Laflamme, H. Barnum, D. Dalvit, J. Dziarmaga, J. Gubernatis, L. Gurvits, G. Ortiz, L. Viola, and W.H. Zurek. Introduction to quantum information processing. *arXiv:quant-ph/0207171*, 2002.

[25] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.R. Rarity. A step towards global key distribution. *Nature*, 419:450, 2002.

[26] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337, 1995.

[27] M. Lewenstein, B. Kraus, J.I. Cirac, and P. Horodecki. Optimization of entanglement witnesses. *Phys. Rev. A*, 62:052310, 2000.

[28] M. Lindenthal. *Long-Distance Free-Space Quantum Communication with Entangled Photons*. PhD thesis, University of Vienna, 2006.

[29] H.K. Lo and H.F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.

[30] I. Marcikic, A. Lamas-Linares, , and C. Kurtsiefer. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.*, 89:101122, 2006.

[31] D. Mayers. Unconditional security in quantum cryptography. *J. Assn. Comput. Mac.*, 48:351, 2001.

[32] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[33] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, The Netherlands, 1995.

[34] K.J. Resch, M. Lindenthal, B. Blauensteiner, H.R. Bohm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderback, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger. Distributing entanglement and single photons through an intra-city free-space quantum channel. *Opt. Exp.*, 13:202, 2005.

[35] M.A. Rowe, D. Kielpinski, V. Meyer, C.A. Sackett, W.M. Itano, C. Monroe, and D.J. Wineland. Experimental violation of bell's inequality with efficient detection. *Nature*, 409:791–794, 2001.

[36] B.E.A Saleh and M.C. Teich. *Fundamentals of Photonics*. John Wiley & Sons Inc., Hoboken, N.J., second edition, 2007.

[37] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:657, 1949.

[38] P.W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441, 2000.

[39] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Free-space distribution of entanglement and single photons over 144km. *arXiv:quant-ph/0607182*, 2006.

[40] G.S. Vernam. Cypher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elec. Eng.*, 55:109, 1926.

[41] G. Weihs. *Ein Experiment zum Test der Bellschen Ungleichung unter Einsteinscher Lokalität*. PhD thesis, Universität Wien, 1999.

[42] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of bell's inequalities under strict einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, 1998.

[43] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.