On Experimental Quantum Communication and Cryptography

by

Chris Erven

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics - Quantum Information

Waterloo, Ontario, Canada, 2012

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.

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

C. Erven

Abstract

One of the most fascinating recent developments in research has been how different disciplines have become more and more interconnected. So much so that fields as disparate as information theory and fundamental physics have combined to produce ideas for the next generation of computing and secure information technologies, both of which have far reaching consequences. For more than fifty years Moore's law, which describes the trend of the transistor's size shrinking by half every two years, has proven to be uncannily accurate. However, the computing industry is now approaching a fundamental barrier as the size of a transistor approaches that of an individual atom and the laws of physics and quantum mechanics take over. Rather then look at this as the end, quantum information science has emerged to ask the question of what additional power and functionality might be realized by harnessing some of these quantum effects. This thesis presents work on the sub-field of quantum cryptography which seeks to use quantum means in order to assure the security of ones communications. The beauty of quantum cryptographic methods are that they can be *proven* secure, now and *indefinitely* into the future, relying solely on the validity of the laws of physics for their proofs of security. This is something which is impossible for nearly all current classical cryptographic methods to claim.

The thesis begins by examining the first implementation of an entangled quantum key distribution system over two free-space optical links. This system represents the first test-bed of its kind in the world and while its practical importance in terrestrial applications is limited to a smaller university or corporate campus, the system mimics the setup for an entangled satellite system aiding in the study of distributing entangled photons from an orbiting satellite to two earthbound receivers. Having completed the construction of a second free-space link and the automation of the alignment system, I securely distribute keys to Alice and Bob in two distant locations separated by 1,575 m with no direct line-of-sight between them. I examine all of the assumptions necessary for my claims of security, something which is particularly important for moving these systems out of the lab and into commercial industry. I then go on to describe the free-space channel over which the photons are sent and the implementation of each of the major system components. I close with a discussion of the experiment which saw raw detected entangled photon rates of

565 s^{-1} and a quantum bit error rate (QBER) of 4.92% resulting in a final secure key rate of 85 bits/s. Over the six hour night time experiment I was able to generate 1,612,239 bits of secure key.

With a successful QKD experiment completed, this thesis then turns to the problem of improving the technology to make it more practical by increasing the key rate of the system and thus the speed at which it can securely encrypt information. It does so in three different ways, involving each of the major disciplines comprising the system: measurement hardware, source technology, and software post-processing. First, I experimentally investigate a theoretical proposal for biasing the measurement bases in the QKD system showing a 79% improvement in the secret key generated from the same raw key rates. Next, I construct a second generation entangled photon source with rates two orders of magnitude higher than the previous source using the idea of a Sagnac interferometer. More importantly, the new source has a QBER as low as 0.93% which is not only important for the security of the QKD system but will be required for the implementation of a new cryptographic primitive later. Lastly, I study the free-space link transmission statistics and the use of a signal-to-noise ratio (SNR) filter to improve the key rate by 25.2% from the same amount of raw key. The link statistics have particular relevance for a current project with the Canadian Space Agency to exchange a quantum key with an orbiting satellite - a project which I have participated in two feasibility studies for.

Wanting to study the usefulness of more recent ideas in quantum cryptography this thesis then looks at the first experimental implementation of a new cryptographic primitive called oblivious transfer (OT) in the noisy storage model. This primitive has obvious important applications as it can be used to implement a secure identification scheme provably secure in a quantum scenario. Such a scheme could one day be used, for example, to authenticate a user over short distances, such as at ATM machines, which have proven to be particularly vulnerable to hacking and fraud. Over a four hour experiment, Alice and Bob measure 405,642,088 entangled photon pairs with an average QBER of 0.93% allowing them to create a secure OT key of 8,939,150 bits. As a first implementer, I examine many of the pressing issues currently preventing the scheme from being more widely adopted such as the need to relax the dependance of the OT rate on the loss of the system and the need to extend the security proof to cover a wider range of quantum communication

channels and memories. It is important to note that OT is fundamentally different than QKD for security as the information is never *physically* exchanged over the communication line but rather the joint equality function $f(x) = f(y)$ is evaluated. Thus, security in QKD does *not* imply security for OT.

Finally, this thesis concludes with the construction and initial alignment of a second generation free-space quantum receiver, useful for increasing the QKD key rates, but designed for a fundamental test of quantum theory namely a Svetlichny inequality violation. Svetlichny's inequality is a generalization of Bell's inequality to three particles where any two of the three particles maybe be non-locally correlated. Even so, a violation of Svetlichny's inequality shows that certain quantum mechanical states are incompatible with this restricted class of non-local yet realistic theories. Svetlichny's inequality is particularly important because while there has been an overwhelming number of Bell experiments performed testing two-body correlations, experiments on many-body systems have been few and far between. Experiments of this type are particularly valuable to explore since we live in a many-body world. The new receiver incorporates an active polarization analyzer capable of switching between measurement bases on a microsecond time-scale through the use of a Pockels cell while maintaining measurements of a high fidelity. Some of the initial alignment and analysis results are detailed including the final measured contrasts of 1:25.2 and 1:22.6 in the rectilinear and diagonal bases respectively.

Acknowledgements

First, I must thank my co-supervisors Dr. Gregor Weihs and Dr. Raymond Laflamme for taking a chance on an engineering student who'd picked up a few extra quantum physics courses to fulfill his curiosity while in undergrad and letting me buy, build, break, fix, and play with equipment worth more than a contingent of luxury cars. Their insightful comments, hands on help, and continuous support throughout my degree have been an inspiration to me. I must also thank the other members of my advisory committee; Dr. Norbert Lütkenhaus, for his extensive knowledge of QKD and security proofs, and his insightful and thought provoking comments; Dr. Kevin Resch, for his wide array of optics knowledge and willingness to always lend an ear to problems in the lab and offer helpful suggestions; and Dr. Joe Emerson, for stepping in at the last minute to fill the role of my internal/external examiner. And lastly, I must also thank Dr. Wolfgang Tittel for kindly agreeing to be my external examiner, offering many helpful suggestions on this thesis and challenging me during the defense.

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 all of her love, understanding, moral support, and in particular her patience for the non-linear nature of a PhD and its ever changing projects, timelines, and end dates. It's been a long road, but I wouldn't want to have taken it with anyone other than you.

Thank you to all of the administrative staff at the IQC for all of their help and support throughout the years. I am grateful for financial support from the IQC, the Bell family through their Bell Family Fund for Quantum Computing Scholarship program, the National Sciences and Engineering Research Council of Canada for their NSERC PGS D postgraduate scholarship, and the University of Waterloo for their President's scholarship.

I have been fortunate to have had the help of many high school and undergraduate co-op students as well as graduate students and research assistants during these experiments and I have made every effort to list their contributions in the introduction to each chapter. I have to thank Christophe Couteau, the one and only postdoc in the PEG group, for all of his optics advice and help in the lab when I was starting out; Mike Ditty, for all of the help with the random requests from my projects; Rolf Horn, my partner in crime during the

PhD, for his unfailing help in the lab at a moments notice, commiseration on the trials and tribulations of quantum optics work and the non-standard nature of our degrees, exercise on the badminton court, and the commercial musings about our work; and Gina Passante, who wrote up her PhD in parallel with me and always knew how I was feeling when I was about to chuck my laptop out the window, commiserating with her hopefully helped us both get through it a little easier.

To all of the members of the University of Waterloo Varsity badminton team, of which I have been a part from 2000 and had the privilege to also coach since 2006, thank you. You always provided me with a respite where I could come and forget about work and other problems, and instead exercise and focus on a game I've loved for years while relaxing with friends. It was here that I truly learned about the commitment, training, and dedication necessary to excel at a sport. The friendships I have made with such a wide variety of talented people are some of my most special and the things I have learned about teamwork, fair play, hard work, and all the intangible people skills that come with interacting in a team atmosphere will guide me for the rest of my life. To all of the older guys at the KW badminton club that accepted me into their group, there are few things I look forward to more than coming to shoot the breeze with you and getting some exercise and great games at the same time.

Last, but certainly not least, I would like to thank Martin Laforest, Mike Wesolowski, Osama Moussa, Rolf Horn, Gina Passante, Chris Jackson, Peter Groszkowski, Nathan Killoran, Easwar Magesan, Adam Paetznick, Dave Pitkanen, Jeremy Chamalliard, Jonathan Lavoie, Deny Hamel, Evan Meyer-Scott, Casey Myers, J.C. Boileau, Marcus Silva, Colm Ryan, and any others I might have missed for the many needed: volleyball, tennis, poker, hockey, and golf games; beers (many many beers); and friendship that have made my time at Waterloo so special. And many thanks to all of the other IQC faculty, staff, and students who have enriched my time at IQC many times over.

Throughout my time as a graduate student I have learned many things. But these last three were perhaps the most important:

1. There is a whole lot in this world that I do not understand.
2. It is counter-productive to pretend that I do.

3. But I should never stop trying to... because I'll get there in the end.

My sincerest thanks to each and every person that helped me along the way.

Every so often,
In moments few and far between,
The veil is pulled back,
Revealing a little bit more of this wondrous universe,

This is the ultimate reward,
For science has its own virtue,
We can understand,
And we should never stop asking the question,

"Why?"

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

For more than half a century Moore's law, describing the trend of the transistor's shrinking size, has proven to be uncannily accurate [111]. However, we are now approaching a fundamental barrier as the size of a transistor approaches that of an individual atom and the laws of quantum mechanics take over. Over the last few decades quantum information science has emerged to investigate the exciting question of what additional power and functionality might be realized by harnessing these quantum effects. Indeed, it was discovered early on that quantum computers can perform exponentially faster computation for particular tasks such as the simulation of quantum systems [56] and the factoring of large numbers [148].

1.1 Quantum Information Processing

Quantum information processing exploits 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. While the subject of quantum information processing has exploded over the last two decades, I will focus in this thesis on a small subset involving the development and improvement of a secure quantum key distribution system, the implementation of a new

cryptographic primitive in a quantum setting called oblivious transfer, and on the development of a free-space optical receiver and measurement device for use in an experiment exploring some foundational aspects of quantum mechanics. For this, I first *very* briefly mention a few general concepts of quantum information processing that will be needed along the way[1]. For the most part, I have aimed to make each chapter as self-contained as possible, including any relevant background material at the start of the chapter.

1.1.1 Photonic Qubits

A number of physical implementations are being pursued to build a quantum computer. Over the past few years, photonics has emerged as a leading approach for the following reasons: single photons are largely immune to noise; can easily be manipulated to realize one-qubit logic gates; allow the encoding of qubits in several degrees of freedom; and are ideal for the communication of quantum states.

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. Like a classical bit, a qubit can be in one of two orthogonal states. In the language of quantum mechanics the state of a qubit is represented by a vector in a two-dimensional *Hilbert* space, with the states $|0\rangle$ or $|1\rangle$ known as the computational basis. However, unlike for classical computing, a qubit can also exist in a superposition of states. Any normalized linear combination of the basis states is permissible, with a general state given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

where α and β are in general complex numbers referred to as amplitudes satisfying the relation $|\alpha|^2 + |\beta|^2 = 1$, which ensures the proper normalization for the state. Two qubits are represented by states of the form $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ where there is again a normalization condition.

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

[1]For a more complete treatment please refer to Ref. [112].

to form flux, phase, or charge qubits. However, 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. As mentioned to start this section, photons are ideal qubits for quantum communication and cryptography schemes because of their weak interaction with each other and most matter[2]. This weak interaction translates into low decoherence rates, so that the qubits maintain their quantum states for a long time [112]. Also, they move at the speed of light which makes it possible to transmit them very quickly over large distances.

Since the qubit state is normalized, it can also be rewritten as

$$|\psi\rangle = \cos\frac{\theta}{2}|H\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.2}$$

allowing the *Hilbert* space of one qubit to be conveniently graphically represented on the Poincaré sphere. Here the angles $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$ define a point on the three dimensional unit sphere, also know as the Poincaré sphere, shown in Fig. 1.1. Pure states lie on the surface of the sphere while mixed states are found inside the sphere.

The actions of a halfwave plate (HWP) and quarterwave plate (QWP), two optical devices which I will use often in my optical setups, can be seen using the Poincaré sphere. A HWP rotates the polarization state of a photonic qubit in the equatorial plane (ie. the xz-plane of linear polarization states) around the R-L axis, while a QWP in general converts linear polarization states into elliptical polarization states with a rotation around any vector in the xz-plane. The most important polarization states of a photonic qubit and their correspondence between the computational states and the axes on the Poincaré sphere are shown in Table 1.1.

A HWP and QWP are examples of single qubit gates or single qubit rotations. In quantum information theory, operations are performed with one and two qubit gates corresponding to unitary operators. While this thesis will not have much need for the language

[2]Photons can be made to interact strongly with matter, but usually cavity schemes are used to increase their coupling and the probability of their absorption. Certainly in free-space and optical fibres photons interact very weakly with their environment.

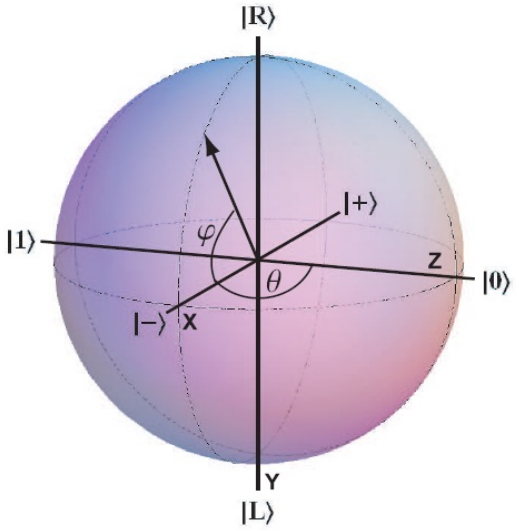

Figure 1.1: A graphical representation of the polarization state of a single photonic qubit, the Poincaré Sphere.

Polarization State	Linear Combination	Name	Linear Polarization Angle	Axes
$\|H\rangle$	$\|H\rangle$	horizontal	0°	Z
$\|V\rangle$	$\|V\rangle$	vertical	90°	Z
$\|D\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	diagonal	45°	X
$\|A\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	anti-diagonal	135°	X
$\|R\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	right circular	-	Y
$\|L\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	left circular	-	Y

Table 1.1: The table shows some of the most important states of light. Any polarization state can be produced from a linear combination of horizontal and vertical polarization.

of quantum gates, I mention it here since I will use this language when describing the quantum key distribution experiments. More precisely, I will refer to the random unitary transformation as a single photon transits a singlemode fibre which needs to be undone in order to recover the expected correlated results.

1.1.2 Entanglement

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. Einstein, Podolsky, and Rosen (EPR) studied these states in 1935 [43] for purely philosophical concerns about the 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 [25] 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 that 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 Sec. 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 that validate the predictions of quantum mechanics using various types of entangled particles, such as photons [11, 162], single ions [129], 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 that can be used for quantum cryptography, known as the Bell states. They have the following form using the polarization

of photons:

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle) \tag{1.3}$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle) \tag{1.4}$$

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 $\frac{1}{2}$. 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 and these correlations will extend to any basis. This anti-correlation of the entangled $|\Psi^{-}\rangle$ state will be a key feature of quantum cryptographic protocols.

1.1.3 Bell's Inequality

In 1964 J.S. Bell [16] derived an inequality for correlation measurements that 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 measured independently, 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 [35]. A slightly modified version of their inequality is given by

$$S(\mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}') = |E(\mathbf{a}, \mathbf{b}) + E(\mathbf{a}', \mathbf{b}) + E(\mathbf{a}, \mathbf{b}') - E(\mathbf{a}', \mathbf{b}')| \leq 2 \tag{1.5}$$

where $E(\mathbf{a}, \mathbf{b})$ is the expectation value of polarization correlation measurements made on a two photon system with the polarization measured at the angles $\mathbf{a}$ and $\mathbf{b}$ respectively[3]. Also note that boldface notation is used to denote a measurement setting (eg. $\mathbf{a} = 0°$) while non-boldface notation is used to denote a particular measurement outcome (eg. $a = \pm 1$). We will see a generalization of Bell's inequality in Ch. 5 when I discuss the spacelike separated Svetlichny inequality experiment.

The following short derivation of the CHSH inequality is due to a combination of A. Peres [121] and Nielsen and Chuang [112]. It is a useful starting point for my discussion of Sveltichny's inequality in Sec. 5.1.1. 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 $\mathbf{a}$ and $\mathbf{a}'$, while Bob can measure his photon at the angles $\mathbf{b}$ and $\mathbf{b}'$. For a particular choice of measurement angle, the measurement device can either tell the observer that the photon was polarized parallel or perpendicular to the chosen angle. For example, Alice measuring a photon at an angle $\mathbf{a} = 0°$ (the H/V basis) can either get the result H or V. A measurement result parallel to the measurement angle (ie. H) is assigned a value of +1, while the orthogonal measurement result (ie. V) is assigned a value of -1. Let the corresponding measurement results for the angles $\mathbf{a}$, $\mathbf{a}'$, $\mathbf{b}$, and $\mathbf{b}'$ be represented by the variables a, a', b, and b'. These variables can have the values ± 1.

Now consider the equation

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

since $b, b' = \pm 1$ it is easy to see that either $a(b + b') = 0$ or $a'(b - b') = 0$ which means that Eq. 1.6 must equal ± 2. Now, if several trials are run these quantities are converted to expectation values and taking the absolute value gives the CHSH inequality of Eq. 1.5.

Quantum mechanics maximally violates the CHSH inequality, attaining a value of $S = 2\sqrt{2}$, if the two photons are in any of the Bell states of Sec. 1.1.2 and the angles $\mathbf{a} = 0°$, $\mathbf{b} = 22.5°$, $\mathbf{a}' = 45°$, and $\mathbf{b}' = 67.5°$ are used. In this case the first expectation value

[3]Notice that to violate a Bell inequality it is sufficient to measure in one of two linear polarization bases (typically Alice in the 0° and 45° bases and Bob in the 22.5° and 67.5° bases for maximum violation) without the need to measure any elliptical states. When we come to Svetlichny's inequality in Sec. 5.1.1 we will generalize the measurements to make use of those in the circular basis as well.

reduces to $E(\mathbf{a}, \mathbf{b}) = -\cos(\mathbf{a} - \mathbf{b})$ and similarly for the other expectation values. This violation can also be used to show entanglement since $S > 2$ can only be achieved with entangled states.

Locality requires that the measurement outcomes of Alice are independent of the measurement outcomes of Bob and is what allows me to group the measurement results as I do on the right side of Eq. 1.6. Realism on the other hand assumes that the measurement outcomes must have some predetermined value according to the properties of the system (including any hidden variables) and is what allows me to claim that $a, a' = \pm 1$ for Alice and $b, b' = \pm 1$ for Bob.

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. Or said another way, the fair sampling assumptions means that the sample of data is representative of the full set of particles, rather than some special subset for which there appears to be a Bell inequality violation.

In experiment, the expectation values $E(\mathbf{a}, \mathbf{b})$ are calculated from the number of events for each set of measurement angles as follows

$$E(\mathbf{a}, \mathbf{b}) = \frac{C_{++}(\mathbf{a}, \mathbf{b}) + C_{--}(\mathbf{a}, \mathbf{b}) - C_{+-}(\mathbf{a}, \mathbf{b}) - C_{-+}(\mathbf{a}, \mathbf{b})}{N} \tag{1.7}$$

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

$$N = C_{++}(\mathbf{a}, \mathbf{b}) + C_{--}(\mathbf{a}, \mathbf{b}) + C_{+-}(\mathbf{a}, \mathbf{b}) + C_{-+}(\mathbf{a}, \mathbf{b}). \tag{1.8}$$

1.1.4 Visibility

I quickly mention the definition of visibility since it is one of the typical measures I will use to describe the operation of my entangled sources. The visibility is obtained via joint

polarization measurements on the entangled photon pairs. In general, the fringe visibility of a two-photon state is obtained by setting the polarization analyzer on Alice's side to the fixed angle $\mathbf{a}$ while rotating the polarization analyzer on Bob's side from 0 to 2π. The number of coincident events, $N(\mathbf{a}, \mathbf{b})$, detected which are polarized parallel to Alice and Bob's polarization analyzers will exhibit the usual fringes ubiquitous to optical interference experiments and will be given by

$$N(\mathbf{a}, \mathbf{b}) = V \sin^2(\mathbf{a} - \mathbf{b}) N_{total} \tag{1.9}$$

where N_{total} is the total number of particles measured, and V, the visibility (which is what I am interested in) is given by

$$V = \frac{N_{max}(\mathbf{a}, \mathbf{b}) - N_{min}(\mathbf{a}, \mathbf{b})}{N_{max}(\mathbf{a}, \mathbf{b}) + N_{min}(\mathbf{a}, \mathbf{b})} \tag{1.10}$$

where $N_{max/min}$ are the maxima/minima of the observed coincidences.

In any basis, there is a fringe visibility curve associated with $\mathbf{a}$ and its orthogonal angle $\mathbf{a} + \frac{\pi}{2}$. In a polarization analyzer where the measurement is just as good for either angle there is no point to measuring the second curve. However, with the polarizing beamsplitters (PBS) I use in my polarization analyzers there is typically a $\sim 2\%$ error in the reflected vertically polarized arm. Thus, if I was only to use the maxima associated with the transmission arm of my PBS I would overestimate the total visibility I see with my equipment and the quantum bit error rate (QBER, see Sec. 2.1 for definition) I measured in a QKD experiment would not match with the source visibility I measured beforehand. Thus, to calculate my documented visibilities I actually use an average visibility for these two cases. This is convenient since my polarization analyzers (described in Sec. 2.4.3) are already setup to measure both of these maxima and minima and rather than measure two entire fringe visibility curves in order to calculate the visibility I will instead directly measure the maxima and minima in a basis and use the formulas

$$N_{max}(\mathbf{a}, \mathbf{b}) = C_{+-}(\mathbf{a}, \mathbf{b}) + C_{-+}(\mathbf{a}, \mathbf{b}) \tag{1.11}$$

and

$$N_{min}(\mathbf{a}, \mathbf{b}) = C_{++}(\mathbf{a}, \mathbf{b}) + C_{--}(\mathbf{a}, \mathbf{b}) \tag{1.12}$$

where $C_{+-}(\mathbf{a}, \mathbf{b})$ represents the number of events where the first photon was measured parallel to $\mathbf{a}$ while the second was measured orthogonal to $\mathbf{b}$ and similarly for the other three terms. I will then plug these results into Eq. 1.10 to compute the visibility[4].

Lastly, I remark that to decide whether the two-photon state from the source is entangled or not, visibilities must be measured in two conjugate bases (such as the rectilinear and diagonal bases). When the visibilities of both satisfy $V > 1/\sqrt{2} \sim 0.7071$, a classical description no longer suffices to describe the state of the photon pair (since classical correlations could not produce these joint visibility measurements) and one concludes that the state of the photons is entangled. This is also the minimum value for both visibilities at which the violation of a Bell inequality becomes possible as does secure quantum key distribution. This argument assumes that one of the four Bell states from Eq. 1.3 or Eq. 1.4 are being created, since in general there are many other entangled states which can have much lower visibilities and not produce a Bell inequality violation.

1.2 Quantum Cryptography

Quantum cryptography has become one of the first mature applications to develop out of the new field of quantum information processing. From the initial ideas of uncloneable quantum money by Wiesner [163] in the 1970's, to the first concrete quantum key distribution (QKD) protocol (BB84) discovered by Bennett and Brassard [19] in 1984; QKD has rapidly become a very practical application of quantum information science.

Bennett and Brassard showed how one could distribute a random secret key between two parties (Alice and Bob) using single qubits along a quantum channel [19]. The security of their scheme was due to random measurements of the qubits in one of two complementary, non-orthogonal bases, and the fact that quantum mechanics prohibits any potential eavesdropper (Eve) 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

[4]For example, measuring the visibility in the HV basis, Eq. 1.10 would become $V = (C_{HV} + C_{VH} - C_{HH} - C_{VV})/(C_{HV} + C_{VH} + C_{HH} + C_{VV})$.

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 a number of different QKD protocols that can be grouped into two main categories: prepare-and-measure QKD, and entangled QKD. The prepare-and-measure QKD protocols have Alice sending randomly selected quantum states from a particular set to Bob, which he then measures. From the states that Alice sends and the measurements that Bob makes, they can generate a secure key. Whereas, the entangled QKD protocols see a central source of entangled particles send a photon from each pair to Alice and Bob. Alice and Bob each make random measurements on their photons and from these measurements they generate a secure key. Both methods can generate a secure key, but as is becoming more evident in the literature the entangled QKD protocols seem to suffer less from side channel security loopholes[5]. There are many different protocols for quantum key distribution too numerous to list here, a good overview of QKD and various implementation schemes can be found in Refs. [64, 42, 133].

1.2.1 The BB84 Protocol - Prepare-and-Measure QKD

The first QKD scheme proposed was the prepare-and-measure BB84 protocol discovered by Bennett and Brassard [19]. In this protocol Alice sends Bob a series of linearly polarized single photons randomly encoded in one of two maximally conjugate[6] polarization bases (H/V or $+45°/-45°$). She does this by first generating a sequence of two digit binary

[5]Side channels refer to the fact that while a QKD protocol might have been proven secure in theory, deficiencies in the experimental implementation might open up side channels for an eavesdropper to exploit in order to gain information about the key. Obviously, if these side channels were not taken into account in the original security proof, then the QKD system will not be secure, even though the original theoretical protocol was. The most obvious example of this is the recent quantum hacking experiment by Makarov *et al.* [62] which exploited a deficiency in detector design to allow an eavesdropper to gain full knowledge of Alice and Bob's key.

[6]The bases are maximally conjugate in the sense that any pair of vectors, one from each basis, have the same overlap, e.g. $|\langle H| + 45°\rangle|^2 = \frac{1}{2}$. In other words, measuring a photon in one basis (e.g. H/V) which was encoded in the conjugate basis (e.g. $+45°/-45°$) produces a random result.

random numbers [7] which she then uses to choose which photon polarization state to send to Bob according to the prescription $\{|\psi_{00}\rangle = |H\rangle, |\psi_{01}\rangle = |V\rangle, |\psi_{10}\rangle = |+45^\circ\rangle, |\psi_{11}\rangle = |-45^\circ\rangle\}$. Bob then randomly (using a random-number generator independent from Alice's) analyzes the polarization of each photon he receives in one of the two conjugate polarization bases which Alice encoded the photons in (H/V or $+45^\circ/-45^\circ$). At this point, whenever Alice and Bob used the same basis they should get perfectly correlated results. It is interesting to note that neither Alice nor Bob can control the key which results from this protocol. Indeed, it is the product of both of their random choices which produces the key and assures its security.

Bob then translates his polarization measurements into a classical bit string using the assignments $\{H, +45^\circ\} \rightarrow 0$ and $\{V, -45^\circ\} \rightarrow 1$. Alice, knowing which sequence of states she sent, can also translate them into a bit string. These are Alice's and Bob's raw keys. Alice and Bob then have to sift their bit strings down to only those events where they used the same polarization basis, since these are the only cases where they should be correlated, to arrive at their sifted keys. They do this by Bob publically announcing to Alice which basis he measured each photon in, while Alice correspondingly announces whether each measurement was compatible or not[8]. Ideally, Bob's sifted key is identical to Alice's sifted key but due to imperfections in the setup (background photons, detector noise, and polarization imperfections) there are usually errors between Alice's and Bob's sifted keys. Alice and Bob correct these errors by using an error correction scheme over a public channel thus arriving at their reconciled keys. During the error correction Alice and Bob are able to estimate an upper bound on any information an eavesdropper might have gained based on the error rate which they observe. Alice and Bob then perform classical privacy amplification on their reconciled keys to reduce any knowledge Eve might have

[7] The task of generating random numbers is in and of itself a very hard task and quantum mechanical means are usually necessary to generate truly random numbers.

[8] Note that Bob is not revealing any of his measurement results which form the key, nor is Alice revealing any of the states she sent which forms her key. They are only announcing each basis they used which does not leak information about their keys to an eavesdropper other than whether an operation the eavesdropper might have performed was compatible with their operations. The eavesdropper cannot go back in time to use the basis information to gain perfect knowledge of Alice and Bob's key without disturbing the states of the photons.

about their keys to an exponentially small amount at the cost of shortening their keys. Alice and Bob then have identical shared, secret keys which they can use to communicate securely between themselves.

1.2.2 The BBM92 Protocol - Entangled QKD

The BBM92 protocol [21] is an entangled QKD scheme which essentially symmetrizes the BB84 protocol by having *both* Alice and Bob make random measurements in one of two non-orthogonal complementary bases (H/V or $+45°/-45°$) on photons from an entangled photon pair source. In this protocol, a source of entangled photon pairs, usually in the $|\Psi^-\rangle$ Bell state of Eq. 1.3, is placed between Alice and Bob. 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 (H/V or $+45°/-45°$). Then, just as in the Prepare-and-Measure scheme (Sec. 1.2.1), Alice and Bob must sift their measurement results down to only those where they both measured in the same basis. Error correction and privacy amplification then proceed just as in the Prepare-and-Measure protocol so that Alice and Bob eventually end up with identical, shared, secret keys.

The randomness in the key resulting from the entangled QKD protocol is due to the fact that measuring the $|\Psi^-\rangle$ state randomly collapses it to one of the two possibilities. Again, neither Alice nor Bob can control the key which results from the protocol, it is the product of their random basis choices and the state collapse which produces the key. Intuitively, the security of the protocol is due to the fact that any measurements Eve might choose to make on either photon travelling to Alice or Bob will necessarily disturb their state and ruin the perfect anti-correlations present in Eq. 1.3, thus increasing the error rate and alerting Alice and Bob to her presence.

1.2.3 Implementations

There are many different protocols for quantum key distribution, a good overview of several QKD schemes can be found in the review papers by Gisin *et al* [64] and Scarani *et al*

[133]. Quantum cryptography with the BB84 protocol can be performed ideally with single photons [23] or, more practically, with weak coherent laser pulses [17]. However, the weak coherent laser pulse schemes are open to the photon number splitting attack (PNS) 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. As a consequence of the PNS attack, prepare-and-measure QKD systems are much more limited in the maximum tolerable loss for which security can be proven, which consequently limits the maximum distance a QKD system might be able to securely cover. Fortunately, a method for overcoming the photon-number-splitting attack for the weak laser pulse implementations has been developed using decoy states [75]. Quantum key distribution protocols have also been extended to use entangled qubit pairs as in the Ekert91 protocol proposed by Ekert in 1991 [44] or the BBM92 protocol by Bennett, Brassard, and Mermin in 1992 [21].

There are now a number of different QKD protocols which have been demonstrated using both optical fibers and free-space optical links as their quantum channel [162, 102, 72, 127, 84, 155]. Some of the more recent free-space experiments include the distribution of entanglement through intra-city free-space links by Resch *et al.* [127] and Peng *et al.* [119], the distribution of entanglement over 144 km and subsequent generation of a secure key by Ursin *et al.* [156], and the complete implementation of a free-space QKD system which included all key extraction routines by Marcikic *et al.* [102] and Erven *et al.* [48]. Even newer is the demonstration of the feasibility of free-space QKD using continuous variables by the group of Leuchs [45, 14, 68]. For a comprehensive overview of both the theory and different experimental implementations of QKD please refer to the recent review article by Scarani *et al.* [133].

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 [70], 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 [89]. 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[9] leads to purely random keys, which are very hard to create classically but are an important ingredient for secure communication [76].

1.2.4 Security Proofs

The intuition behind the security of quantum key distribution is based on one of the tenets of quantum mechanics: measurement disturbs a quantum system. A second property of quantum mechanics, the No-Cloning theorem [165], completes the security intuition for quantum key distribution by showing that its impossible for an eavesdropper to clone or copy the photons sent to Alice and Bob; thus, preventing her from interacting with copies so as not to disturb Alice and Bob's original photons. This means that any eavesdropper attempting to gain information about the photons as they are sent to Alice and Bob will necessarily disturb their state. This disturbance will have measurable consequences for Alice and Bob and will show up in the error rate induced in their measurements on their photons. There are then two important error rates [64, 97] by which I will claim my QKD system is secure in the following chapters:

1. Error Rate $< 14.6\%$ - QKD system secure against **symmetric individual attacks**[10]
2. Error Rate $< 11\%$ - QKD system secure against **coherent attacks**[11]

with both of these being in the long key limit.

[9] 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, but individually each measurement and thus each bit in the key is random.

[10] Symmetric individual attacks are attacks where Eve is restricted to interacting with each qubit being sent from Alice to Bob one at a time, ie. she interacts with them individually.

[11] Coherent attacks are the most general attacks allowed by quantum mechanics where Eve can collectively interact her own quantum systems with every qubit sent from Alice to Bob, delay any measurements she might make on her quantum systems until Alice and Bob announce their measurement bases, and make a collective measurement on all her systems at once. This attack allows Eve to maximize the information she might gain about their key and minimize the disturbance she causes in their error rate.

Security proofs and the vulnerabilities of QKD systems is a PhD thesis in its own right. Most of the attacks in the literature exploit deficiencies in a particular implementation of a QKD system rather than problems with the QKD protocol itself. As such, each paper is usually quite specific to a particular implementation or a particular piece of hardware being used. By far, the biggest overall vulnerability is side-channel attacks where the implementation deviates from the ideal protocol and leaks information into various side channels that the security proofs do not take into account. While it is virtually impossible to rule out all side-channel attacks for a system, particularly the prepare-and-measure systems; one possible solution is device-independent security proofs [5] which might finally provide a complete proof of security for a real QKD system. Currently though detection efficiencies are nowhere near as good as they need to be in order to apply device-independent security proofs and consequently almost all QKD systems, commercial or educational, display vulnerabilities which a potential eavesdropper might exploit.

1.3 Overview of this thesis

Chapter 1 provides a short introduction to quantum information processing and quantum cryptography. It contains some of the general background information necessary for later parts of the thesis including: pertinent information on photonic qubits and entanglement, a discussion of Bell's Inequality (which the Svetlichny inequality work of Ch. 5 will build on), and the definition for visibility (a metric I commonly use to describe the performance of my entangled sources). I then move on to discuss quantum cryptography, classifying the field into the two broad categories of Prepare-and-Measure QKD and Entangled QKD. I finish by mentioning some of the most pertinent work on implementations of QKD and the proofs of its security. This chapter was written solely by myself and drew upon the references therein.

Chapter 2 details a two free-space link QKD experiment performed early on during my PhD. I begin by first reviewing the BBM92 QKD protocol implemented by the system. I then move on to closely detail and discuss the assumptions going into my security claims for the system, something that is extremely important for the future of the technology and its

security in light of recent problems with side channel attacks and detector blinding schemes. I then quickly mention a few words about the free-space channel over which my entangled photons travel before getting into the particular implementation of my system including the entangled photon source, free-space optics, polarization analyzers and detectors, and classical post-processing routines. I finish with a discussion of the results obtained during the experiment and in particular the performance of my classical error correction routines.

Even though a substantial portion of the work followed from preparations during my Masters degreee, I made a number of improvements during my PhD as well as constructed and automated the second free-space link. Additionally, all of the data collection and its subsequent analysis, as well as the work on the security claims for my system, were performed during my PhD. As such I include details of the experiment in its entirety since it provides a nice summary of my experimental setup which is referred back to many times in this thesis. The experiment was done in collaboration with a large group of people, all of whom are listed at the beginning of the chapter and to which I am truly grateful. While I had a lot of help during the project, I remained the project manager having a hand in every facet of the system and collected all of the data discussed in this thesis.

Chapter 3 examines three different projects seeking to improve the final key rate of my QKD system. The first improvement was made at the measurement hardware level and examined the efficiency gains possible by non-uniformly biasing the basis selection. I perform one of the first security analyses of this scheme in the finite key limit case for use in my system. During the security analysis I benefitted from a collaboration with postdoc X. Ma and some of his initial work in this area. With security taken care of, I then proceed to carry out and analyze a number of experiments varying the basis biasing, eventually showing a 79% improvement in the key generation rate over the unbiased case.

The second improvement was made at the source technology level and saw the development of a second generation entangled photon source based on a Sagnac interferometric design. To begin I first detail some background information on spontaneous parametric down-conversion and the techniques of quasi-phase matching and periodic poling in order to increase the effective non-linearity of certain crystals. I then detail the design of the source and all of the setup and alignment procedures necessary for its optimized operation. During the construction and alignment of the source I collaborated with D. Hamel during

his Masters work and benefitted from a number of techniques developed by him. I close with a discussion of some of the performance metrics of the new source comparing it against my first source. In particular the new source is two orders of magnitude brighter than my first source with a much narrower bandwidth of 0.23 nm allowing for the possibility of eventually running the QKD system under twilight and daylight conditions.

Finally, I detail a third improvement made at the software post-processing level with the implementation of a signal-to-noise ratio (SNR) filter on the fluctuating single photon counts rates measured over the free-space link. But first I perform three different experiments measuring the probability distribution of the (fluctuating) atmospheric transmission coefficient (PDTC) for my free-space QKD system verifying that the PDTC does indeed become a log-normal distribution as the fluctuations increase. With this in mind, I then examine the implementation of an SNR filter to cut out those periods of transmission where the losses are high corresponding to a low SNR. During these periods the measured QBER is artificially increased due to a larger proportion of the data being made up of background detections showing no correlations. By cutting out these periods using the optimum block duration of 30 ms and SNR threshold of 95,000 counts/s I am able to increase the final secret key length by 25.2% generated from the same amount of raw data. For this work I benefitted greatly from a close collaboration with another PhD graduate student, B. Heim.

Chapter 4 explores the first implementation of a random oblivious transfer protocol secure in the noisy storage model. I start with some background on the development of the noisy storage model which is capable of proving the security of various protocols under the physical assumptions that an adversary does not possess a large reliable quantum memory and that the noise level of the memory must necessarily increase as the storage time increases. I then outline a simple OT protocol due to Schaffner. In order to proceed with a discussion of the security of the scheme I first layout the experimental implementation of my system and adapt Schaffner's simple protocol to it. With this background out of the way, I proceed to work through all of the relevant security arguments using the appropriate measured values necessary for me to claim security for the system. I note that I make use of some of S. Wehner's (a collaborator on the project) Mathematica code from the original theory paper, which I adapted to my experimental setup. Beyond that, I was the sole person responsible for carrying out the security calculations for my system.

Following the theory work, I then outline my results from an experiment lasting 4 hrs and 21 mins which was able to generate 8,939,150 bits of ROT key from a total of 2.704×10^{10} signals before losses with an intrinsic QBER of 0.93%. In the results, I highlight a number of issues pertinent to the security of the scheme many dealing with the implementation of a one-way error correction algorithm not the least of which is the fact that the algorithms required over 30.5 hrs to complete. To close, I discuss some of the most pressing issues currently holding ROT back from becoming more widely applicable, the two most important of which are: the need to relax the dependence of the ROT rate on the loss of the system, and the importance of developing security proofs to cover a wider range of quantum communications channels. I discuss these drawbacks not to critique the usefulness of ROT but rather to highlight areas where future theoretical work would be very beneficial much in the same way that security proofs for QKD have benefitted from much work over the last fifteen years.

Chapter 5 describes the design and implementation of second generation free-space receivers incorporating an active polarization analyzer for use in a space-like separated Svetlichny inequality violation. The experiment is being done in collaboration with a large group of people, all of whom are listed at the beginning of the chapter. I begin first with some background on: the Svetlichny inequality, which we want to test, building on the description of Bell's inequality in the introduction; a previous experiment by Lavoie *et al.* testing the Svetlichny inequality, albeit in a non-spacelike separated manner; and finally, the operation of a Pockels cell, the main device used to perform active basis switching quickly enough such that locality and freedom-of-choice conditions can be enforced.

With this done, I then move into my design for the new receiver, and the setup and alignment procedures necessary for the accurate operation of the PC. For the alignment, I benefit from a quantum random number generator and Pockels cell logic developed by L. Richards, Z. Yan, and Prof. T. Jennewein. I go through a number of steps needed to align the PC for proper operation, including: tuning the alignment of the PC, an initial measurement of the halfwave voltage, a scheme allowing the reduction of the operating voltage of the PC to the quarterwave voltage, verifying the proper operation of the PC, a duty cycle measurement, the setup needed to operate the PC as a HWP at 22.5°, and finally a procedure for fine-tuning the rotational alignment of the PC. After the PC is

properly aligned I am able to measure contrasts of 1:25.2 and 1:22.6 in the rectilinear and diagonal bases, respectively.

Chapter 6 closes this thesis with some conclusions about the work presented here. I try to tie the experiments detailed here into a larger picture for future quantum cryptography experiments and advances. In closing, I mention some of the exciting new prospects for extending this work and others towards future applications and implementations.

Chapter 2

Quantum Key Distribution Over Two Free-Space Optical Links

In this chapter I detail some of the first experimental work performed during my PhD thesis where a real-time entangled QKD system that distributes entangled photon pairs to Alice and Bob each over an optical free-space link was implemented. The work followed directly from the preparations during my Masters work [47] and resulted in the publications of Ref. [161] (© Society of Photo Optical Instrumentation Engineers 2007) and Ref. [48] (© The Optical Society 2008). Specifically, during my PhD I automated the pointing and alignment of the free-space links, built a second 1,325 m free-space link to the Perimeter Institute, solved problems with the polarization analyzers, improved the error correction routines, and took all of the data included in this chapter. Additionally, with the data collected I performed all of the analysis presented here and examined all of the security assumptions necessary to claim security for the system. While the results do follow from a lot of the work done for my Masters thesis, I include the experiment here in its entirety since it also provides a nice summary of my experimental setup which I refer back to many times in subsequent chapters.

In the experiment, I performed QKD with entangled photon pairs following the BBM92 protocol. While fibre implementations have produced some of the fastest systems to date [40], until reliable quantum repeaters are realized, fibre implementations will be limited

to a transmission distance of $\leq$ 200 km. Even with expected future advances in fibre, source, and detector technology, secure key distribution will still be limited to $\leq$ 400 km. This has prompted increased attention on free-space implementations. Indeed, a number of studies have been performed to evaluate the possibility of performing QKD with an orbiting satellite such as the International Space Station [114, 126, 12, 120, 9, 26]. Therefore, experience with free-space quantum key distribution in a variety of setups and experimental conditions will become very valuable for future long distance quantum communication experiments.

The chapter begins by describing the BBM92 entangled QKD protocol (Sec. 2.1) which is used in the experiment, then the assumptions necessary to guarantee the security of the implementation are examined (Sec. 2.2), next free-space communication through the atmosphere is mentioned (Sec. 2.3), followed by a description of the experimental implementation of the system (Sec. 2.4), finally an extensive discussion of the results from the experiment is given (Sec. 2.5), followed by a conclusion (Sec. 2.6).

This work was done in collaboration with a large number of people. P. Forbes, I. Soellner, N. Ilic, and E. Bocquillon, all co-op or exchange students at the Institute for Quantum Computing (IQC), provided much help with late night data collection, system testing, and the implementation of a number of small components for the system. B. Schmidt, a co-op student with the University of Toronto, programmed the initial error correction and privacy amplification routines. M. Peloso, a research assistant at the IQC, provided the initial design for the polarization analyzer and free-space optics and oversaw much of their intial construction. R. Horn, D. Smith, M. Laforest, and R. Kaltenbaek, all graduate students or postdocs at the IQC, provided optics advice and construction and testing help for the system. R. Irwin and T. Gerhardt, both high school students from the Waterloo area, provided programming and system characterization help. J. Thompson and P. McGrath, both co-op students at the University of Waterloo, provided a lot of help in the initial setup, characterization, and optimization of the source systems in the lab. Professors N. Lütkenhaus (IQC), H.K. Lo (U of T), and K. Resch (IQC) all provided enlightening discussions on the optical setup, theory of QKD, and security considerations for the system. H. Epp and the Environment and Parks Department of the City of Waterloo removed a particularly annoying arboreal eavesdropper that was performing a denial-of-

service attack on Bob's CEIT-PI free-space link. And finally my professors R. Laflamme and G. Weihs of the IQC and the Institut für Experimentalphysik provided a great deal of help in the background of QKD and quantum optics, and hands-on help with the optics in the lab. I oversaw the entire project, having a hand in every facet of the system from building the entangled photon source, to improving the error correction routines originally developed by B. Schmidt, to reworking the polarization analyzers and free-space optics originally developed by M. Peloso for easier practical use, to programming all of the real-time software programs necessary to align the system and ultimately perform the QKD protocol. I collected all of the data shown in the following sections with the help of those above and performed the subsequent data and security analysis.

2.1 BBM92 Protocol

The BBM92 protocol [21] (already mentioned in Sec. 1.2.2) using polarization-entangled photon pairs is a very elegant variation of the BB84 QKD protocol [19] which essentially symmetrizes the BB84 protocol. In my system, I have a source which produces polarization-entangled photon pairs in the $|\psi^-\rangle$ state (Eq. 2.1). These pairs are then split up with one photon from each pair being sent to Alice and Bob. Alice and Bob *both* measure their half of each pair randomly in one of two non-orthogonal complementary bases, the horizontal/vertical basis ($H = 0°$ and $V = 90°$) or the +/- basis ($+ = +45°$ and $- = -45°$). These measurements form Alice and Bob's raw keys. After measuring a sufficient number of photon pairs during the distribution phase, Alice and Bob sift down to only those events where they both measured in the same basis by communicating publically over a classical channel which basis they measured each photon in. Whenever they measured in the same basis their results should be anti-correlated (as shown in Eq. 2.1) and allow them to form a secret key; whereas, any measurement results where they measured in different bases will be random and should be discarded.

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) \tag{2.1}$$

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 sifted key.

After sifting, the sifted key goes through two more processing steps before it is turned into the final secure secret key. While theoretically Alice and Bob should measure identical raw keys, in a practical real life set-up (even without an eavesdropper) there will be small imperfections which contribute to a non-zero quantum bit error rate (QBER). Thus, it is necessary to perform classical error correction on the raw key to remove these errors. Finally, even though no eavesdropper might have been present, for absolute security any non-zero QBER must be assumed to correspond to information about the key being revealed. Additionally, during the classical error correction step, parities of different key bits are publically exchanged between Alice and Bob in order to correct these errors. This leaked information must also be taken care of. Thus, as a last step, Alice and Bob perform a classical privacy amplification protocol on their error-corrected key to reduce the maximum potential information an eavesdropper 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 [158] to communicate securely between themselves.

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 [165, 39] which prevents an eavesdropper from making copies of the qubits and then delaying their 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 monitoring the QBER over the course of their key distribution and verifying that it remains below the security threshold for their QKD protocol. Information theoretic arguments concerning the mutual information between Alice, Bob, and any eavesdropper, can then be used to derive an upper bound for an acceptable QBER in order to assure security against the

most general attacks allowed by quantum mechanics.

A few words can be found on some of the outstanding issues in QKD security proofs in Sec. 1.2.4, with one of the most important being recent work on side channels. Another pressing issue is that of finite key statistics and its effect on the statements of security. Most initial security work in QKD assumed the infinite key limit where the size of the key, n, was allowed to go to infinity helping, among other things, to remove some pesky terms in the key rate formulas. It was assumed that for all intents and purposes real systems quickly produced keys approaching this limit. However, it was recently shown that key lengths needed to be on the order of $\sim 10^7$ bits before secure keys could start to be generated [32]. Since work on finite key statistics was in its infancy during these experiments, I used the tolerable upper bound of 11% for my QBER [97] where the long key limit was assumed. We will see in Sec. 3.1.1 work in follow up experiments where I attempted to incorporate the major finite size key effects into my statement of security.

2.2 Security Assumptions

Although the unconditional security of many QKD protocols has been shown [133], practical implementations are always different from the ideal theory and the possible presence of side channels require that great care is taken when claiming that one has implemented an unconditionally secure quantum key distribution system. Certain assumptions, which are required for the security proofs, are not always met in practice. To that end, I fully state the assumptions going into my claim of security for my QKD system here.

First, to prevent a man-in-the-middle attack, all classical communications between Alice and Bob must be authenticated using a short amount of initial secret key for the first few messages and by key generated by the system afterwards. The key generation process is still efficient because the number of bits needed for authentication is logarithmic in the size of the key [6]. Since authentication is also a problem for classical cryptography and is easily solved using a small amount of pre-shared key along with well established secure classical authentication algorithms, I neglect it for my implementation and focus instead on the security assumptions relevant to the implementation of key distribution with quantum

means.

Second, I need to make certain assumptions about my detectors in order to assure the security of my system; namely, that each of my detectors have equal detection efficiencies, that each of the four channels in the detectors are independent, and that the dead-time of the detectors is a negligible security concern. As will be shown in the discussion of my results (Sec. 2.5), the detection efficiencies for each of Alice's and Bob's detectors were not equal. Attacks are known that can exploit a detector inefficiency mismatch [125, 101] and perhaps leave my system vulnerable to an eavesdropper. To properly deal with this problem in a QKD system with passive measurements one needs to carefully equalize the efficiencies of all the detectors without exposing further security loopholes. In a QKD system with active detection electronics a possible solution is to randomly assign which detector will measure "0" and which will measure "1" for each incoming photon in order to balance out the detection efficiencies and prevent an eavesdropper from taking advantage of this loophole. Since I employed a passive measurement system and properly dealing with this problem is an active area of research, I instead chose as an intermediate step to estimate the amount of extra privacy amplification needed to take care of the unequal *a priori* probabilities of having a "0" or "1" in the raw key and subtract it from the final key.

The assumption that each of the four channels in my detectors are independent means that the probability of detecting a photon on any channel is independent of whether a photon was previously detected on any other channel. While this is a natural assumption to make, it is not always found in practice and depends on the electrical design and physics of the detectors. Worse, it has recently been shown [103, 96, 62] that it is possible for an eavesdropper to blind and then classically control the single photon detectors based on avalanche photodiodes (APDs) typically used in QKD experiments. Though careful analysis suggests that a proper detector implementation might not have this problem [167]. Additionally, each detector channel has a certain dead-time after a detection event, in my case 50 ns, where the channel cannot detect another photon until it has been reset. To ensure security, it is important to reject multiple detection events that fall within the dead-time of the detectors; however, I assume that their influence on the security of my system was negligible since the rate of detected photons is low enough that any lingering effects of

one channel firing should have dissipated before the next channel detection event and the probability of having two detection events in the dead-time window was extremely small. Considering that detector side channel problems and their proper solutions are currently an active area of investigation, I leave them as outside the scope of this work and assume that the security of my system is not significantly compromised by these issues and that proper detectors can be built and used in a future system.

Third, spatial filtering, with a pinhole placed at the focus of my large receiving lens, was not used in the polarization detector boxes described below since the spectral and temporal filtering employed was sufficient to eliminate most background light and allow the identification and measurement of high fidelity quantum states. Nonetheless, it is known that if different detectors see slightly different spatial modes, an eavesdropper could control their relative efficiencies by varying the spatial mode of the input signal [60]. However, a significant effort was expended to make the relevant dimensions in the detector box symmetric and identical in order to avoid precisely this kind of attack. Additionally, the multimode fibres and their collimators themselves effected spatial filters, further limiting the attack of an eavesdropper. Strictly speaking this attack might still be possible, but is assumed to be minimal for our system.

Fourth, double clicks, that is when two detectors register a photon at the same time, need to be kept track of and should be assigned a random bit value. For entanglement based QKD it is unclear whether double pair emissions from the source lead to the same drastic security loophole experienced by weak coherent pulse QKD; namely, the photon number splitting attack [74, 28]. Nevertheless, it is important to keep track of these events and assign a random measurement result when a double click is observed. In the experiments described here, I did not explicitly monitor and record double clicks, instead the system chose whichever event it registered first. This is similar to a random choice within the detector time jitter, and is assumed to be sufficient for the security of our system.

Finally, I assume that the security proof by Ma *et al.* [97] applies to my system, since it is the closest proof to my experimental implementation. However, it does not precisely encompass my implementation on its own since it assumes the validity of the squashing model of detection and that active basis switching is performed. However, I can make it apply to my system since the validity of the squashing model for the active basis switching

detection scheme has recently been shown [15, 154, 79]. Additionally, it has also recently been shown that the requirement for active basis switching can be relaxed to include the passive scheme, which is used in this experiment [1]. I thus inherit the same two assumptions used in their proof when claiming security for my system. The assumptions are that I was operating in the long key limit, and that the bit and phase error rates can be assumed to be equal. Preliminary results suggest that the overhead is indeed dramatic for finite key statistics and many more bits are needed than the formulas in many security proofs suggest. Nevertheless, secure key generation with the rates observed with my system should still be within the realm of possibility. The proof also makes the simplification that the bit and phase error rates are equal which needs to be carefully examined for our system.

2.3 Free-Space Communication

Any signal sent over long distances will suffer losses from diffraction. Diffraction is the spreading of light after it passes through a small opening (in my case it will be the sending telescope aperture). It can be viewed as a direct result of the uncertainty principle since knowing the transverse position of the light (within the aperature) necessarily means that there must be uncertainty in the transverse momentum. This causes the beam to widen as it propagates (for LEO satellite distances the beam width on the ground will typically be on the order of 10 m) preventing it from being easily re-focused to the size it was when it exited the sender telescope[1], and will lead to photons being missed by any receiver telescope smaller than the beam size. The smaller the opening, the worse the diffraction. This is usually the main effect which causes loss in free-space systems over any sizeable distance, especially a satellite downlink but can be countered by using bigger telescopes or a shorter transmission wavelength.

Atmospheric transmittance is mainly due to diffraction but is also caused by the absorption of light by molecules in the atmosphere. Fig. 2.1 shows the atmospheric transmittance

[1]It is possible to focus the beam back to its initial size with a lens but usually the beam has spread to such a size that practical lenses are no longer available. Additionally, atmospheric turbulence would make it challenging to maintain the beam in the center of such a lens.

for a typical maritime location from ground (sea-level) to space at the zenith (directly overhead). Since most of the atmosphere is in the first 20 km or so, Fig. 2.1 is valid for any altitude above 20 km. The transmittance varies with wavelength depending on which types of molecules are present in the atmosphere and at which concentrations. It is thus possible to find various transmission windows where absorption for a certain range of wavelengths is minimal. Atmospheric turbulence also has an effect on the transmittance of a free-space channel. It is due to fluctuations in the refractive index due to local temperature variations. This effect acts like an additional pointing error, causing a broadening of the beam as well as beam wander. Turbulence will be discussed in more detail in Sec. 3.3 when I detail an experiment that examines free-space link transmission statistics.

Molecular scattering on the other hand is an effect that gets worst with shorter wavelengths and is the reason why the graph in Fig. 2.1 decreases as you move towards the left and shorter wavelengths. This puts a bound on how short one can make the wavelength of light before the gains from diffraction no longer outweigh the losses from atmospheric transmittance. Other losses can come from pointing errors, losses in the optical components comprising the sender and receiver telescopes, and the detection efficiency of the single photon detectors; all of which are wavelength dependent.

2.4 Implementation

This experiment represented the first real-time implementation of a two free-space link entanglement based quantum key distribution system using the BBM92 protocol (described in Secs. 1.2.2 and 2.1). The system was comprised of a compact spontaneous parametric down-conversion (SPDC) source, two free-space telescope links, two compact passive polarization analysis modules, avalanche photodiode (APD) single photon detectors, time-stampers, GPS time receivers, two laptop computers, and custom written software.

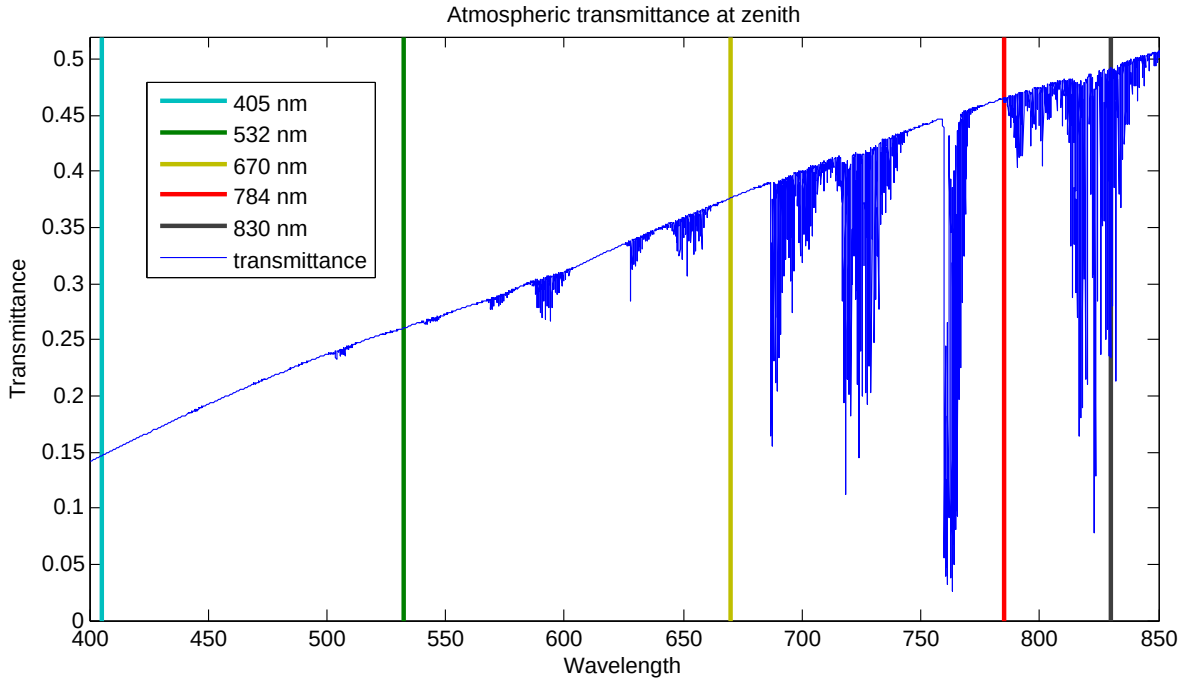

Figure 2.1: The atmospheric transmittance of a free-space channel for a typical maritime location from ground (sea-level) to space at the zenith (directly overhead). Since most of the atmosphere is in the first 20 km or so, it is valid for any altitude above that, but will be need to be scaled for horizontal terrestrial free-space links according to their distance [26].

2.4.1 Entangled Photon Source

Entangled photon pairs were generated via a compact type-II spontaneous parametric down-conversion (SPDC) source [86], which was built on an optical breadboard measuring 61 cm by 46 cm. A schematic of the source is shown in Fig. 2.2. The source was pumped by a 50 mW, 407.5 nm continuous wave violet diode laser from Blue Sky Research that was focused to an approximate radius of 25 μm in a 1 mm thick β-BBO non-linear optical crystal. The down-converted photon pairs at a degenerate wavelength of 815 nm were split off via two small prism mirrors. An achromatic doublet lens (f = 150 mm) collimated

the down-converted photons and a half waveplate oriented at 45° plus a 0.5 mm β-BBO crystal in each arm compensated for longitudinal and transverse walk-off effects. In general, as discussed in Sec. 3.2.1, the state produced in the down-conversion crystal is given by Eq. 3.18 with some arbitrary phase, φ, between the two polarizations. Thus, the angle of one of the compensator crystals was also used to set the relative phase between horizontal and vertical polarizations in order to produce the desired singlet Bell state, $|\psi^-\rangle$, of Eq. 2.1. After compensation, the photons were coupled into short singlemode optical fibres using aspheric lenses (f = 11 mm), which could then be connected either to long singlemode fibres which carried the photons to the rooftop sending telescopes or to local detectors. The fibres passed through manual polarization controllers which were used to undo the random polarization rotation (random unitary) induced by the singlemode fibres.

For local alignment, the short singlemode fibres were connected to a singlemode fibre - air - multimode fibre bridge which contained a narrowband spectral filter, centred at 815 nm with a 10 nm bandwidth (FWHM), in order to get rid of any residual laser light and background light before connecting the fibres to APD single photon detectors (PerkinElmer). These were the same filters that were used in the polarization analysis modules (discussed in Sec. 2.4.3). Connecting the fibres to the detectors with this method and inserting the optional polarizers (see Fig. 2.2) mounted on flip mounts allowed me to measure the local quality of the entangled photon source. Typically, I measured a pair rate of 12,000 s^{-1} and total single photon count rates on each side of 100,000 s^{-1}. The local entanglement quality was ascertained by measuring the visibility (see Sec. 1.1.4 for definition) of the source in the rectilinear (H/V) basis and the diagonal ($+45°/-45°$) basis. For the experimental run detailed in the following, I measured visibilities of 99.6% and 91% respectively shortly before the start of the experiment. This corresponded to a local QBER of 2.35%. The limited visibility in the diagonal basis was likely due to broad spectral filtering (10 nm) and uncompensated transverse walk-off in the β-BBO crystal which was aggravated by the narrow pump beam spot. The broad spectral filtering in the polarization detector box likely allowed some weakly entangled photon pairs through the filters which still had a strong correlation in the rectilinear basis (because of the nature of the down-conversion process), but almost no correlation in the diagonal basis. Any uncompensated transverse walk-off in the β-BBO crystal would lead to distinguishability

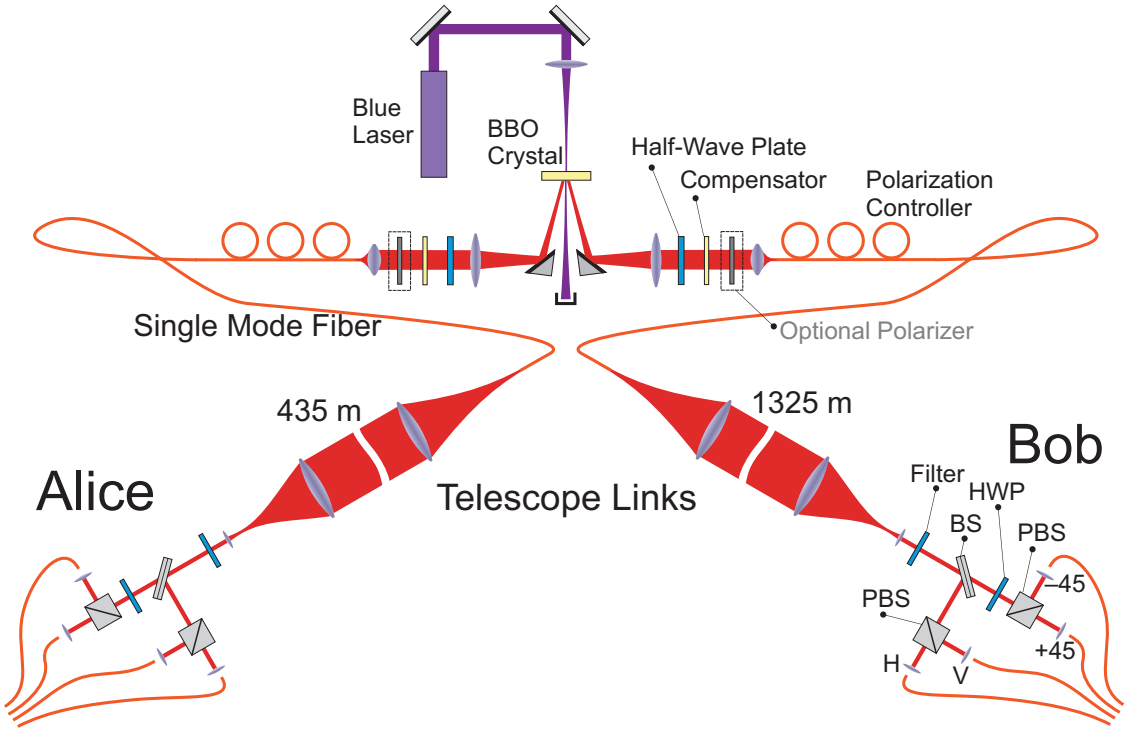

Figure 2.2: Experimental schematic of the entangled photon source, free-space link optics, and the passive polarization detection optics. Polarization entangled photons are generated via type-II spontaneous parametric down-conversion in a β-BBO nonlinear optical crystal pumped by a blue diode laser. Walk-off effects are mitigated with a half waveplate and compensator crystal in each arm. Optional polarizers allow the measurement of the local source visibilities. The entangled photons are coupled into singlemode fibres and transported to sender telescopes where they are then sent over a free-space link and collected with receiver telescopes. The photon polarizations are then measured in a passive polarization detector box which uses a 50/50 beamsplitter to perform the basis choice and the proper combination of half waveplates and polarizing beamsplitters to perform the polarization measurement in the correct basis.

and ruin the entanglement between the photons.

2.4.2 Free-Space Optics and Experiment Layout

For experimental runs, the short singlemode fibres were connected to longer 30 m singlemode fibres which transported the photons to two sending telescopes situated in telescope enclosures on top of the CEIT building, shown in Fig. 2.3, in the middle of the University of Waterloo campus. The sender telescopes consisted of a fibre adapter which held the end of the singlemode fibre along the optic axis of the collimating lens at its focus. The light was then allowed to naturally expand into the achromatic doublet lens (f = 250 mm, d = 75 mm) which collimated the light into an approximately 50 mm beam. The fibre adapter was mounted onto a translation stage driven by a high-resolution stepper motor which could adjust the focusing of the telescope. The same motors were used in the mount which held the sender telescope to adjust its azimuthal and elevation angles. All the motors could be controlled remotely from an operator at Alice's or Bob's location in order to align the sender telescope with the receiver system.

The source location was a potentially untrusted third party location with the receivers situated at two distant locations with no direct line of sight between them (see Fig. 2.3). Alice's receiver sat in an office in the BFG building, a free-space distance of 435 m away from the source. Bob, on the other hand, sat in an office at the Perimeter Institute, 1,325 m away from the source. This produced a total separation of 1,575 m between Alice and Bob.

2.4.3 Receivers and Polarization Analyzers

The receiver system consisted of a receiver telescope with a passive polarization detector box, that was mounted onto a homemade precision tip/tilt stage for fine adjustment of the receiver's pointing. The receiver telescope consisted of an achromatic doublet lens (f = 200 mm, d = 75 mm) and a second small lens (f = 10 mm, d = 5 mm) which collimated the photons down into a beam approximately 3 mm in diameter. The beam then passed through a narrowband spectral filter (described above in Sec. 2.4.1) to remove as much background light as possible and into the passive polarization analysis box shown

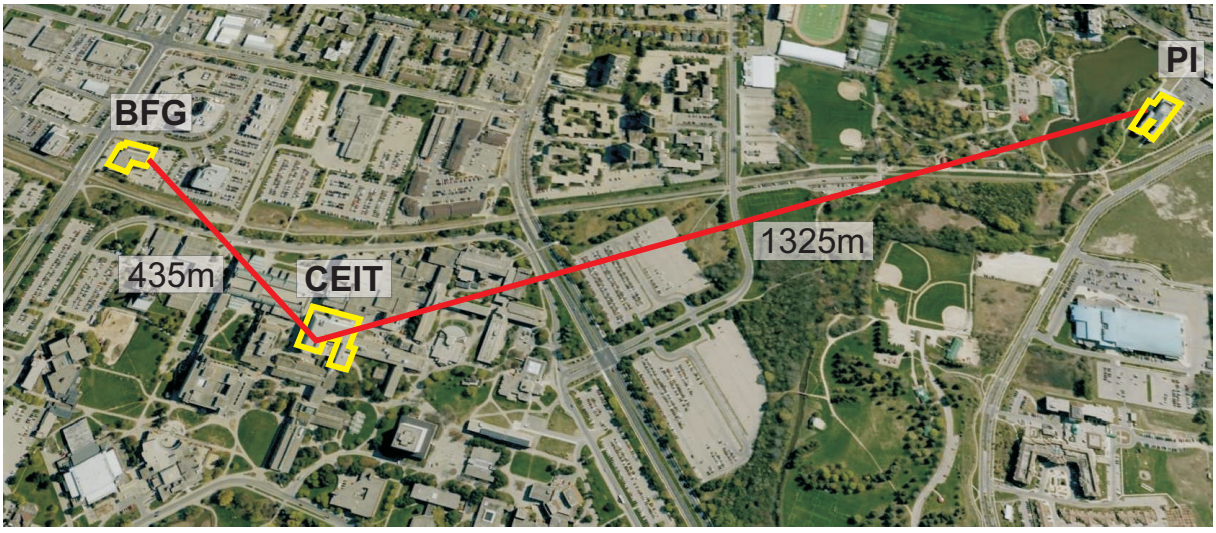

Figure 2.3: Map of the QKD setup showing the University of Waterlo and Perimeter Institute campuses with the source located in the CEIT building, Alice located 435 m away in an office at the BFG building, and Bob located 1,325 m away in an office at PI. Courtesy of Google Earth and Tele Atlas. Map Data © Tele Atlas 2008

in the bottom right portion of Fig. 2.2. A 50/50 nonpolarizing beamsplitter performed the basis choice by randomly reflecting or transmitting an incoming photon. Measurement of the photons in the diagonal basis was performed by a half waveplate and a polarizing beamsplitter in the transmitted arm; while measurement of the photons in the rectilinear basis was performed in the reflected arm with only a polarizing beamsplitter. The photons were then collected into four multimode fibres with permanently mounted aspheric lenses (f = 11 mm).

Tests of the polarization detector boxes revealed the typical leakage of some horizontally polarized photons into the vertical channel at the polarizing beamsplitters which would lead to an increase in the QBER rate of up to 1.5%. The average local QBER rate for our source combined with this error in the polarization analysis boxes yielded a baseline average QBER of 3.85%.

Finally, the photons delivered through the four multimode fibres were detected by a quad single photon counting module from PerkinElmer which had an approximate detection efficiency of 50% at my wavelength. In order to make the system simpler and remove the need for a separate timing channel to identify pairs of entangled photons, each photon detection event was time-stamped with timetagging units, developed by Dotfast Consulting, which had a timing resolution of 156.25 ps. Since photon pairs are created via parametric down-conversion at the same time in the β-BBO crystal, entangled photon pairs correspond to simultaneous detection events after path length differences are taken into account. Accepting only simultaneous detections reduces the accidental background almost to zero. However, this requirement forced me to experiment at night, since the background detection rates experienced during the day both overloaded my photon detectors and made entangled photon identification with this method infeasible.

2.4.4 Measurement and Classical Post-Processing Software

At each location, GPS timing units from Spectrum Instruments provided a highly accurate 10 MHz clock for the timetagging units. A one pulse per second (1PPS) signal provided a means to continually re-synchronize the electronics at Alice's and Bob's locations automatically, allowing indefinite stable timing operation of the whole system. Detection data

was then passed via a USB connection to a laptop computer at Alice's or Bob's locations, which then performed the classical parts of the BBM92 protocol (see Sec. 2.1).

At the beginning of the experiment, Alice's and Bob's computer clocks were first synchronized to <100 ms using a NIST timing application [113] in order to give them an accurate common start time to within 100 ms. A dedicated measurement thread in the software was responsible for continually processing detection events and sending data on to a dedicated coincidence thread. The coincidence thread then exchanged the timing information for all of the detection events, collecting the timetag lists for both Alice and Bob in Alice's computer. The lists were then processed with a coincidence algorithm in order to identify entangled photon pairs. The coincidence algorithm first calculated a histogram of coincident events in order to determine the timing offset between Alice's and Bob's timetag data. Coincidence detection was then performed using a coincidence window of 2 ns in order to identify the indices for all entangled photon pairs in their measurement lists. At this point, Alice and Bob extracted their raw keys, corresponding to entangled photon detection events, from their measurements using the index lists generated by the coincident algorithm. Along with the timing information, Alice and Bob also exchanged measurement basis information for each detection event. This allowed the coincidence thread to additionally sift the raw key data down to only those detection events where Alice and Bob measured in the same basis, yielding the sifted key. All of the classical communication was performed over an ordinary classical internet connection.

Ideally, Alice and Bob would have now shared identical keys which they could use to encrypt data; however, due to imperfect state production, transmission, and polarization analysis, not to mention any intervention by an eavesdropper, errors were expected between the sifted key. Errors were removed by performing a modified cascade error correction algorithm [29] on the sifted key. Cascade works by using public discussion to compare the parities of randomly chosen blocks from the sifted key and then performs a binary search on any blocks where the parities differ in order to identify and correct the error. It uses a multi-pass strategy in order to correct all errors with a high probability. During error correction, each parity communicated essentially leaks one bit of information to any eavesdropper monitoring the classical communication channel. The number of bits revealed during error correction was noted so that it could be taken care of in the privacy amplification stage.

The last step was for Alice and Bob to perform privacy amplification to reduce the amount of information an eavesdropper might possibly know about the key to an exponentially small amount at the cost of reducing the size of their key somewhat. First, Alice and Bob calculated the fraction of their raw, error free key which they could safely keep after privacy amplification. The calculation for this came from the proof of security which most closely matched my physical implementation [97]. It bounds an eavesdropper's information as a function of the QBER and estimates the necessary key reduction factor using Eq. 2.2

$$N_{\text{secure}} = N_{\text{sift}}(1 - h_2(\text{QBER})) - \text{N}_{\text{leakage}} - \text{N}_{\text{safety}} \tag{2.2}$$

where N_{secure} is the final number of secure bits which Alice and Bob could keep after privacy amplification, N_{sift} is the number of bits after error correction, $h_2(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function, N_{leakage} is the number of bits revealed during error correction, and N_{safety} is an additional safety parameter, which I set to 30 bits for this experiment. Using this reduction ensured that my system was secure both against symmetric individual attacks (QBER $< 14.6\%$) and coherent attacks (QBER $< 11\%$); generating no key if the QBER rose above 11%. Note that it is possible to achieve secure key distribution with QBER's above 11% [13] but it requires the use of two-way classical post-processing which we did not utilize in our system. Thus, the upper limit of secure key generation for my system was a QBER of 11%. It should also be noted that this is the key rate formula that is calculated in the infinite key limit as work on finite key statistics was still in its early stages at the time that this experiment was performed.

Alice and Bob then performed privacy amplification by applying the 2-universal hash function [33] given by Eq. 2.3

$$k_{\text{secure}} = (m \cdot k_{\text{corrected}} + n) \bmod p \tag{2.3}$$

to the raw error corrected key, keeping the last N_{secure} number of bits from the end. Here k_{secure} is the final secure key, $k_{\text{corrected}}$ is the error corrected key, m and n are large random numbers (smaller than p) generated by a random seed shared by Alice and Bob, and p is a large prime number. Alice and Bob then verified that they had established identical keys after these information reconciliation steps by checking the random hash value of their keys a number of times.

2.5 Results

The experiment detailed below was performed on April 28, 2008. First I detail the alignment of the two free-space optical links and the initial photon detection rates, then I show the measured quantum bit error rates (QBER) and key rates over the course of the experiment, next I reconstruct the coincidence matrix for Alice and Bob's measurement results and estimate the additional amount of privacy information needed to take care of the potential information that could have leaked to an eavesdropper based on the detector efficiency mismatch experienced, following that I examine the efficiency of my Cascade error correction algorithm, and then close the section with a summary of the results from additional single and double link experiments that were performed leading up to the main two free-space link experiment.

2.5.1 Initial Alignment

At the beginning of the experiment, the two free-space links were initially aligned with a 658 nm red laser diode coupled into a singlemode fiber, connected to the sending telescopes, and sent over the free-space links. After the shorter 435 m BFG link, this produced a spot at the receiver approximately 30 mm in diameter that typically wandered less than 10 mm from its centroid position. Airy rings were clearly visible in the spot over this shorter distance. The spot produced after the 1,325 m PI link was significantly worse, with a diameter of approximately 100 mm and a typical beam wander of 50 to 100 mm from its centroid position. Additionally, Airy rings were rarely visible in the spot indicating a significant amount of scintillation within the beam. A significant amount of the drastic degradation over the longer link can be attributed to the fact that the beam passed over an exhaust vent in the Physics building shortly after leaving the sender telescope.

Across the shorter BFG free-space link I received about 29,000 photons/s from the source, while I received about 10,000 photons/s from the source across the PI link. Taking into account the detection efficiencies of 64% and 60% for Alice and Bob's polarization detector boxes respectively[47], this yielded a link transmission efficiency of approximately 45.3% for Alice and 16.7% for Bob. The average detection rates for each of Alice and Bob's

detectors are shown in Table 2.1 including an estimate of the counts due to background light, dark counts, and photons received from the source.

	Average Detection Rates (photons/s)							
	H	V	+	-	Total	Background	Dark Counts	Source
Alice	5,203	7,755	6,741	6,194	25,893	14,693	1,200	10,000
Bob	7,845	12,296	11,219	10,980	42,340	12,140	1,200	29,000

Table 2.1: Detection rates for each of Alice and Bob's detectors including an estimated breakdown of events due to background light, dark counts of the detectors, and photons received from the source. As will be discussed below in Sec. 2.5.3, one can already note a detector efficiency mismatch between each of Alice and Bob's four detectors.

2.5.2 QBER and Key Rates

During the experiment an average coincidence rate of 565 s^{-1} was observed while the real-time coincidence rate varied wildly due to the beam fluctuations over the PI link. Fig. 2.4 (a) shows the QBER observed over the course of the experiment from 11:55 pm until 6:15 am at which point the rising sun saturated my detectors and made correct coincidence detection impossible due to the high background. This caused the QBER to skyrocket and prevented further secure key generation. The total average QBER during the experiment was observed to be 4.92% of which 2.11% and 2.81% were X and Z errors respectively. The increase in the QBER from the baseline 3.85% expected to the observed 4.92% was most likely due to residual uncompensated birefringence in the singlemode fibre used to transport the photons from the source to the sender telescopes and to accidental coincidences.

Fig. 2.4 (b) shows the key rates observed during the experiment with the raw key rate shown in blue, the sifted key rate in red, the theoretical maximum possible final key rate taken in the infinite key limit secure against coherent attacks (QBER $< 11\%$) in the model from [97] with an error correction algorithm operating at the Shannon limit[2] in green, and

[2]Between 1948-1949, Shannon wrote two papers which developed a mathematical framework for the

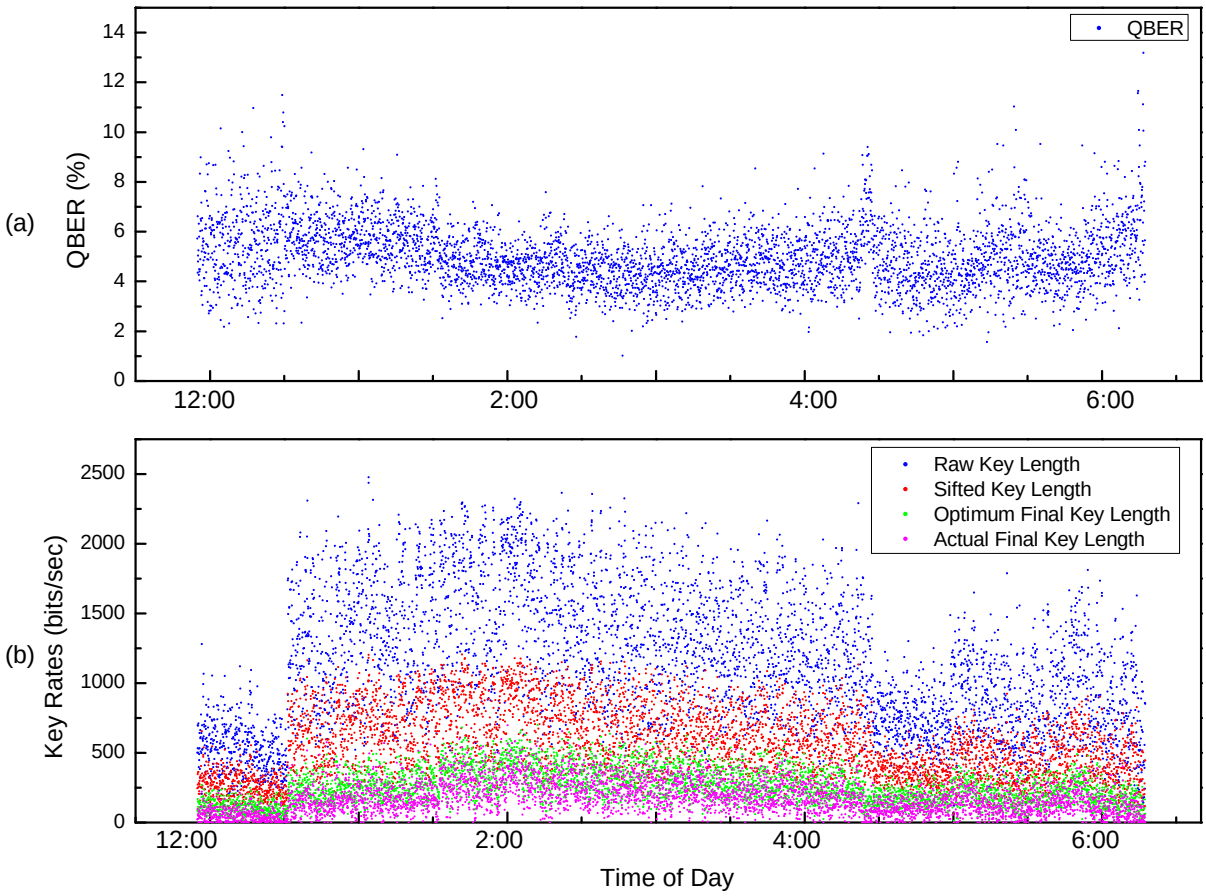

Figure 2.4: The measured (a) QBER and (b) key rates over the course of the two free-space link experiment. The raw key rate is shown in blue, the sifted key rate is shown in red, the maximum potential final key rate using error correction algorithms operating at the Shannon limit is shown in green, and the actual observed final key rate is shown in magenta. During the experiment I measured an average QBER of 4.92% and average rates of 565 bits/s for the raw key, 284 bits/s for the sifted key, 124 bits/s for the optimum final key, and 85 bits/s for the actual final key. Each data point before roughly 12:30 am is taken every second; whereas, each data point after this time is composed of two seconds worth of data. The data was taken on April 28, 2008.

the actual observed final key rate shown in magenta. The jump in raw key rate around 12:30 am is due to changing the collection time from one second to two seconds for each data point which was necessary due to the low count rates in order to maintain a software coincidence lock. Further drops in key rates though were due to the system slowly becoming misaligned during the night.

Over the course of the experiment, I observed an average raw key rate of 565 bits/s, an average sifted key rate of 284 bits/s, an average optimal final key rate of 124 bits/s, and an average actual final key rate of 85 bits/s. As can be seen in Fig. 2.4 (b), the final key rate for my system was below the theoretical limit due to the fact that my classical post-processing routines did not operate at the Shannon limit. The experiment generated a total raw key of 10,806,880 bits, a total sifted key of 5,422,762 bits, a maximum possible optimal final key of 2,374,384 bits, and an actual final key of 1,612,239 bits. In other words, the experiment was able to generate over 200 kB of secure key during the night with an efficiency of 0.1492 secure key bits generated from every raw key bit.

2.5.3 Reconstructed Coincidence Matrix and Detector Efficiency Mismatch

Table 2.2 shows the reconstructed coincidence matrix from Alice and Bob's measurement data recorded during the experiment. The detection totals for Alice and Bob's measurements of H, V, +, and - are also displayed and show an obvious variation in the detection efficiencies for each channel. As was discussed earlier, detector efficiency mismatches open a loophole which an eavesdropper can exploit. Since methods to properly deal with such

theory of communication [143, 144]. Among his many results, he was able to quantify the theoretical minimum amount of information needed to error correct two near identical strings with an error rate of e between them as $h(e)$, which is the binary entropy function ($h_2(e) = -e\log e - (1-e)\log(1-e)$) detailed earlier. With an error correction algorithm operating at the Shannon limit, my error correction term $N_{leakage}$ given in the key rate formula of Eq. 2.2 would in fact equal this term. However, as the main text indicates, my error correction algorithm operated less efficiently than the Shannon limit, modifying the amount of information needed to $f(e)h(e)$ where $f(e)$ now represents the error correction efficiency and typically $f(e) \geq 1$ with $f(x) = 1$ at the Shannon limit.

unequal detection efficiencies without exposing a security loophole were an active area of research at the time of this experiment, I instead carried out the following analysis.

		Alice				
		H	V	+	-	Total
	H	39,497	1,218,454	393,100	355,074	2,006,125
Bob	V	1,300,749	112,793	682,595	854,848	2,950,985
	+	680,032	878,628	51,217	1,262,143	2,872,020
	-	548,695	955,146	1,374,648	63,261	2,977,750
	Total	2,604,973	3,165,021	2,501,560	2,535,326	

Table 2.2: The reconstructed coincidence matrix for Alice and Bob from the two free-space link experiment. Also shown are the entangled photon detection totals for each of Alice and Bob's four detectors. The larger VV versus HH entries of the table also clearly show the higher number of errors in the vertical polarization channel of the polarization analyzers due to the typical leakage of some horizontally polarized photons into the vertical channel at the polarizing beamsplitters mentioned before in Sec. 2.4.3.

As an intermediate step, I performed a first estimate of the extra privacy amplification needed to take care of the unequal *a priori* probabilities of having a 0 or 1 in the raw key. I treated Alice's raw key as the correct one and assumed that Bob was correcting his raw key during the error correction step to match Alice's. Thus, it is the *a priori* probabilities of Alice ending up with a 0 or 1 in her raw key that I was interested in. I calculated Alice's *a priori* probabilities of getting a 0 or 1 according to Eq. 2.4

$$p_{0/1} = \frac{N_{0/1}}{N_0 + N_1} \tag{2.4}$$

where $N_{0/1}$ is the number of 0's/1's measured over the course of the experiment which can be computed from the last line in Table 2.2. Calculating these, I found $p_0 = 0.4725$ and $p_1 = 0.5275$. In order to take care of this imbalance during privacy amplification, I would then have to add a term to Eq. 2.2 so that it becomes Eq. 2.5

$$N_{\text{secure}} = N_{\text{raw}}(1 - h_2(\text{QBER}) - \text{h}_2(\text{p}_0)) - \text{N}_{\text{leakage}} - \text{N}_{\text{safety}} \tag{2.5}$$

where here the $h_2(p_0)$ term is the extra information leaked by the unequal *a priori* probabilities of Alice getting a 0 or 1. Note that the binary entropy function is symmetric so that it does not matter if I use $h_2(p_0)$ or $h_2(p_1)$ in Eq. 2.5. Computing the extra term for my experiment I find that as a first estimate I would have had to shrink the final key size by an additional 0.22% to compensate for the unequal *a priori* probabilities.

Table 2.2 also allows one to calculate an average observed visibility of 88.6% in the H/V basis and 91.7% in the +/- basis during the experiment. Normally one should see a higher visibility in the H/V basis, not the +/- basis (as evidenced by the local visibilities presented in Sec. 2.4.1). However, for the data presented here I had obviously set the fibre polarization correction to map H/V to +/- and vice versa for this experimental run. Nevertheless, it made no difference to the generation and security of the final key. Fig. 2.5 tracks the visibilities in the two bases throughout the experiment.

2.5.4 Cascade Error Correction Algorithm Performance

During the experiment, my modified implementation of the cascade algorithm used average block sizes of 16, 33, 67, 138, and 314 bits for the 5 passes it made over the sifted key data; revealing an average of 174 bits/s. After error correction, the error corrected key had an average of 1.92×10^{-3} residual errors per bit with 8,150 errorless blocks from a total of 9,564 blocks. The somewhat high residual error rate was due to a number of reasons. Simplifications were made in my implementation of the cascade error correction algorithm; namely, rather than going back through all previous passes of cascade the algorithm instead only went back to the first pass. This reduced the effectiveness of my error correction algorithm; however, this was not the dominant source of error since it has been shown that two passes of cascade are usually enough to remove the majority of errors between two bit strings [150]. The dominant source of residual error was due to using the error rate estimate, performed by publically revealing 10% of the sifted key, in order to determine the proper block size for the cascade algorithm. The relatively small sample sizes caused large statistical fluctuations in the error rate estimate leading to a poor choice of the block sizes used in cascade. Improper block sizes in cascade can strongly reduce its effectiveness and were the major source of error in my error correction algorithm. Also,

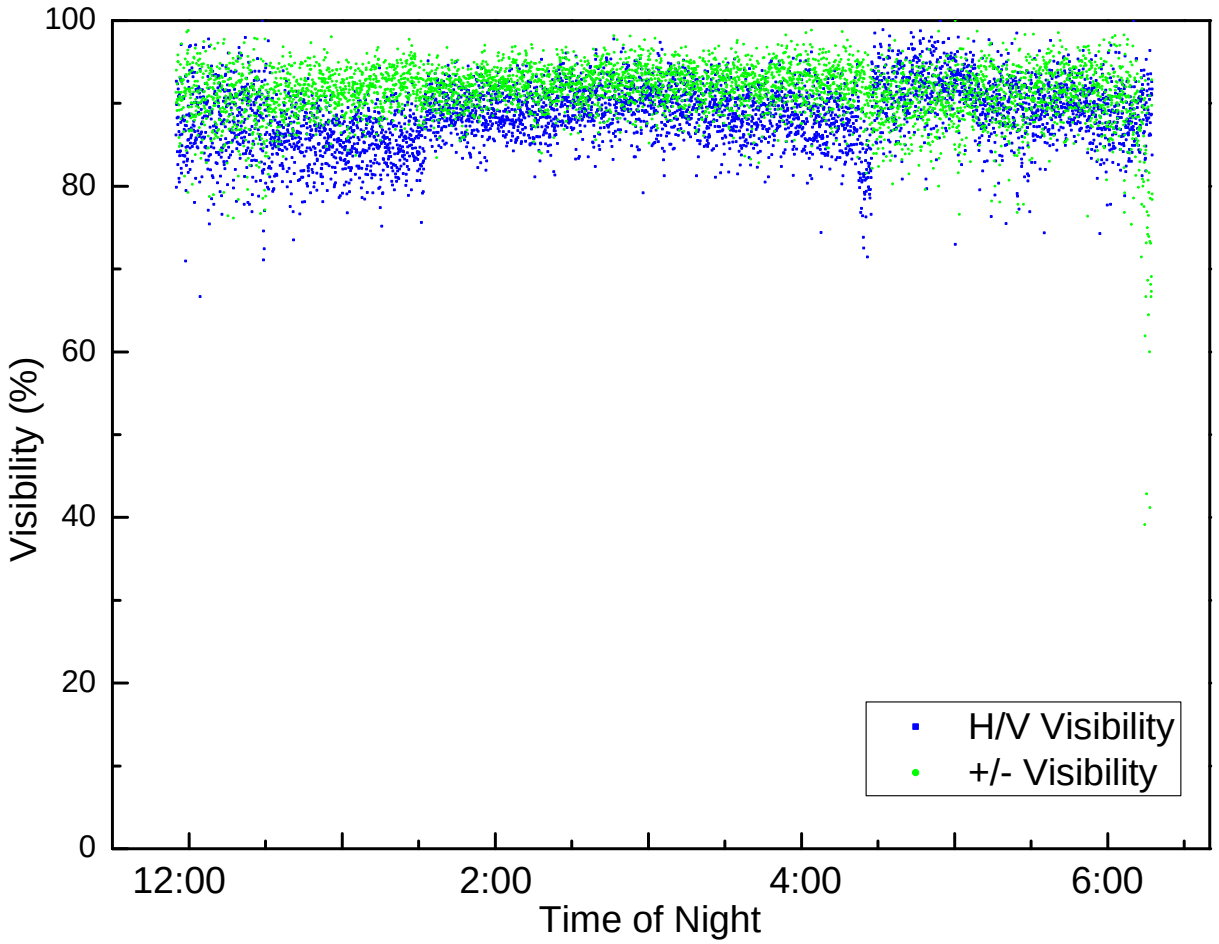

Figure 2.5: The visibility of the source in the rectilinear (H/V) basis shown in blue and diagonal basis ($+45°/-45°$) shown in green over the course of the experiment. The average visibilities of the two bases recorded during the night were 88.6% and 91.7% respectively. The data taken on April 28, 2008.

cascade is optimized to work on blocks with errors spread uniformly throughout, in order to accomplish this the sifted key should be randomized before performing cascade on it.

To test the impact of the block size on the residual error rate I performed off-line tests by running the saved sifted key data through cascade only this time using either the error rate observed during error correction on the previous block of data or a running average error rate from the last few blocks of data. I saw a significant improvement in the observed residual error rates for the same sifted key data sets. Further, Sec. 3.1 will detail an experiment where cascade was properly implemented with efficient block sizes, sifted key randomization, and the optimizations discussed in Sugimoto *et al.* [150] and will show that the residual error rate can indeed be set to any desired level dependent upon the number of passes performed with the cascade subroutines. The fact that the error rate estimation was useless to optimize the block sizes for cascade should be noted and removes any lingering reasons to even estimate the error rate in the first place and waste 10% of the key. Theoretical protocols usually describe doing this in order to detect an eavesdropper; however, the error correction algorithm itself already yields the true error rate which can be used to test the security of the key. Thus, since the error rate estimation was clearly useless in optimizing the error correction algorithm, there is no reason to do an error rate estimation.

Table 2.3 shows the average classical communication load in bytes per second during the experiment for the coincidence routine (timetag info sent, coincident index list received), error rate estimation (10% of the measurement results sent, estimate of the error rate received), and error correction (parity bits sent, index of corrected bit received) from Alice's side. In this first implementation I only made a minimal attempt at optimizing the classical communication load; for example, I sent individual parity bits as a full byte of data. The majority of the communication load was due to sending the timetag information necessary to identify coincident detection events corresponding to the detection of entangled photon pairs. Efforts can be made to ensure that the observer with the lowest detection rates is the one to send the timetag data across. Additionally, compression algorithms can be investigated to be used on the timetag information however their usefulness might be limited since the timetag data is random and does not show any patterns. Usually compression algorithms exploit patterns in the data in order to compress it. Beyond these

ideas there is not much that can be done to lower the communication load for coincident detection and it will remain the dominant classical communication load in any system that uses timing information to identify entangled photon pairs.

Alice					
Coincidence routine		Error rate estimation		Error correction	
sent (timetag info)	received (coin index list)	sent	received	sent	received
252,000	9,515	233	8	724	714

Table 2.3: The classical communication load (presented in bytes/s) for the different classical communication tasks performed by the QKD software in order to perform the BBM92 protocol.

2.5.5 Summary of Additional Experiments

Leading up to the main double free-space link experiment detailed above, I performed additional experiments with the following combinations of free-space links: a system with completely local detection (used to gauge a baseline for the detection and error rates of the system), one 435 m free-space link and local detection, two 435 m free-space links to adjacent offices in the IQC building, one 1.325 km link to PI and local detection, a second night's worth of data for the full two link system with one 435 m and one 1.325 km free-space link, and the two link experiment I have been describing so far. The data for each experiment is summarized in Table 2.4. From the table it is clear that the wildly varying free-space link to PI cut down the raw detection rates significantly, whereas the more stable BFG link showed higher rates. The QBER varied from experiment to experiment depending on how well I was able to align the bases between the source and receiver locations and compensate for the random polarization rotation induced by the long singlemode fibres used to carry the photons to the sender telescopes.

Lastly, a proof-of-principle Bell inequality violation experiment [16, 35] was performed just before the QKD experiment explained in detail above. Over the course of half an hour of data collection I was able to measure an average Bell parameter of 2.51 ± 0.11, almost 5 standard deviations above the classical limit of 2.

Situation	Key Rates (bits/s)				
	Raw	Sifted	Optimal Final	Actual Final	QBER
Local System	6,025	3,052	1,894	-	2.91%
1 435m BFG link	2,812	1,402	656	-	4.55%
2 435m BFG links	1,170	582	177	100	6.58%
1 1.35km PI link	1,398	714	334	244	4.58%
435m BFG & 1.35km PI links #1	857	425	86	34	7.98%
435m BFG & 1.35km PI links #2	565	284	124	85	4.92%

Table 2.4: The data from a variety of QKD experiments with different experimental free-space link setups.

2.6 Conclusion

In conclusion of this chapter, I have detailed the experimental implementation of the first real-time two free-space link entangled quantum key distribution system including all error correction and privacy amplification algorithms. The experiment spanned a distance of 1,525 m with no direct line of sight between Alice and Bob. The source was placed between Alice and Bob with line of sight to each one and took advantage of the fact that in an entanglement based scheme the source need not be in a trusted location. The system implemented the BBM92 protocol and sent pairs of entangled photons over two separate free-space optical links to be detected by Alice and Bob and turned into a secure key. Custom software was written to extract entangled photon detection events using a coincidence detection algorithm rather than relying on timing information from a separate classical channel. Over the course of more than six hours of continuous night time operation the system generated an average raw key rate of 565 bits/s, sifted key rate of 284 bits/s, and final secure key rate of 85 bits/s while observing an average QBER of 4.92%.

Chapter 3

Improving the Performance of the Free-Space QKD System

Following the work from the last chapter, part of the focus for my PhD turned to improving and optimizing the key rates for the QKD system detailed in Ch. 2. While the completion of the first implementation of a real-time two free-space link entangled QKD system represented a nice step forward in QKD research, it is clear that a QKD system with a secret key rate of 85 bits/s is of little practical interest. Consequently, I then attempted to improve the system in three different ways, involving each of the major disciplines comprising the system: measurement hardware, source technology, and software post-processing.

This chapter begins with a description of the first improvement made at the measurement hardware level, for this I implemented the idea of Lo *et al.*[92] to use a biased basis choice in Alice and Bob's polarization analysis modules allowing them to increase the chances of randomly measuring in the same basis from 50% to asymptotically approaching 100% (Sec. 3.1). The experiment investigated the security of such an idea and the efficiency gains from its implementation. There are three main reasons why this work is important: it was one of the first attempts made at a security analysis for the biased scheme taking into account finite statistics; also, since biased non-polarizing beamsplitters are difficult and expensive to make, an analysis for the optimal biasing under real experimental conditions is critical; and lastly, while the biasing idea works in theory, there are a number of ques-

tions about the actual efficiency improvement one can expect that can only be answered by studying a real world implementation. As a further consequence of the experiment, an optimization of the Cascade algorithm was also implemented and studied (Sec. 3.1.4).

The second improvement made was at the source hardware level and involved the development of a second generation source of entangled photon pairs, using the idea of a Sagnac interferometric loop, with a higher entangled photon pair production rate and improved visibilities translating into a lower QBER (Sec. 3.2). While the first investigations by Kim *et al.*[77] followed by the optimizations of Fedrizzi *et al.*[54] were crucial in establishing this type of source as a viable candidate for use in a QKD system, many of their figures of merit were studied and stated in such a way as to make them as attractive as possible. It was very important to study the use of such a source in a QKD implementation operating in a realistic parameter regime in order to fully characterize and evaluate its potential. In addition to improving the QKD system, the construction of a second generation source was also mandatory if I wanted to implement the oblivious transfer protocols described in Ch. 4. While I was very excited to be the first to implement some of these protocols, they had much more stringent requirements on the allowable QBER in order to maintain security making the development and investigation of this new source doubly important.

Finally, with the applications of satellite QKD alluded to in the previous chapter at the forefront of my mind, the last improvement was to study the free-space link transmission efficiency statistics more carefully (Sec. 3.3.2) and to investigate the use of a signal-to-noise ratio filter implemented in the classical post-processing in order to improve the overall final secret key rate (Sec. 3.3.3). The free-space link transmission efficiency probability distribution has a profound effect when evaluating the potential for any satellite QKD mission and with such limited time windows for transmission it is important to evaluate any ideas that have the potential to increase the yield of secret key for a fixed number of sent signals. This is also true of the biased basis experiment.

3.1 Entangled Quantum Key Distribution with a Biased Basis Choice

The idea of Lo *et al.* [92], to bias the basis choice in QKD, had been around since 1998 before finally being published in 2005. In their paper, Lo *et al.* examined a key feature of the BB84 protocol [19] (the idea also applies to the BBM92 protocol [21] used in my system and many others); namely, that the bases used are chosen randomly, independently, and uniformly. Most security proofs, including the seminal work by Shor and Preskill [149], have so far relied heavily on the symmetry which a uniformity of basis choice provides. For example, it allowed the sifted data from both bases to be grouped together, a simple error correction algorithm to be performed on the grouped data producing a single error rate, and for the phase error rate to be inferred from the bit error rate. However, uniformly chosen bases have the consequence that on average half of the raw data is rejected leading to an efficiency limited to at most 50%. This is the reason for the curious factor of $\frac{1}{2}$ that appears in the key rates of many security proofs [95, 97].

However, what Lo *et al.* discovered was that it is possible to remove this symmetry requirement and in principle asymptotically approach an efficiency of 100%. Their scheme relied on two changes to the BB84 protocol: non-uniformity in the choice of bases, and a refined data analysis. The first change of non-uniformity in the basis choice is what allows Alice and Bob to achieve much higher efficiencies with their raw data. In fact, Lo *et al.* showed that this efficiency could be made arbitrarily close to 100% in the long key limit. The second change of a refined data analysis allows Alice and Bob to maintain the security of their system since a simple error analysis is no longer sufficient.

In the following sections, I begin by detailing one of the first security analyses of the biased scheme for the finite key limit case (Sec. 3.1.1). Many theoretical articles have assumed that the biasing idea can be used to improve their key rates; however, there have been few studies examining the practical usefulness of the idea particularly for the real life scenario where one has a finite key. For example, it is important to know whether such a scheme would be useful in future satellite QKD experiments where the key is potentially quite short. Indeed, whether it remains a useful idea in realistic experimental settings or

whether other experimental deficiencies prevent it from being a truly useful, practical idea was one of the aims of this work.

Following the security analysis, the experimental implementation used to study the idea is then given (Sec. 3.1.2). The experiment used a local entangled QKD system and a simulated variable non-polarizing beamsplitter to alter the biasing of the basis choice in order to allow me to study the efficiency gains for the protocol in a real life setting. While using a simulated beamsplitter is less than ideal, it is precisely because of the fact that reliable variable non-polarizing beamsplitters do not exist coupled with the lack of knowledge of the optimal parameters for an experimental implementation of the biasing idea which make this work important to the QKD community. Fixed, non-polarizing, biased beamsplitters are difficult and expensive to make. By studying the optimal biasing ratio and the effect of the different parameters on the security of the system, I was able to learn which parameters were important and make informed recommendations for future improvements to the QKD system.

Lastly, I report on the results of the experiment and compare the efficiency of the biased protocol with those of an unbiased protocol (Sec. 3.1.3). Already one result, while obvious, has important practical consequences for both a biased and an unbiased QKD system. Namely, one needs to wait until the entire raw key is exchanged before it can used. In the case of an unbiased QKD system this has already been realized since the privacy amplification step needs to act on the whole key. However, the reasons for this go further in a biased system because the security argument is so finely balanced that it is not until the final raw key bit is exchanged that the users have enough information about the error rates in both bases to legitimately claim security for their key distribution. Also, the perfection of my error correction algorithm, necessary for the proper implementation and comparison of the biasing idea, was the first implementation of the optimized Cascade algorithm developed by Sugimoto and Yamazako [150] in a real QKD system. As error correction algorithms have an important practical effect on the efficiency of real key generation, I report on the improvements over the original Cascade algorithm[29]. The results of this work were published in Ref. [51] ().

3.1.1 Theory of Security

It is important to realize that the original paper by Lo *et al.*[92] was primarily concerned with proving the security of their biased scheme under the assumptions of the long key limit. Mostly their work consisted of re-writing the QKD security proof of Shor and Preskill[149] only this time incorporating their idea of a biased basis choice. While this was indeed an important step to show that their idea was viable and secure, it did not offer a proof of security for a realistic implementation of the idea where one would end up with a finite key nor did it offer a prescription for how an experimentalist would go about doing such a thing. Thus, one of the first contributions of this work was to provide a proof of security for the biased protocol using an analysis that took into account the finiteness of the generated key. While the finite key analysis I performed was admittedly a rudimentary first attempt at a security proof, it did take care of the parameters having the largest effect on security. Further, even though more refined methods are now available for analyzing security in the finite key limit, the security of QKD in the finite key limit is still an active area of research without a complete solution.

The security analysis I now describe follows from some initial work by my colleague, Xiongfeng Ma. Xiongfeng aided me in the initial setup and definition of the problem as well as contributed some initial Matlab code based on Ref. [97]. He also pointed out Ref. [97] as a reference for the random sampling theory used to analyze the main effect of the finite statistics. I also benefitted from useful discussions with Prof. Norbert Lütkenhaus primarily concerning some of the different finite statistics effects. Lastly, I had a number of helpful discussions with R. Kaltenbaek, T. Moroder, H. Hasseler, and O. Moussa while completing this project. Apart from this initial help, I was the sole contributor to this work.

Lo *et al.* [92] proposed their protocol as a modification to the original BB84 protocol [19] which is a prepare-and-measure scheme. As a first step in the security analysis, I made the simple extension to the entanglement based BBM92 scheme employed in my system which I am allowed to do since the proof by Lo *et al.* already relied on expanding the BB84 scheme into an imagined entanglement based scheme. Additionally, I use the recently developed squashing model [15, 154, 79] which allows me to assume that I am

dealing with qubits so that the proof by Lo *et al.* holds (double clicks are assigned a random choice within the detector time jitter, discussed in Sec. 2.2, as required for the squashing model).

The biased basis scheme has two main changes: first, Alice and Bob now choose their measurement bases randomly and independently but non-uniformly with substantially different probabilities. This is what allows for a much higher probability for coincident basis detection and consequently higher secret key generation efficiencies with the same amount of raw data. With uniformity removed, the second change necessary is a refined error analysis since an eavesdropper could now easily break a system which performed a simple error analysis on the lumped data by eavesdropping primarily along the predominant basis. To ensure security, it is crucial for Alice and Bob to divide their data into two subsets according to the bases used and compute an error rate for each subset separately. It is only with this second addition that I can ensure the security of this biased scheme.

I begin by establishing the necessary quantities that we will use in the security analysis. I define e_{bx} (δ_{px}) and e_{bz} (δ_{pz}) to be the bit (phase) error rates in the X (diagonal) and Z (rectilinear) bases respectively, where an e is used to denote a measurable quantity and a δ is used to denote a quantity that has to be inferred. Note that the bit error rates, e_{bx} and e_{bz}, are known exactly by Alice and Bob once they perform error correction since they can count the number of errors found during error correction. However, the phase error rates, δ_{px} and δ_{pz}, need to be estimated from the bit error rates since they are not directly accessible from Alice and Bob's measurement data.

In order to estimate the phase error rates, the quantities p_{bx} (p_{px}) and p_{bz} (p_{pz}) are defined to be the bit (phase) error probabilities in the X and Z bases respectively. Since a basis independent source and basis independent errors are assumed, we know that

$$p_{pz} = p_{bx} \qquad p_{px} = p_{bz}. \tag{3.1}$$

Now in the long key limit e_{bx} will converge to p_{bx} while δ_{pz} converges to p_{pz}. Using Eq. 3.1 now allows me to say that

$$\delta_{px} = e_{bz} \qquad \delta_{pz} = e_{bx} \tag{3.2}$$

in the long key limit. Obviously for finite key lengths this equality will no longer hold

exactly and we will have to consider statistical fluctuations. I will address the finite key size effects in a moment, but for now assume that Eq. 3.2 holds.

The key point of the security analysis rests in the privacy amplification part [20], which I perform in my system with the usual 2-universal hash functions discovered by Wegman and Carter [33][1]. Alice and Bob need to take care of the bits that are potentially exposed to an eavesdropper during error correction over the classical channel. They also need to estimate the phase error rates for the two bases in order to estimate the amount of an eavesdropper's information on the quantum signals that were distributed. Privacy amplification is then applied to reduce the information of any potential eavesdropper from these two sources to an arbitrarily small amount. This leads to the following key generation rate according to Ref. [97], expressed in terms of secure bits per raw bit, and using Eq. 3.2 above we have

$$\begin{aligned} R &\geq (1-q)^2[1 - f(e_{bx})h_2(e_{bx}) - h_2(\delta_{px})] \\ &\quad +q^2[1 - f(e_{bz})h_2(e_{bz}) - h_2(\delta_{pz})] \\ &\geq (1-q)^2[1 - f(e_{bx})h_2(e_{bx}) - h_2(e_{bz})] \\ &\quad +q^2[1 - f(e_{bz})h_2(e_{bz}) - h_2(e_{bx})] \end{aligned} \tag{3.3}$$

where q is defined to be Alice or Bob's (biased) probability of measuring in the Z basis and $(1-q)$ is their probability of measuring in the X basis, $f(x)$ is the error correction inefficiency as a function of the error rate (normally $f(x) \geq 1$ with $f(x) = 1$ at the Shannon limit), and $h_2(x) = -x \log x - (1-x)\log(1-x)$ is the binary entropy function. For this initial analysis, the key rate formula assumes that Alice and Bob each pick the same identical bias.

[1]It is important to note that my implementation of the 2-universal hash functions operates sequentially on blocks of 1022 bits of error corrected key, rather than on the whole key at once. While it has been known for some time, it has only recently been emphasized that to maintain security in QKD, an implementation must perform privacy amplification on the *entire* error corrected key of 10^6 bits or more. It should be noted that currently *no* experimental or commercial QKD systems meet this security requirement for their implementation of privacy amplification [2]; however, it was recently pointed out to me that an algorithm by Krawczyk [83] does exist which is capable of efficiently hashing large quantities of key at once. Any future experiments and implementations of QKD should make use of this algorithm for privacy amplificaiton.

Apart from having to separate the error correction for each basis in order to perform a refined error analysis, I also benefit from separating the key rate into contributions from the X and Z bases since the key rate can still be positive for an error rate higher than 11% in one basis so long as the other error rate is low enough. This can be seen in Fig. 2 of Ref. [98], which analyzed key rates for the case of decoy state QKD, since I am using local operations and one way classical communication (1-LOCC) in my post-processing. Note that the cascade error correction algorithm, which I use, is considered 1-LOCC post-processing since the two way classical communication is not used to perform advantage distillation. Also note that in this treatment of Cascade I assume that Eve learns both the positions of the errors and the revealed parity bits.

Finite Size Effects

With the secure key rate and the parameters affecting it properly introduced, the last thing to take care of are the finite key size effects since these will be very important in determining how to balance the optimal biasing ratio. For this analysis I assume the main finite key size effect is due to parameter estimation; namely, the possible statistical fluctuations on the phase error rates which are estimated from the bit error rates. There are other possible finite key size effects including: authentication, the leakage of information during error correction, the probability of failure for error correction and error verification, and the probability of failure of privacy amplification [135, 32]. However, as the following discussion shows, their effect can be assumed to be negligible when compared to parameter estimation.

For my system the probability of failure for parameter estimation is on the order of 10^{-6} since, as I discuss below, I can choose a safety margin on my phase error estimates so that the probability that the actual phase error rates lie outside this range is less than 10^{-6}. Also, I do not implement authentication on the classical channel (for the reasons described in Sec. 2.2), so I ignore its effect on the key rate[2]. The information leaked during error correction does not contribute any finite key size effects since the exact number of

[2]Note though that the resources required for authentication scale logarithmically in the length of the secret key generated by a QKD session [6].

bits exposed are directly counted during error correction and taken care of in the privacy amplification step [94]. The error correction and verification algorithm I implemented is that of Sugimoto and Yamazaki [150] which allows me to bound the failure probability and thus set its value. For this experiment, I set the probability of failure for the error correction algorithm to $< 10^{-10}$. Lastly, the probability of failure for the privacy amplification step is assumed to be negligible since it depends on the privacy amplification algorithm used and it is assumed that ones with a suitably small failure probability are available. While this analysis is not a final security proof, it does suffice to establish parameter estimation as the main contributor to the finite size effects. The security of QKD incorporating finite statistics is an active area of research, further suggestions for incorporating a stricter finite key analysis can be found in Refs. [67, 134, 135, 32].

With parameter estimation established as the main contributor to finite size effects, I need to consider the statistical fluctuations on the parameter estimation in order to discuss the optimal bias between the two bases. As was stated above, both error rates e_{bx} and δ_{pz} converge to $p_{bx} = p_{pz}$ in the long key limit; however, this is no longer valid in the finite key limit. Instead, standard random sampling theory can be used to determine the following formula [97] for the estimates of my phase error rates[3]

$$\begin{aligned} P_{\epsilon_z} &\equiv \text{Prob}\{\delta_{pz} > e_{bx} + \epsilon_z\} \\ &\leq \exp[-\frac{\epsilon_z^2 n_{xx}}{4e_{bx}(1-e_{bx})}], \end{aligned} \tag{3.4}$$

where n_{xx} is the number of bits generated from Alice and Bob both measuring in the X basis, and ϵ_z is a small deviation from the measured bit error rate[4]. Eq. 3.4 allows me to put a bound on the probability that the phase error rate deviates from my measured bit

[3]Technically, the random sampling formula used in Eq. 3.4 from Ref. [97] is only correct in the long key limit; however, as stated by the authors it suffices as a first approximation for the fluctuations in the finite key limit.

[4]For example, if Alice and Bob measure 10,000 qubits in the X basis ($n_{xx} = 10,000$), find an error rate of 5% ($e_{bx} = 0.05$), and set their desired deviation to 1% ($\epsilon_z = 0.01$), then Eq. 3.4 would allow them to say that the probability that their phase error rate (δ_{pz}) deviates by more than ϵ_z is less than 0.52%. Or said another way, if I use $\delta_{pz} = 0.06$ in my key rate formula then I am confident that my key was generated securely with a probability of 99.48%.

error rate by more than ϵ_z and thus allows me to make use of Eq. 3.1 so long as I also include ϵ_z. With this addition, my key rate formula becomes

$$\begin{aligned} R \;\geq\; & (1-q)^2[1 - f(e_{bx})h_2(e_{bx}) - h_2(e_{bz} + \epsilon_x)] \\ & + q^2[1 - f(e_{bz})h_2(e_{bz}) - h_2(e_{bx} + \epsilon_z)], \end{aligned} \tag{3.5}$$

which is the same as before except for the addition of ϵ_x and ϵ_z which are now necessary to deal with the finite key statistics.

With this analysis finished, we can now try to find the optimal bias between the two bases. Given estimates for e_{bx}, e_{bz}, and N (the total coincidence count), and picking $P_\epsilon = P_{\epsilon_x} + P_{\epsilon_z} = 10^{-6}$, I can optimize the deviations ϵ_x and ϵ_z according to Eq. 3.4 to achieve my desired confidence probability. Then, using these values and my estimated parameters, I can graph the key rate (normalized in terms of secure key bits per raw key bit) versus the bias ratio q as shown in Fig. 3.1. The inset shows the estimates for the parameters needed in order to find the optimum bias: N is the total number of entangled pairs sent to Alice and Bob over the course of the experiment, P_ϵ is the confidence probability desired for my phase error statistics, e_{bx} and e_{bz} are the estimated bit error rates in the X and Z bases, and f is the observed error correction efficiencies for key generated in the X and Z bases Fig. 3.1 shows that the key rate is maximized for a bias of $q = 0.97$.

Examining Fig. 3.1 one can see that a maximum also occurs around $q = 0.03$ though it is slightly lower than the one at $q = 0.97$. At first sight, it seems obvious that the efficiency curve should be symmetric about the middle point $q = 0.5$. However, the curve is not entirely symmetric because the error rates and consequently the error correction efficiencies are not identical in the two bases. The error correction efficiency plays the largest part in the overall rate since it costs a fraction of $f(e)h(e)$ in the final key generation rate. Thus, since error correction costs more in the X basis than the Z basis ($f_X > f_Z$) because the error rate is higher in the X basis ($e_{bx} > e_{bz}$), the optimum rate is also lower when the bias is skewed towards the X basis (ie. $q < 0.5$). This is an important result of this work since it has practical consequences for any real QKD implementations that want to use the biasing idea but is typically is not examined in theoretical papers.

As a last comment, it is important to understand how the biased protocol utilizes the optimum bias in order to make the most efficient use of the raw key data. The optimum

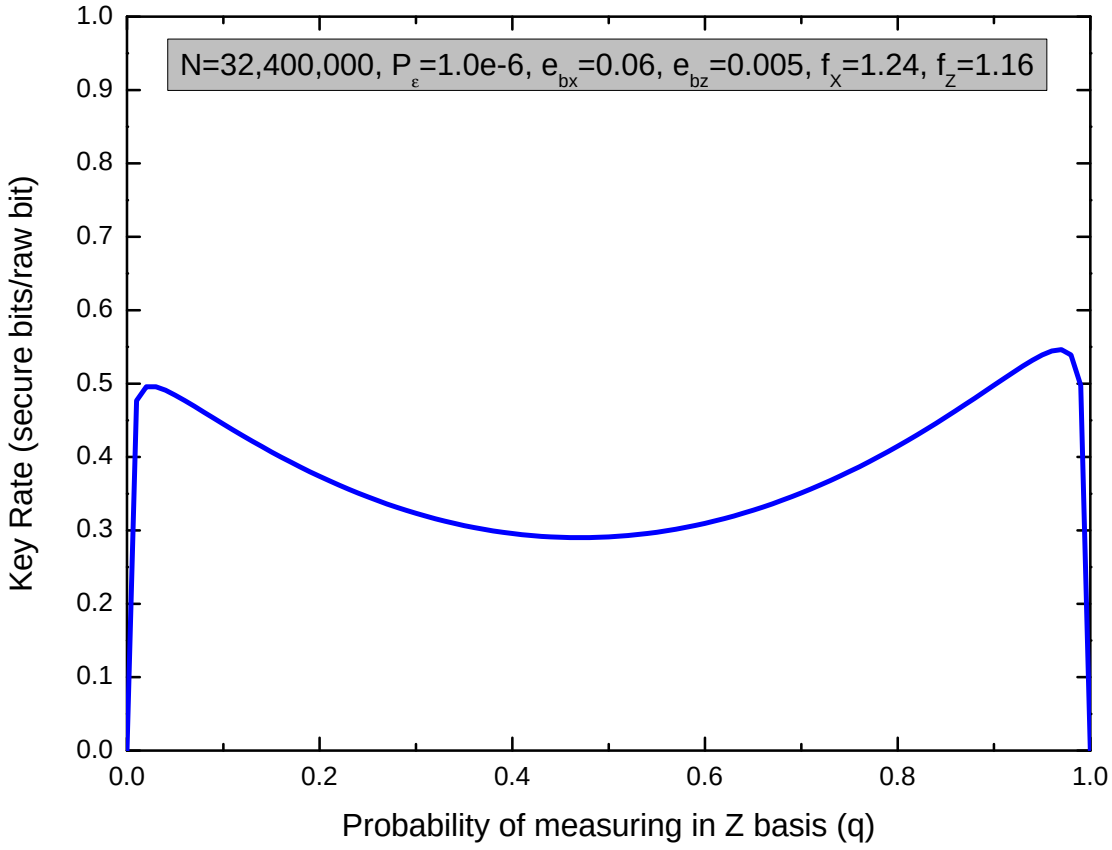

Figure 3.1: Plot of the key generation rate (R) in terms of the bias ratio (q).

bias, q, along with the optimum deviations, ϵ_x and ϵ_z, are chosen such that only the minimum number of measurements are made in the weak basis in order to achieve the desired confidence probability P_ϵ. This has the consequence that privacy amplification of the measurement results from the strong basis has to be deferred until the end of the entangled photon distribution phase. It is only with the last distributed photon that Alice and Bob gain enough statistics in the weak basis to allow them to privacy amplify all of the error corrected key generated in the strong basis over the course of the experiment. They will obtain small amounts of privacy amplified key from the weak basis over the course of the experiment, but the majority of the key that comes from the strong basis will not be

available until after the distribution phase is completed.

This is fundamentally different than in unbiased experiments. While in unbiased experiments privacy amplification still needs to be deferred until enough statistics are gathered to satisfy the finite key security arguments, one can still imagine it being a more real-time application by privacy amplifying key in chunks of sufficient size so that some secret key becomes useable during the entangled photon distribution phase. However, in the case of a biased experiment in order to make maximum use of the biasing idea one must *always* wait until the *end* of the entangled photon distribution phase before it becomes possible to use any of the secret key.

3.1.2 Implementation

The experimental implementation of the biased QKD experiment made use of the entangled QKD setup described in Sec. 2.4 with Alice and Bob locally measuring photons while sitting next to the source. As was mentioned before, reliable variable non-polarizing beamsplitters do not exist, and further fixed biased non-polarizing beamsplitters are difficult and expensive to make. One of the goals of this work was to study the optimal biasing ratio and the major parameters affecting the proper bias choice in order to layout a prescription for choosing the proper bias in future implementations. In order to do this, I simulated a variable biased beamsplitter in the following experiments. As a side comment, the difficulties associated with biased beamsplitters might suggest one possible reason for employing an active basis selection scheme (for instance, using Pockels' cells) over a passive one since biasing might be done more easily. However, the active schemes would have their own complications for generating truly random, biased bit strings at a high enough rate for their polarization modulators. As one final comment, I mention the recent work by Ma *et al.*[99] which included details of a fibre-based tunable directional coupler (TDC) (in essence, a variable beamsplitter). Their TDC worked by changing the separation between two fibres and thus the evanescent coupling between the light fields in each fibre and was able to achieve modulating visibilities (or Michelson visibilities, ie. the experimentally measured contrast between setting it to a theoretical 0% and 100% transmission) above 95%. While this would have significantly degraded the key rates in my experiment, possibly nullifying

any advantage gained from biasing, refining this idea is one possibility for implementing a variable beamsplitter in a future biased QKD system.

In order to implement the biased protocol I simulated a biased beamsplitter by placing the appropriate attenuators in the transmission arm of the original 50/50 beamsplitter (BS) (see Fig. 2.2) used to perform the basis choice in the polarization analysis module as shown in Fig. 3.2. Also, in order to directly compare the efficiencies of experiments with different

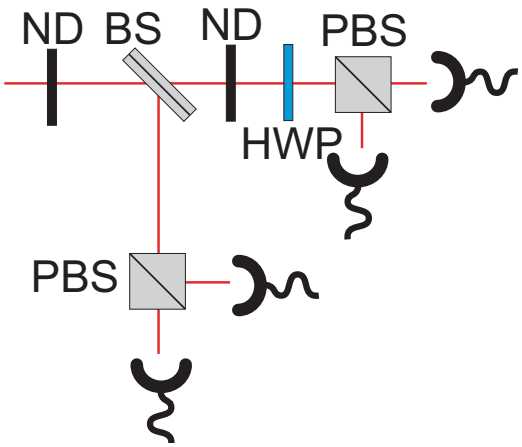

Figure 3.2: Schematic of the polarization analysis module with a neutral density (ND) filter placed in the transmission arm of the 50/50 beamsplitter (BS) in order to achieve the desired bias in the measurement results. (Polarizing beamsplitters (PBS), half waveplate (HWP))

biases I used additional attenuators ahead of the beamsplitter to make the rates of each experiment with a different bias equal. The attenuators were placed in the transmission arm (X, diagonal basis) so that the Z (rectilinear) basis was the one which Alice and Bob predominantly measured in. As was mentioned earlier, I make this choice because error correction costs a factor of $f(e)h(e)$ (with $f(e) > 1$) while privacy amplification only costs a factor of $h(e)$ in the key generation rate. Thus, since the Z (rectilinear) basis has a much lower intrinsic error rate, I would like to make it the predominant basis since less error correction is needed than if I were to choose the X (diagonal) basis as the predominant one.

My custom written software, discussed in Sec. 2.4.4, needed to be modified in order to analyze the error rates in both bases separately and to defer the privacy amplification until the end of the entangled pair distribution phase. Error correction was first performed on the X basis measurements followed by the Z basis measurements, revealing the bit error rates e_{bx} and e_{bz}. The number of bits revealed during the error correction of the X and Z measurements were recorded. After the distribution phase, I used the actual experimental results for N, n_{xx}, n_{zz}, q, e_{bx}, e_{bz}, $f(e_{bx})$, and $f(e_{bz})$, along with the desired P_{ϵ_x} and P_{ϵ_z} to calculate the optimum ϵ_x and ϵ_z according to Eq. 3.4. This allowed me to distill the maximum amount of key from my raw data. The appropriate privacy amplification factor, according to Eq. 3.5, was then calculated for each measurement set. Privacy amplification using a 2-universal hash function [22, 20, 33] then took care of the bits revealed during error correction, the estimated phase error rates, and the additional safety margin needed for the finite key statistics to produce the final secure key.

For this experiment I improved my error correction algorithm since knowing the bit error rates e_{bx} and e_{bz} as precisely as possible was extremely important. To do this, I replaced the initial modified Cascade error correction algorithm [18, 29] with the optimized Cascade algorithm put forth by Sugimoto and Yamazaki [150]. In previous experiments with my original modified cascade algorithm I had achieved a residual bit error rate of 1.92×10^{-3} [48], which was clearly insufficient for realistic key sizes especially with finite key size effects taken into account. In order to be secure, it has been shown that privacy amplification needs to work with key lengths on the order of $\sim 10^7$ bits [32]. Consequently, the probability of residual errors needs to be a least two orders of magnitude less than this in order for the privacy amplification to succeed with high probability. The beauty of the improved optimized Cascade algorithm is that it allowed me to set a parameter, s, which then bounded the residual bit error rate according to $P_{residual} < 2^{-s}$. For this experiment I chose $s = 40$ which gave me a maximum residual bit error rate of 9.09×10^{-13}. Such a simple lower bound formula for the residual error rate was not available for the original Cascade algorithm and further the number of iterations necessary in the original Cascade paper [29] was arbitrarily chosen.

3.1.3 Results

To give a baseline for the experiment, shortly before starting it I measured visibilities of 99.6% and 92.4% in the rectilinear and diagonal bases respectively corresponding to error rates in the two bases of $e_{bx} = 0.038$ and $e_{bz} = 0.002$. The limited visibility in the diagonal basis (high e_{bx}) was due to same reasons discussed in Sec. 2.4.1; namely, broad spectral filtering (10 nm) in the polarization analysis module and uncompensated transverse walk-off in the β-BBO crystal.

Exp	Bias (Z/X)		
#	Alice	Bob	Total
1	0.4570/0.5430	0.4752/0.5248	0.4343/0.5657
2	0.5660/0.4340	0.6074/0.3926	0.6639/0.3361
3	0.7398/0.2602	0.7606/0.2394	0.8938/0.1062
4	0.8804/0.1196	0.9062/0.0938	0.9837/0.0163

Table 3.1: The observed biases in each of the experiments.

I performed four different experiments with the biases shown in Table 3.1, each approximately six hours in duration in order to compare their efficiencies. While the appropriate attenuators were put into the transmission arms of both Alice and Bob's detectors to simulate the desired bias, differences in coupling efficiencies within the polarization analysis modules produced slightly asymmetric biases between Alice and Bob for the Z basis choice. In order to figure out the optimum ϵ's needed and the proper privacy amplification factor, the simple uniform bias analysis given above had to be expanded into a two dimensional analysis that allowed Alice and Bob to have non-identical biases. Fig. 3.3 is the generalization of Fig. 3.1 and plots the key rate (R) versus Alice's bias (shown along the left axis) versus Bob's bias (shown along the right axis). Using this analysis I proceeded to find the optimum ϵ's, calculate the privacy amplification factors, and complete the key generation process.

Fig. 3.4 shows the QBER's in the X and Z bases measured over the course of each experiment. The variation in the QBER estimates can clearly be seen to grow as the sample size shrinks with increasing bias. The average QBER's in the X and Z bases

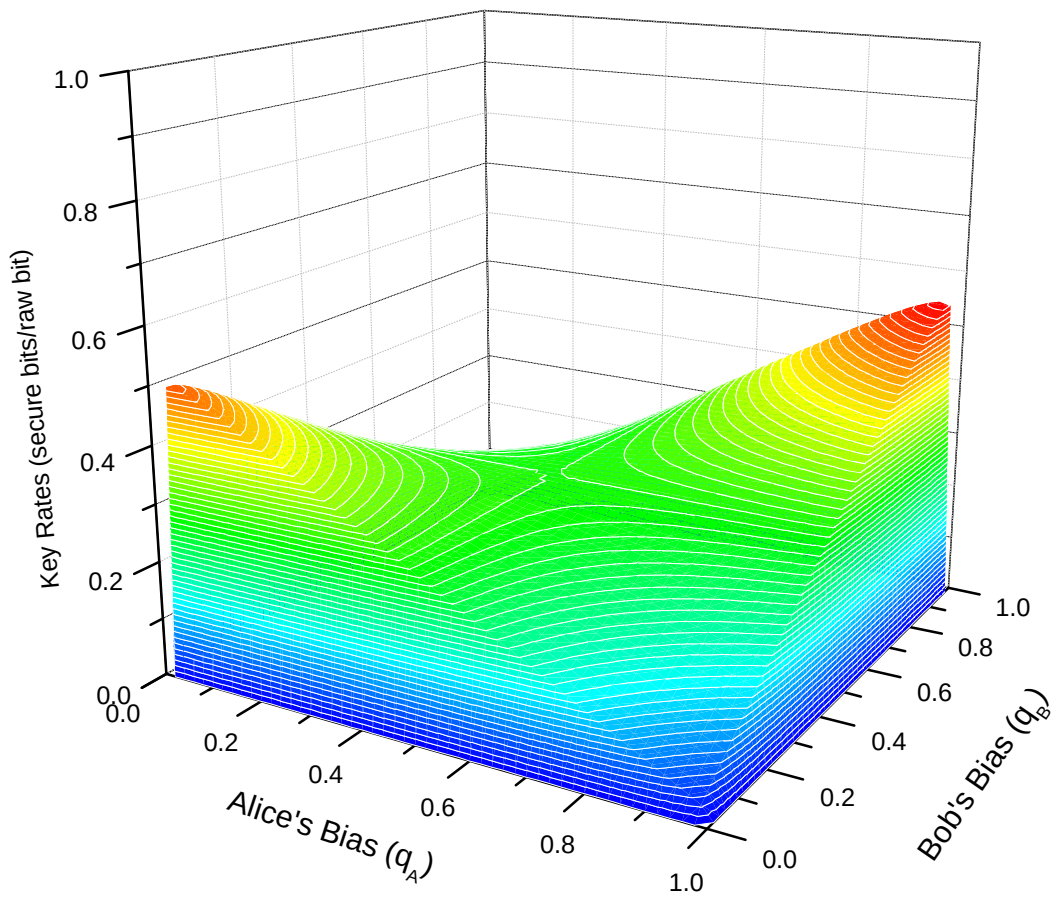

Figure 3.3: Plot of the key generation rate (R) in terms of Alice's bias ratio (q_A) and Bob's bias ratio (q_B). Alice's bias is plotted along the left axis while Bob's is plotted along the right.

for each experiment are tabulated in Table 3.2. The increase in the QBER's from the baseline 3.8% and 0.2% to those observed can be attributed to the typical leakage into the reflected arm of the polarizing beamsplitters in the polarization analysis modules, the uncompensated birefringence in the singlemode fiber used to transport the photons between the source and the polarization analysis modules, and to accidental coincidences.

Exp	QBER		Key Length			Secure Bits	Improvement
#	X	Z	Raw	Sifted	Final	Per Raw Bit	
1	1.39%	5.55%	28,655,075	14,779,423	7,365,984	0.2550	-
2	0.90%	5.76%	29,705,827	15,713,427	8,392,528	0.2825	1.11
3	0.89%	5.36%	29,319,830	18,627,251	10,568,944	0.3605	1.41
4	0.82%	5.80%	32,162,313	26,154,132	14,687,016	0.4567	1.79

Table 3.2: The QBERs and key rates for each of the biased experiments.

Fig. 3.5 shows the raw key rate, sifted key rate, and average final key rate over the course of each experiment. The statistics for each experiment are grouped by the same colour, the upper box holds the raw key rates, the middle box holds the sifted key rates, and the lower box holds the average final key rates for each experiment. Note that I can only show an average final key rate since, as was mentioned previously, privacy amplification has to be deferred until the end of the entangled photon distribution phase and error correction phase, and then is performed on the "entire" sifted key at once. The results of each experiment are summarized in Tab. 3.2 along with the efficiency as compared to the first experiment which I take as the "unbiased" experiment. As one expects, Table 3.2 clearly shows that the efficiency of each experiment increases as the bias increases, reaching a value of 0.4567 secure key bits per raw bit for the final experiment with the near optimum bias of 0.9837/0.0163. Thus, by implementing the biased QKD protocol I was able to increase the secure key generation rate by 79% over the unbiased case.

For each of the experiments, the raw key size was on the order of $\sim 10^7$ bits, which is what most satellite QKD experiments expect to generate for a single satellite pass [26]. Thus, this experiment is important in that it gives a rough upper bound for the improvement one can expect from the biased QKD idea if it were to be implemented on a satellite

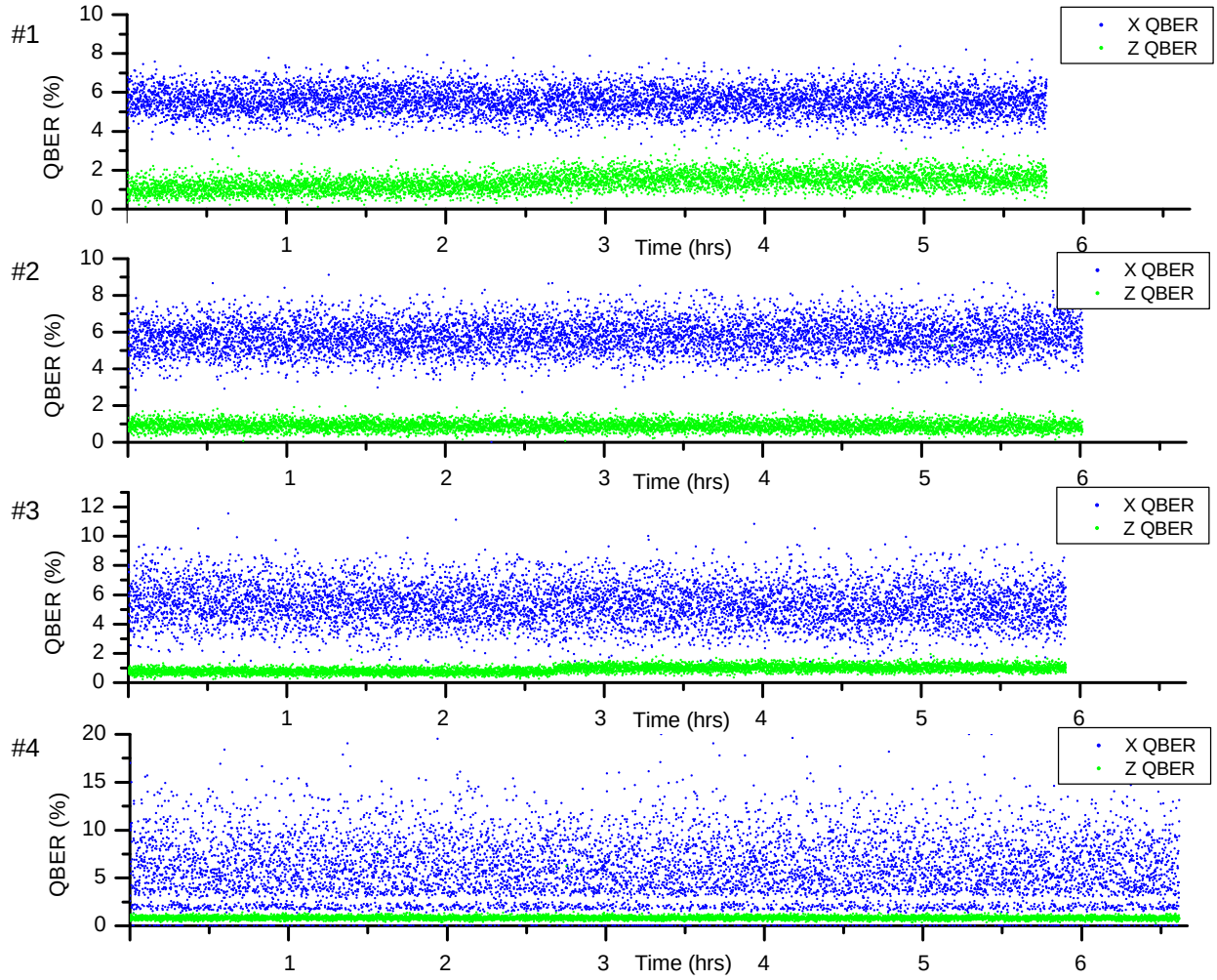

Figure 3.4: Plot of the QBER's in the X (blue) and Z (green) bases over the course of the experiments. The "line" in the blue dots of the bottom graph is likely due to the discreteness of the QBER becoming visible at this small sample size. Zooming in on the figure clearly shows a discrete banding of the QBER values.

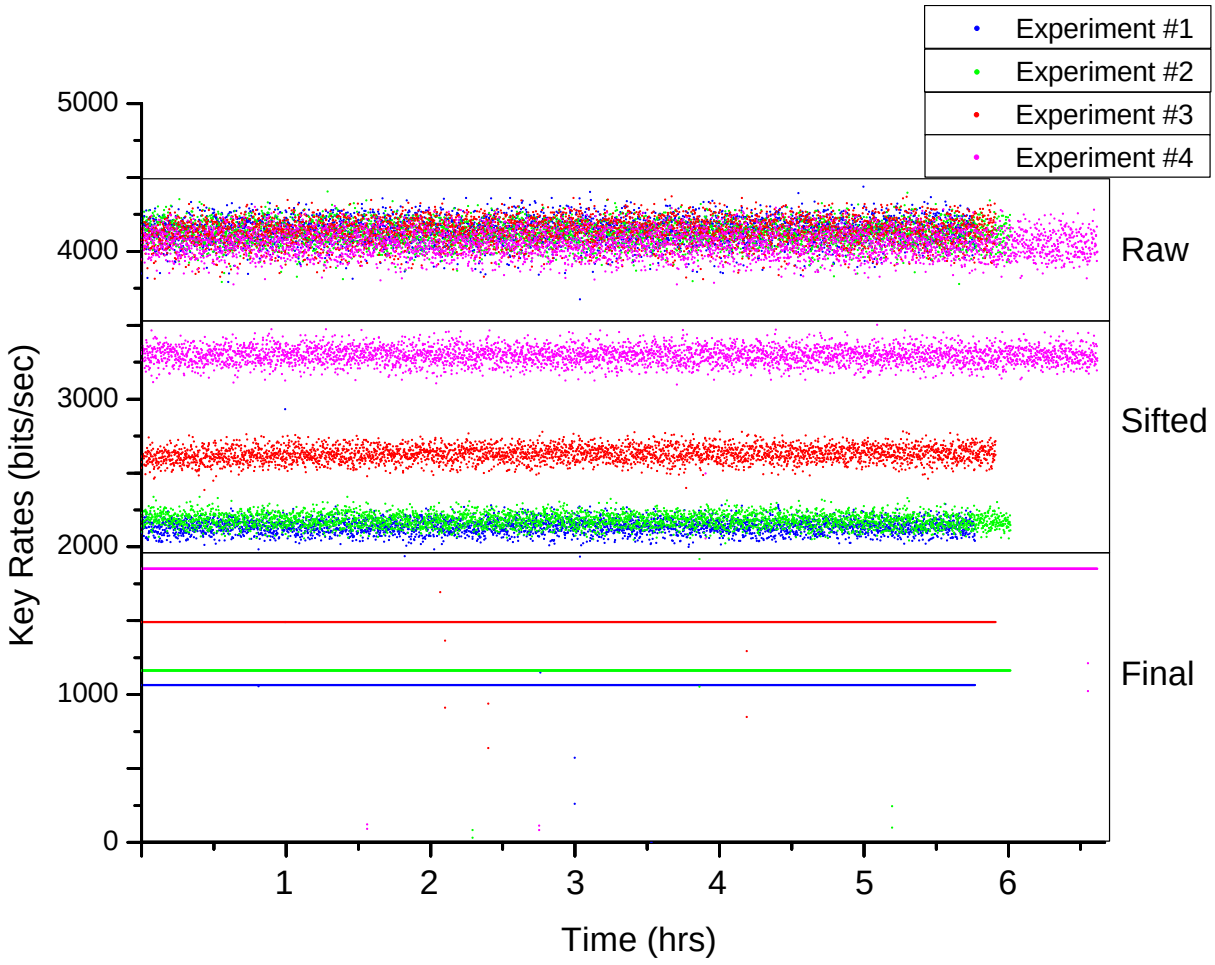

Figure 3.5: Plot of the raw, sifted, and average final key rates over the course of the experiment each experiment. The rates are grouped by colour with Experiment #1 in blue, Experiment #2 in green, Experiment #3 in red, and Experiment #4 in magenta. The upper box holds the raw key rates, the middle box holds the sifted key rates, and the lower box holds the average final key rates

QKD mission. Clearly, using a biased protocol for the generation of secure key bits for a satellite QKD mission would result in a more efficient use of the distributed entangled photon pairs and allow Alice and Bob to distill more secret key from the same amount of raw signals. However, the finite size effects would prevent it from reaching the 100% improvement that is theoretically possible. Only if the total number of distributed entangled photon pairs was increased would the number of sifted key bits per raw key bit approach 1.0 allowing for the most efficient generation of secure key. Also, as mentioned earlier, this work represents a first attempt at incorporating finite key statistics into the biased QKD scheme and already one can see that the improvement is not as drastic as Lo *et al.* originally indicated since I am only able to increase my key production by 79% rather than the full 100% improvement theoretically possible in the asymptotic limit. Thus, my work provides a strong motivation for further research into the effects of finite statistics on the biased basis QKD protocol in order to check whether the efficiency gains are degraded further by a more complete analysis.

3.1.4 Optimized Cascade Algorithm

Since the error correction algorithms (for a high level explanation of the operation of the Cascade algorithm, see Sec. 2.4.4) were greatly improved during this work, it is worthwhile to examine their performance. The error correction algorithms used were developed by Sugimoto and Yamazaki [150] as an optimization of the Cascade error correction algorithm developed by Brassard *et al.* [29] which was first mentioned in an earlier form in [18]. While cascade has proven to be the most popular choice for the error correction algorithm in many QKD experiments, many have noted that the two way communication required will introduce a significant latency into any system meant for commercial use covering a sizeable distance. Further, the programming will become quite complicated with many parallel threads running at once to error correct different blocks of key. Thus, there has been a move in the QKD community towards one-way error correction methods, such as low density parity check (LDPC) codes (discussed in Ch. 4), in order to remove this bottleneck. However, even though Cascade will likely not be the main error correction method used in future systems, it will still find uses as a secondary error correction algorithm. The

reason for this is that while Cascade will *always* find and correct an error, in one-way error correction schemes (like LDPC codes) there is a stopping condition at which point the code gives up trying to correct a block of key. After this, one either needs to try a different code or revert to a different error correction scheme, such as Cascade. Therefore, the analysis given below of the performance of the optimized Cascade algorithm operating in a real QKD system will still be useful for future implementations of QKD.

Tables 3.3, 3.4, and 3.5 give some of the important metrics for the operation of Cascade during experiment #1. Table 3.3 shows the average block sizes used during the error correction of the sifted X and Z keys, while Table 3.4 shows the number of errors corrected during each pass and sequence of Cascade. Each pass represents a particular random shuffling of the bits which are subsequently error corrected in the block sizes given in Table 3.3 using the BINARY primitive [29]. When an error is found, Cascade then goes back through all previous sequences of shufflings of bits to correct errors that were missed beforehand. Table 3.5 shows the average numbers of errors corrected during the use of the BINARY (used in the usual cascade implementation) and BICONF (added in the optimized cascade implementation) primitives [29] and the corresponding number of bits revealed. Additionally, it shows the average key block lengths and QBERs found during Cascade. Using these, the error correction efficiencies for my algorithm are calculated by comparing the actual number of bits revealed to the number of bits which an error correction algorithm operating at the Shannon limit would have revealed. These efficiencies are also shown at the bottom of Table 3.5.

	Pass 1	Pass 2	Pass 3
Average block sizes (X)	16	33	65
Average block sizes (Z)	72	144	289

Table 3.3: Cascade stats - average block sizes.

As was discussed above, the optimized cascade algorithm allows me to set the desired residual error rate via the parameter s which determines the rate according to $P_{residual} < 2^{-s}$. However, as the residual error rate requirements grow more stringent the efficiency of the error correction algorithm relative to the Shannon limit, $f(x)$, will begin to deteriorate.

	Totals	Sequence 1	Sequence 2	Sequence 3
Average number of errors corrected (X)				
Pass 1	31.4	31.4	-	-
Pass 2	27.2	13.6	13.6	-
Pass 3	7.1	2.7	1.1	3.3
Average number of errors corrected (Z)				
Pass 1	5.6	5.6	-	-
Pass 2	4.4	2.2	2.2	-
Pass 3	1.2	0.5	0.2	0.5

Table 3.4: Cascade stats - average number of errors corrected at each step in cascade.

	BINARY	BICONF	Total
Average number of errors corrected (X)	65.8	1.2	67.0
Average number of bits revealed (X)	437.5	53.3	490.8
Average number of errors corrected (Z)	11.2	1.7	12.9
Average number of bits revealed (Z)	98.2	57.6	155.8
	X	Z	
Average key block length	1,207.7	927.2	
Average QBER	5.4%	1.2%	
Error correction efficiency	1.31	1.59	

Table 3.5: Cascade stats - average number of errors corrected, bits revealed, error correction efficiencies, key block lengths, and QBERs.

For all experiments there were no residual errors left in the error corrected key after error correction was performed.

3.2 Development of a Brighter Sagnac Entangled Photon Source

Having demonstrated that the efficiency of the measurement hardware could be increased by properly biasing the measurement bases, I then moved on to improving the entangled photon source used in my system. While the original type-II non-collinear spontaneous parametric down-conversion source (see Sec. 2.4.1) was integral to the initial experiments detailed in Ch. 2 and in the biasing experiments detailed above in Sec. 3.1; it was limited both in its maximum photon pair production rate and the visibility of the entangled pairs in the two bases (H/V and $+/-$), all of which led to a low final secret key rate. Additionally, I had begun investigating how to implement an oblivious transfer protocol in the noisy storage model with my entangled QKD system (see Ch. 4 for more details) and one of the first requirements which my calculations showed was the need for a brighter source with a much lower error rate. Thus, in order to improve the key rate of the system, make it more practical in a real-world scenario, and allow me to experimentally investigate oblivious transfer I developed a second generation Sagnac entangled photon source capable of producing higher visibility entangled photon pairs at rates one to two orders of magnitude larger than my original source.

I begin this section by describing some of the background behind the most common implementation for entangled photon sources (Sec. 3.2.1) including a simple description of spontaneous parametric down-conversion (3.2.1) which is the physical mechanism used to create entangled photon pairs, and periodic poling (Sec. 3.2.1) which is a more recent technique matching the phase of the nonlinear interaction in a material that is responsible for the pair production. I then move on to the design of the source and a description of its operation (Sec. 3.2.2). Next I detail the different steps that must be followed in order to properly align the source and obtain the highest pair rates and visibilities in both bases (Sec. 3.2.3). Finally I close with a discussion of the performance metrics for the new

source (Sec. 3.2.4) and illustrate its improvements over my first generation source. This work resulted in the publication of Ref. [49] (© Springer Berlin Heidelberg 2010) in the conference proceedings for QuantumComm 2009.

During this work, I was the initial investigator of the source's design and ordered the necessary parts for the construction of two new Sagnac sources with helpful insights from Prof. Kevin Resch at the Institute for Quantum Computing in Waterloo, Canada and Prof. Gregor Weihs from the Institut für Experimentalphysik in Innsbruck, Austria. Following this, I worked on the setup of this new source in collaboration with Deny Hamel from the Institute for Quantum Computing in Waterloo, Canada. I benefitted from a number of the setup and optimization techniques developed by Deny over the course of the source construction and alignment.

3.2.1 Background

All of the experiments detailed in this thesis require the use of high quality polarization-entangled photon pairs. While there are other degrees-of-freedom one could use, such as the so-called time-bin encoding [153], the polarization of photons is particularly easy to manipulate and measure. Further, the quantum key distribution experiments outlined in Chs. 2 and 3 utilize free-space optical links in order to distribute the photons. Free-space links are used precisely because they do not have bi-refringence and thus do not influence the polarization of photons, making it the ideal degree-of-freedom to encode qubits in.

Spontaneous Parametric Down-Conversion

The most common method for producing polarization-entangled photon pairs is through the use of a process called spontaneous parametric down-conversion (SPDC) which relies on the $\chi^{(2)}$ optical non-linear susceptibility of certain media. In SPDC, a pump photon is split into two photons of lesser energy (called the signal and idler) via the interaction with the non-linear optical crystal. SPDC 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. SPDC is conventionally split into two different types: type-I refers

to the case when both down-converted photons have the same polarization, and type-II refers to the case when the emerging photon pairs are oppositely polarized.

The following treatment of the theory of down-conversion is due to Refs. [69, 116, 63, 130, 65] and some of the simplifications made therein[5]. The interaction Hamiltonian of a non-linear optical crystal is usually derived by starting from the classical electric field energy density for a non-linear medium and then quantizing the electric field in the usual manner producing the following equation

$$\hat{H} = \epsilon_0 \int_V d^3r \chi^{(2)} \hat{E}_p^{(+)} \hat{E}_s^{(-)} \hat{E}_i^{(-)} + H.C. \tag{3.6}$$

where ϵ_0 is the usual vacuum permittivity; $\chi^{(2)}$ is the optical non-linearity; $\hat{E}_p^{(+)}$, $\hat{E}_s^{(-)}$, and $\hat{E}_i^{(-)}$ are the electric fields of the pump, signal, and idler respectively; $H.C.$ is the hermitian conjugate; and the integral is performed over the volume, V, of the crystal.

The first simplification usually made is to treat the pump as a strong classical field that is for all intents and purposes negligibly affected by the down-conversion process (ie. the depletion of pump photons to create down-converted photons is negligible compared to the strong pump power). Doing so allows one to treat it as a classical monochromatic wave given by

$$\hat{E}_p^{(+)} = E_0 e^{i(\vec{k_p} \cdot \vec{r} - \omega_p t)} \tag{3.7}$$

where $\vec{k_p}$ is the momentum vector of the pump, $\vec{r}$ is the direction of propagation, and ω_p is the frequency of the pump. Additionally, Eq. 3.6 has made the assumption that only one element of the non-linear susceptibility tensor, $\chi^{(2)}$, contributes appreciably to the down-conversion process, which is typically true.

The next step is to look at the quantized electric field of the signal and idler photons which are given by

$$\hat{E}_j^{(-)} = -i \sum_k \sqrt{\frac{\hbar \omega_{k,j}}{2\epsilon_0 V}} \vec{\epsilon}_k \hat{a}_{k,j}^\dagger e^{-i(\vec{k_j} \cdot \vec{r} - \omega_{k,j} t)} \tag{3.8}$$

where $j = s, i$ stands for either the signal or idler field, the sum is taken over the different modes k, $\omega_{k,j}$ is the frequency of mode k for photon j, $\vec{\epsilon}_k$ is the unit polarization vector

[5]For a more complete treatment of SPDC please refer to Refs. [69, 116, 63, 130, 65] and the references therein.

for mode k, $\hat{a}^{\dagger}_{k,j}$ is the creation operator for mode k and photon j, $\vec{k_j}$ is the wavevector of photon j, and $\omega_{k,j}$ is the frequency of mode k for photon j. To make the problem a little more tractable one then makes the assumptions that the fields are all plane waves travelling in the z direction (replacing $\vec{k}\cdot\vec{r}$ with kz) and that the produced down-converted beams are single mode (allowing us to drop $\sum_k$). This yields the following equation for the pump

$$\hat{E}_p^{(+)} = E_0 e^{i(k_p z - \omega_p t)} \tag{3.9}$$

and the following equation for the signal and idler fields

$$\hat{E}_j^{(-)} = -i\sqrt{\frac{\hbar\omega_j}{2\epsilon_0 V}}\hat{a}_j^{\dagger} e^{-i(k_j z - \omega_j t)}. \tag{3.10}$$

The full quantum state evolution in the interaction picture is then given by

$$|\psi(t)\rangle = e^{\frac{1}{i\hbar}\int_0^t dt' \hat{H}(t')}|vac\rangle_{s,i} \tag{3.11}$$

where the initial state of the quantum field is the vacuum. However, with the non-linearity being very weak (typically on the order of 10^{-6} to 10^{-9}), expanding the exponential to first order is often sufficient (with the second order term leading to double pair emissions mentioned later). Considering only the non-vacuum term leaves one with

$$|\psi(t)\rangle = \frac{1}{i\hbar}\epsilon_0 E_0 \int_{-\infty}^{\infty} dt' \int_V d^3 r \chi^{(2)} \left[-i\sqrt{\frac{\hbar\omega_s}{2\epsilon_0 V}}\right]\left[-i\sqrt{\frac{\hbar\omega_i}{2\epsilon_0 V}}\right]\hat{a}_s^{\dagger}\hat{a}_i^{\dagger} e^{i(k_p - k_s - k_i)z} e^{-i(\omega_p - \omega_s - \omega_i)t}|vac\rangle_{s,i} \tag{3.12}$$

which can then be integrated over the x and y directions to yield

$$|\psi(t)\rangle = \frac{iE_0 L_x L_y \sqrt{\omega_s \omega_i}}{2V}\int_{-\infty}^{\infty} dt' e^{-i(\omega_p - \omega_s - \omega_i)t}\int_0^{L_z} dz \chi^{(2)} e^{i(k_p - k_s - k_i)z}|1,1\rangle_{s,i} \tag{3.13}$$

where L_x and L_y are the height and width of the non-linear optical crystal.

Now assuming that $\chi^{(2)}$ has no z dependence the last two integrals can be performed to get

$$|\psi(t)\rangle = \frac{iE_0 L_x L_y \sqrt{\omega_s \omega_i}}{2V}\chi^{(2)} e^{-i(\frac{\Delta\omega}{2})t}\delta\left(\frac{-\Delta\omega t}{2}\right)e^{i(\frac{\Delta k}{2})L_z} L_z sinc\left(\frac{\Delta k L_z}{2}\right)|1,1\rangle_{s,i} \tag{3.14}$$

where $\Delta\omega = \omega_p - \omega_s - \omega_i$ and $\Delta k = k_p - k_s - k_i$. The *sinc* function can be further approximated as a delta function leading to the two requirements that

$$\omega_p = \omega_s + \omega_i \tag{3.15}$$

and

$$\vec{k_p} \approx \vec{k_s} + \vec{k_i} \tag{3.16}$$

in order for the down-conversion signal to be appreciable. The two conditions can also be seen as conservation laws. 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 down-converted photons. The second law is the Conservation of Momentum which requires the wavevector of the pump photon to equal the sum of the wavevectors of the two generated photons. The second condition is also known as phase-matching since it relates the fact that the pump beam must stay in phase with the down-converted signal and idler beams in order for constructive interference to continually amplify the down-converted modes. If proper phase-matching is not achieved then the power transferred to the down-converted modes reaches a maximum and then starts to contribute to the reverse process (second harmonic generation) creating pump photons at the expense of photons in the down-converted mode. Without proper phase-matching this cyclical process happens along the length of the crystal.

Quasi-Phase Matching and Periodic Poling

To obtain a bright source of down-converted entangled pairs, one generally wants the pump beam and down-converted beams to interact for as long as possible. However, because the frequencies of the pump and down-converted photons are so far apart, material dispersion of the non-linear crystal causes their phase fronts to become out of sync so that they do not stay coherent for very long. This is the underlying physical reason why phase-matching can be difficult to accomplish in non-linear optical crystals. This also limits the useful crystal length which in turn limits the brightness of the source.

The typical solution to achieve phase-matching is to use crystals that exhibit birefringence. In birefringent phase-matching the interacting waves have their polarizations

arranged so that the birefringence of the crystal effectively cancels out the dispersion allowing for the coherent evolution of SPDC. Unfortunately, birefringent phase-matching usually only allows SPDC in a small range of wavelengths in any particular crystal material so that temperature tuning and angle tuning must also be used to tailor the birefringence experienced by each photon. However, there are a number of problems with these methods. Firstly, some of the non-linear coefficients of the non-linear susceptibility tensor are not always affected strongly by birefringence. And secondly because the direction of propagation is dictated by the birefringent phase-matching conditions it is usually not along one of the crystallographic axes leading to walk-off effects which once more limit the useful crystal length.

To combat the problems associated with birefringent phase-matching, the techniques of quasi-phasematching and periodic poling were developed both to allow materials with stronger non-linearities to be used and to allow for collinear down-conversion along a crystallographic axis in order to increase the distance over which a coherent interaction could be maintained. Quasi-phasematching is a tool which maintains the direction of power flow from the pump field to the down-converted fields created by the interaction with the non-linear crystal [71]. Mathematically, by periodically reversing the non-linear crystal, quasi-phasematching is achieved by adding an extra term to the phase-matching condition of Eq. 3.16 to yield the new phase-matching condition given by

$$k_p = k_s + k_i + \frac{2\pi}{\Lambda} \tag{3.17}$$

where Λ is the period of the inversion, which can now be engineered [65]. Physically, quasi-phasematching is achieved by inverting the non-linear response of the crystal precisely when the pump and the down-converted fields become 180° out of phase with each other. At this point, the down-converted fields would normally begin transferring power back to the pump field but the effect of the crystal inversion is to essentially reset the overall phase mismatch back to zero allowing the down-converted field to continue to grow.

Quasi-phasematching was first proposed by Armstrong *et al.* [10] in 1962 where they envisioned periodically reversing the non-linear crystal by physically cutting the crystal into thin slices of the appropriate thickness and then reassembling it while rotating every

second slice by 180°.[6] Obviously this would be impractical for the typical periods required which are on the order of 1-100 μm. Instead, periodic poling was developed by Yamada *et al.* [166] in 1993 to periodically reverse the electrical domains in a ferromagnetic material by applying voltages to attached electrodes as the crystal is grown. Since the initial experiments of Yamada *et al.* periodic poling has been studied to the point where it has become a well controlled process [107, 71]. It is typically used with two main families of crystals: lithium niobate ($LiNbPO_3$ or LN) and lithium tantalate ($LiTaO_3$ or LT), or potassium tytanyl phosphate ($KTiPO_4$ or KTP) and its isomorphs [65]. In the source detailed below I use periodically poled KTP (or PPKTP) to produce the down-converted photon pairs.

It should be mentioned that periodic poling is usually augmented by temperature tuning of the crystal to make up for any imprecision in the precise poling period of the crystal to allow for the generation of down-converted photons at the specific desired wavelength. However, temperature tuning in this context does not bring with it the same problems as in birefringent phase-matching since a collinear configuration can now be used along a crystallographic axis. This removes many of the walk-off effects and allows the use of much longer crystals with a stronger non-linearity to produce a much brighter source with conversion efficiencies on the order of 10^{-6}.

Previous Entangled Photon Sources

There have been a number of different configurations for entangled photon pair generation proposed and implemented using SPDC (for an excellent detailed overview of some of the more prominent implementations please refer to Ref. [65] Ch. 2). Polarization entangled photons were first demonstrated in 1988 by Ou and Mandel [115] and Shih and Alley [147] by pumping a type-I down-conversion crystal at one end of an interferometer, flipping the polarization of one of the pairs with a HWP, recombining the photons on a 50/50 BS, and then post-selecting on the detection of a photon in each output mode. However, it was not until 1995 that Kwiat *et al.* [86] demonstrated the first direct source of entangled photons using type-II parametric down-conversion where a properly phase-matched crystal

[6] For a good review of quasi-phasematching please refer to Ref. [73].

produced two cones of down-converted photons and entangled photons were collected at the two points where the cones overlapped. This is the same source used in my earlier QKD experiments detailed in Ch. 2 and Sec. 3.1.

A second direct source of entangled photons was developed in 1999 by Kwiat *et al.* [87] only this time using a type-I SPDC sandwich scheme in which two identical nonlinear crystals were placed back-to-back with one of them rotated by 90°. By using a pump laser polarized at 45°, pairs could be produced in either crystal and, so long as thin crystals were used, there would not be enough information to distinguish which crystal the pair came from thus producing an entangled quantum state. The photons here were produced along two overlapping cones giving the advantage that a much higher percentage of the down-converted photons were entangled allowing for a much brighter source than the first type-II source. However, the rates were still limited by the necessity to use thin crystals.

While these two types of sources remained the main workhorses for creating entangled photon pairs in many quantum optics labs for over ten years, they were still limited in their pair production rate both by limitations on the maximum crystal length that could be used and on the percentage of the down-converted photon pairs which could be collected. It was soon realized that both of these constraints could be relaxed if degenerate collinear SPDC was employed by placing a nonlinear crystal in each arm of a Mach-Zender interferometer [85]. Collinear generation allowed for a much more efficient collection of the photon pairs since rather than being generated into many modes distributed around a cone they would instead be generated into just a few tightly packed modes propagating in the same direction as the pump. Thus, the collection efficiency could be much higher even when collecting into singlemode fibres. Additionally, the collinear configuration meant far fewer problems with longitudinal and transverse walk-off, allowing for the use of longer crystals which improve the brightness of such a source.

This type of source was first demonstrated by Kim *et al.* [78] in 2001 and further improved using a folded interferometer by Fiorentino *et al.* [58] in 2004. While a promising first attempt at utilizing collinear generation to produce brighter sources, they both had the major drawback that the interferometer which the crystals were placed in had to remain phase-stable in order for entangled photon pairs to be produced. This required the use of sophisticated stabilization equipment for the interferometer and ultimately limited

the quality (ie. high visibility) of the entanglement produced. The situation changed however when a design incorporating an inherently phase-stable Sagnac interferometer was developed.

3.2.2 Design

The design of a Sagnac entangled photon source was originally invented by Shi and Tomita [146] and then further developed by Kim *et al.* [77, 164] and subsequently had its focusing and mode-matching optimized by Fedrizzi *et al.* [54]. The goal of such a source is to produce photon pairs in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + e^{i\varphi}|VH\rangle). \tag{3.18}$$

A schematic of the Sagnac source I built is shown in Fig. 3.6. It is pumped with a 404 nm grating stabilized, power tuneable, laser (iWave-405-S) with a maximum power of 50 mW from Toptica Photonics. The pump laser first passes through an optical isolator (IO-5-405-LP from Thorlabs) and HWP to remove any possible back reflection effects of the pump laser on itself. Two dichroic mirrors are then used both to steer the pump laser and to remove any possible photons generated by the pump laser around 800 nm that could make it through the source and erroneously be recorded as entangled photons. A HWP and QWP[7] are then used to adjust the phase in the output state of the photon pairs, given by Eq. 3.18, in order to produce the desired $|\psi^-\rangle$ state (see Eq. 2.1).

A periodically poled KTP (PPKTP) non-linear optical crystal, with dimensions 20 mm $\times$ 1 mm $\times$ 1 mm made by Raicol Crystals Ltd., is placed at the center of the interferometer loop. The PPKTP crystal is phase-matched to generate photon pairs in a collinear

[7]Normally a QWP waveplate is rotated, using a rotation mount, around the pump beam passing normally incident to its face. However, if I was to operate the QWP like this then its action and the action of the HWP would become coupled. To avoid this problem, I set the QWP to its zero axis (ie. it rotates the pump by 0° and has no effect) and then rotate the QWP, mount and all, to change the incident angle of the pump beam with the QWP face causing the pump beam to pass through slightly more QWP material. This has the effect of adjusting only the phase of the pump beam independently of the HWP action.

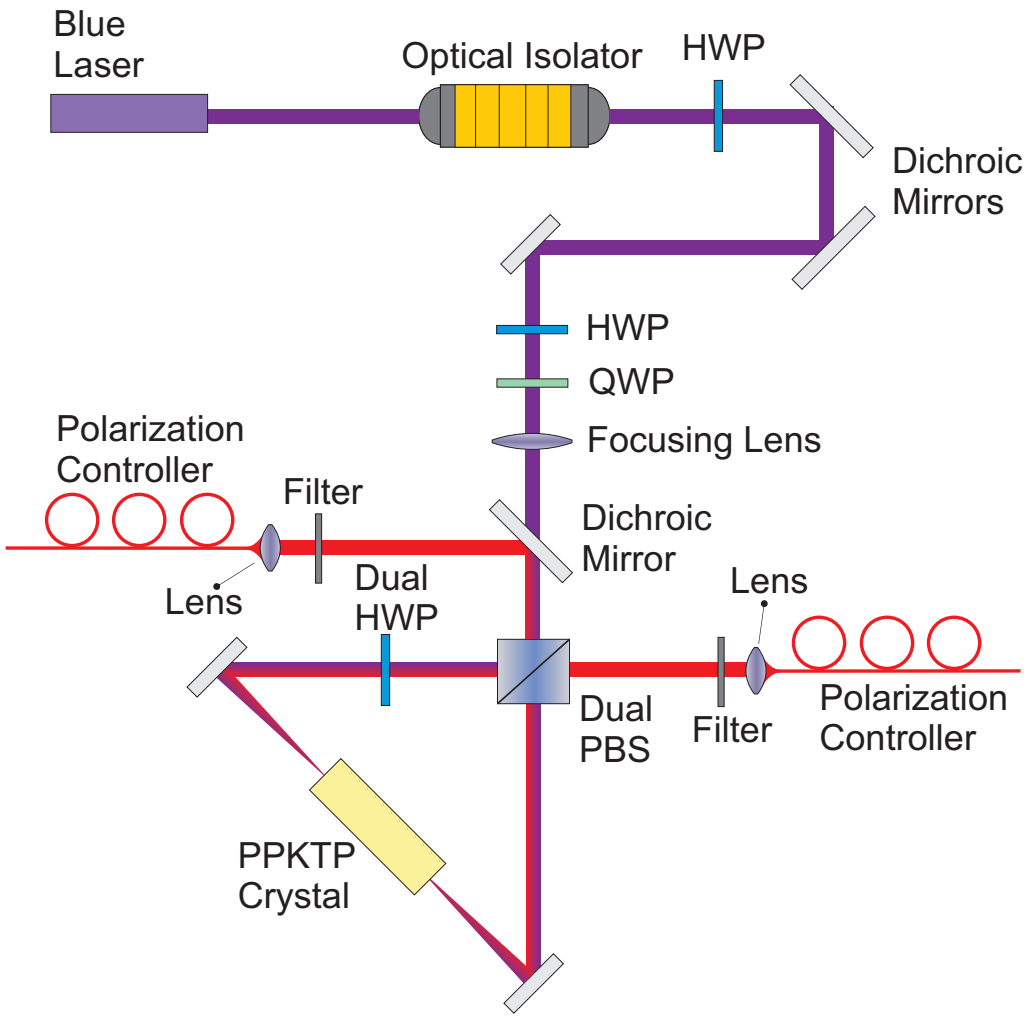

Figure 3.6: Experimental schematic of the Sagnac interferometric entangled photon source. Entangled photon pairs are produced by bi-directionally pumping a PPKTP non-linear optical crystal, which produces down-converted polarization-correlated photon pairs. The dual wavelength HWP and PBS are responsible for removing the path information of the photons, thus producing entangled photons, and for separating the pairs of photons into two paths for fibre coupling.

configuration at a degenerate wavelength of 808 nm. The pump laser is focused with an achromatic doublet lens ($f = 200$ mm) positioned so that the focus is at the approximate center of the PPKTP crystal. Entangled photons are produced by sending 45° polarized light (adjustable with the HWP) onto a dual wavelength polarizing beamsplitter (PBS) which has the effect of bi-directionally pumping the PPKTP crystal sitting in the middle of the interferometer loop. A dual wavelength HWP rotates the pump in one arm by 90° and ensures that the pump is properly polarized so that the crystal produces down-converted polarization correlated photon pairs in both directions around the loop. The dual wavelength HWP also rotates the polarization of the down-converted photons traveling counter-clockwise around the loop. This has the effect of erasing the path information after the down-converted photons are split on the dual wavelength PBS. Thus, after the dual wavelength PBS, polarization entangled photons have been generated.

The two beams of entangled photon pairs are collected directly from one port of the dual wavelength PBS and via a dichroic mirror responsible for splitting the down-converted photons from the blue pump laser at the second exit port. The beams first pass through a 635 nm long pass filter to get rid of any residual photons from the pump laser and allow for the initial alignment of the couplers (Singlemode Fibre Positioner model# 9091 from Newport) responsible for collecting the entangled photon pairs. Narrowband interference filters (5 nm bandwidth) are then placed after the red low pass filter with their central transmission wavelength tuned by tilting their angle with respect to the incident entangled photon pair beam. The entangled photons are coupled into short singlemode optical fibres which pass through manual polarization controllers used to undo the unwanted random unitary caused by the singlemode fibres. The fibres can then either be connected to local detectors for calibration; to local polarization analyzers to perform a local QKD, Bell, or oblivious transfer experiment; or to long singlemode fibres running to the sending telescopes on the roof of CEIT to perform a free-space QKD experiment.

3.2.3 Setup and Alignment

While the design of the Sagnac source is relatively simple and straightforward, its construction is rather sensitive to a number of important dimensions and angles, many of

which are coupled in their influence. During the construction and alignment of the source I gained many insights into the proper sequence of steps necessary to align the source for a maximum pair rate and high visibilities. I also benefitted greatly from a number of the setup and optimization techniques developed by Deny Hamel during his own work with his Sagnac source, which is detailed in his Masters thesis [65]. In the following I outline the best sequence of steps in order to align a Sagnac entangled photon source. When measuring the coincidence count rate of the source I used a coincidence window of 3 ns to minimize accidental coincidences.

1. **Temperature tuning**
   The first step is to determine the proper temperature tuning for the PPKTP crystal. The wavelengths of the down-converted photons can be adjusted both by adjusting the wavelength of the pump laser or by adjusting the temperature of the PPKTP crystal placed in an oven, with the preferred method being through temperature tuning. To do this, setup the PPKTP crystal in a simple linear configuration with the pump laser focused into the crystal on one side and the resulting pairs collected with a coupler on the opposite side using a filter to get rid of the pump. Then feed the coupled photons into a spectrometer to measure their wavelengths. Assuming one wants to work at the temperature which produces photon pairs of degenerate wavelengths[8], alternate between increasing the temperature by 0.1°, allowing the crystal temperature to stabilize, and measuring a spectrum for the photon pairs. Fig. 3.7 (a) shows the results for non-degenerate pair production at an initial temperature of 56.0°. Here two peaks, one for horizontally polarized photons and one for vertically polarized photons, are clearly visible. Fig. 3.7 (b) shows the results for degenerate pair production once the proper temperature of 60.4° was found[9].

[8]This method is equally good to produce pairs with different wavelengths. One of the advantages of a Sagnac source is that photon pairs can remain highly entangled even when their wavelengths are far from the degeneracy point [54].

[9]Alternatively, one can leave the temperature tuning step until after the loop is setup and aligned. Then set the dual wavelength HWP to rotate the pairs by 22.5°, pump in one direction around the loop, connect one of the fibres to the spectrometer, and then perform the same measurements as above alternating between adjusting the temperature and taking a spectrum.

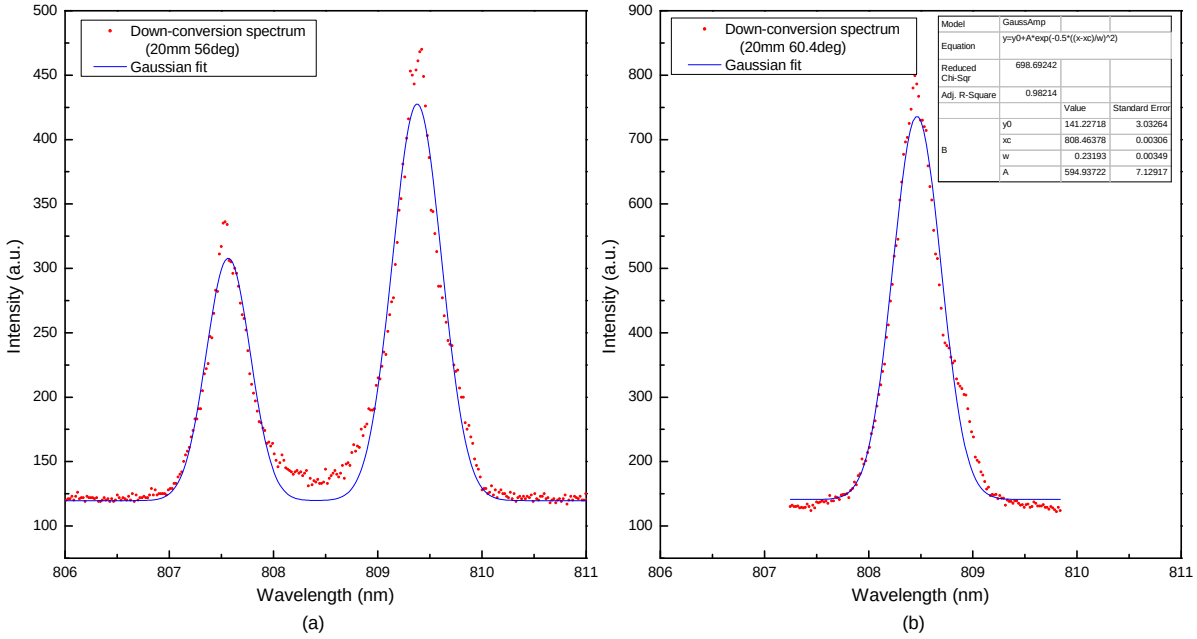

Figure 3.7: The temperature tuning spectrum of the Sagnac source for (a) the initial non-degenerate temperature of 56.0° and (b) the degenerate temperature of 60.4°.

2. **Place the dual wavelength PBS and two mirrors forming the Sagnac loop**
   Next, with the pump laser on and the optics up to the QWP installed (but no focusing lens yet), move the dual wavelength PBS into position on its tip/tilt stage, then place the two other mirrors responsible for creating the interferometer loop mounted in adjustable tip/tilt mirror mounts. Null the QWP and set the HWP to send 45° polarized light onto the dual wavelength PBS. Cycle through adjustment of the PBS and two mirrors to adjust their position and angle so that both the clockwise and counter-clockwise propagating beams are as closely aligned as possible. A good tip is to observe the interference of the counter-propagating pump laser beams at the output port of the PBS. The loop is coarsely aligned when interference fringes become visible.
3. **Setup and align the collimators**
   First place the dichroic mirror, responsible for separating the pump laser from one half of the entangled photon pairs, adjusting it so that it will reflect the entangled photons at approximately 90°. Now place the two couplers responsible for collecting each half of the entangled photon pairs into singlemode fibres installed onto fine translation stages allowing movement in the x and y direction[10]. With a visible red back-alignment laser inserted into the fibres, adjust the position and pointing of each coupler so that the red beam overlaps as closely as possible with the blue pump beam.
4. **Place the focusing lens**
   Now put the focusing lens into position on a z-translation stage and in a mount that allows for x and y adjustment. Center the pump beam on the lens and adjusted the z position of the lens so that it is focused at the approximate middle position between the two loop mirrors where the PPKTP crystal will be placed next.
5. **Place the PPKTP crystal**
   With the PPKTP crystal installed in its oven, place it in a mount which allows for z translation between the two loop mirrors so that the pump laser is focused approximately in the center of the crystal. At sufficiently high power (between 25-

[10]For the setup of the source, the z direction is assumed to be the propagation path of the pump laser, while the x and y directions are the horizontal and vertical directions, respectively.

50 mW) the pump laser will leave a visible trail in the crystal that one can just make out with the eye. Use this to adjust its position and angle with respect to the pump beam so that the pump passes through the center of the crystal normally incident to the entrance face. A red back-alignment laser from each coupler will also be visible passing through the crystal. Use this beam to fine tune the alignment of the couplers so that the red and blue beams are superimposed over one another. Adjust the temperature of the PPKTP oven to produce degenerate wavelength photon pairs.

6. **Place the dual wavelength HWP**
   Place the dual wavelength HWP in the reflected arm of the PBS and adjust its position and pointing so that the pump beam passes through the center of the HWP normally incident to its face.
7. **Fine tune angular pointing of couplers**
   Place the 635 nm low pass filters before the couplers to remove most of the pump beam. If the singlemode fibres are now connected to single photon detectors one should observe count rates slightly higher than the background rates of the detectors. It is a good idea to do this in a darkened room for the best contrast between background photons and down-converted photons. By adjusting the position and angular pointing as well as the focusing of the couplers, maximize the single photon count rates in each arm. One should also see an appreciable coincidence rate between the two arms as well. Now rotate the pump HWP to only pump the loop clockwise and rotate the dual wavelength HWP to rotate the photons by 45°. Next, plug one of the singlemode fibres output from the collimators into a fibre-based 50/50 beamsplitter. Plug the two outputs from the fibre beamsplitter into single photon detectors. Maximize the number of coincidences observed by adjusting only the tip/tilt of the coupler, not the x,y positioning. You can also adjust the focusing of the couplers. This guarantees that the couplers are looking at collinearly produced photon pairs rather than photons emitted from the crystal at an angle. Do the same for the second coupler. In all of the following steps when the couplers are adjusted it is only their x and y positioning that will be adjusted, never adjust their tip/tilt position again.
8. **Fine tune the Sagnac loop**
   The next step is to fine tune the pointing of the Sagnac loop to overlap the counter-

propagating pump laser beams since only a perfect overlapping will produce entangled photon pairs. Adjust the dual wavelength PBS so that it rotates the photons by 90°. Now iterate between the following steps:

(a) Adjust the pump HWP to send H polarized pump photons onto the dual wavelength PBS (ie. pump the source clockwise).

(b) Adjust the x and y position of each coupler to maximize the single photon count rates. Record the micrometer readings for each coupler, the single photon count rates, and the coincidence count rates.

(c) Adjust the pump HWP to send V polarized pump photons onto the dual wavelength PBS (ie. pump the source counter-clockwise).

(d) The single and coincidences rates will be decreased. Again, maximize the single count rates by adjusting the x and y position of each coupler. Record the micrometer readings for each coupler, the single photon count rates, and the coincidence count rates.

(e) Calculate the x and y midpoint for each coupler between the two positions that produced the maximum count rates when the source was pumped clockwise and counter-clockwise. Move each coupler to this calculated midpoint.

(f) Adjust the pump HWP to send 45° polarized pump photons onto the dual wavelength PBS (ie. bi-directionally pump the source).

(g) Now adjust the pointing of the two loop mirrors, first adjusting the azimuthal angle of each and then the elevation angle of each, to again maximize the single and coincidence count rates. You will likely need to iterate between adjusting the azimuthal and elevation angles a few times in order to find the maximum.

The Sagnac loop is aligned once the count rates pumping with H and V are equal to within the Poissonian fluctuations of the source (ie. to within a few thousand for the singles rates and to within 1,000-2,000 for the coincidence rates). At this point, you can also pump with 45° light and adjust the focusing of each coupler again to maximize the rates.

9. **Place the narrow interference filters**

Now place the narrow interference filters (filters with a bandwidth of 5 nm or smaller

are sufficient) between the 635 nm long pass filters and the couplers. Likely you will have to tune the angle which the incoming entangled photon beam makes with their face. Alternate between adjusting their angle and fine tuning the positioning of each coupler to maximize the rates (changing the filter angles will change the beam deflection making a coupler positioning correction necessary). With good interference filters you should only lose roughly 10% of your photons.

10. **Adjust the pump HWP and QWP to produce entangled photons**
    To produce the $|\psi^-\rangle$ state, adjust the pump HWP to send 45° polarized pump photons onto the dual wavelength PBS. With the singlemode fibres connected to polarization analyzers (such as those from Sec. 2.4.3) which are then fed into single photon detectors, observe the visibilities of the photon pairs in the rectilinear (H/V) and diagonal ($+45°/-45°$) bases. The visibility of the photon pairs in the H/V basis should ideally be $> 95\%$. now slowly twist the QWP (its quite sensitive to the angle) to change the correlations in the diagonal basis. If the loop was aligned properly, twisting the QWP should have minimal impact on the correlations in the rectilinear basis. Continue to twist the QWP until the visibility is maximized in the diagonal basis. The visibility might not yet be $> 90\%$.
11. **Fine tune the position of the crystal**
    In order to observe good entanglement in the diagonal basis the pump needs to be focused at the center of the crystal, otherwise a phase shift builds up between photons travelling clockwise around the loop versus those created counter-clockwise around the loop due to the Ghoy phase of the two focused beams [123]. This makes it difficult to properly set the phase of the state with the QWP and will degrade the entanglement if not corrected. With the singlemode fibres connected to polarization analyzers, maximize the visibility of the photon pairs in the diagonal basis by adjusting the z-position of the crystal and its oven. This should not have a significant effect on the visibility of the photons in the rectilinear basis.
12. **Source should now be aligned**
    The entangled source should now be aligned with visibilities $> 97\%$ in both bases at moderate pump powers (I typically worked with a pump laser power of 5 mW before the optical isolator). If the visibilities are not sufficiently high yet, go back

and iterate through the steps from the fine tuning of the angular pointing of the couplers and beyond.

3.2.4 Performance Metrics and Discussion

Using this source, one of the first things I performed was a local QKD experiment to measure its performance metrics and compare with my first generation source used in previous experiments [49]. My first generation source, pumped at a maximum of power of 50 mW and using a coincidence window of 2 ns, was limited to local singles count rates of approximately 100,000 counts/sec(cps) and a coincident entangled photon detection rate of 12,000 cps with observed visibilities of 99.5% and 92% in the rectilinear and diagonal bases respectively. In comparison, local experiments with the new Sagnac source yield single photon detection rates of 400,000 cps in either output path and a coincident entangled photon detection rate of 60,000 cps at only 8 mW of pump power using a 3 ns coincidence window. Additionally, visibilities upwards of 98% and 97% in the rectilinear and diagonal bases respectively are consistently observed for a well aligned source.[11]

Table 3.6 shows the pertinent statistics of both sources for comparison. As one can see, the new Sagnac source improved not only the raw coincidences count rates but also decreased the overall QBER experienced. The visibilities and corresponding QBER seem to degrade less when they pass through the polarization detection optics which is most likely due to the improved polarization compensation accomplished with manual polarization

[11]The statistics quoted for the first generation source were obtained by plugging the singlemode fibres from the source directly into single photon detectors and flipping up polarizers directly into the entangled photon beam paths in front of the couplers and then rotating them to make all of the measurements necessary to reconstruct the visibilities, etc. It was not possible to do this with the new Sagnac source as the couplers were so finely tuned that flipping up polarizers into the beam path deviated the beams enough to significantly affect the count rates and corresponding visibilities. Thus, the statistics for the second generation source are instead quoted with the singlemode fibres connected to the polarization analyzers, the random unitary from the fibres corrected for, and then the fibres connected to the single photon detectors. The polarization analyzers themselves have some loss and errors (eg. it is well known that the contrast in the reflected arm of a PBS is typically much lower than the transmitted arm). For a fair comparison I have included statistics for the Kwiat source when it was analyzed with the polarization analyzers in Table 3.6. The statistics for the Sagnac source were all obtained using the polarization analyzers.

controllers. The compensation is better since the bandwidth of the photons (mentioned next) is much narrower than before allowing the polarization controllers to correct the random rotation of the fibres accurately for more photon pairs. While visibilities for a Sagnac source upwards of 99.5% have been observed by Fedrizzi *et al.* [54] in both bases, these were measured at very low power levels with very high quality polarizers and accidental coincidences subtracted.

	Power (mW)	Singles (cps)	Coins (cps)	Vis (H/V, +/-)	QBER
Kwiat SPDC source					
Direct	50	100,000	12,000	99.5%, 92.0%	2.13%
Pol Analyzers	50	81,000	7,600	99.0%, 88.0%	2.91%
Sagnac source	(set, actual)				
	3, 0.47	56,848	6,685	99.59%, 98.50%	0.53%
	5, 1.75	223,465	28,000	99.20%, 98.09%	0.73%
	8, 3.60	472,654	52,585	97.61%, 96.94%	1.40%
	10, 4.84	647,510	76,931	97.40%, 96.99%	1.43%
	15, 8.13	1,070,875	134,418	97.19%, 96.29%	1.68%
	20, 11.29	1,483,515	182,614	95,94%, 94.52%	2.46%
	25, 14.05	1,817,470	202,714	94.44%, 93.92%	2.94%
	30, 17.25	2,114,969	252,265	94.41%, 93.52%	3.07%
	40, 23.47	2,752,158	337,742	93.84%, 91.93%	3.66%
	50, 29.57	2,933,715	352,901	92.34%, 90.90%	4.26%

Table 3.6: The statistics for the first and second generation sources. The Sagnac source improved on the Kwiat design both in raw count rates and in a lower QBER. However, the ability to pump the new Sagnac source at the full 50 mW of power is doubtful without further filtering techniques or better timing hardware since there is a marked drop-off in visibility and a corresponding increase in the QBER as the pump power is increased.

Another advantage of the Sagnac source over the previous SPDC source is that it is extremely narrowband, with a bandwidth of 0.23 nm (see Fig. 3.7), which allows me to use narrower filters in my polarization analyzers and reduce the number of errors due to accidental coincidences from the detection of background light. As mentioned earlier in

the setup steps, I used interference filters with a bandwidth of 5 nm as well as long pass filters with a cutoff at 635 nm to filter out any remaining blue pump laser light and any background light. In previous experiments with the old SPDC source I was forced to use much wider 10 nm filters in order to maintain appreciable detection rates. Kwiat et al.'s previous experiments [86] with this type of source showed that it typically had a bandwidth which filled most of their 5 nm filters.

The narrow bandwidth of the new Sagnac source also leads to the additional benefit of helping towards daylight compatibility for the QKD system. The main problem encountered with operating a free-space QKD system during daylight hours is the extremely high background light levels. To combat this, there are only 3 possible filtering techniques one can use: spatial, spectral, and temporal. Having a much narrower bandwidth than the previous source will allow future experiments to greatly improve the spectral filtering of the photons at the receiver stations. With a bandwidth of 0.23 nm it should be possible, with careful alignment, to move to 1 nm filters to greatly reduce the background light without seeing a significant drop in the entangled photon detection rates. With slightly improved spatial and temporal filtering, the hope is that it should be possible to run the system in daylight conditions.

The improvement in brightness of approximately two orders of magnitude from the Sagnac source is due to two reasons: better coupling efficiency, and a collinear configuration. Better couplers were used in the Sagnac source to finely tune the coupling of the entangled photons as evidenced by the sensitivity of the coupling to inserting polarizers before the couplers. A collinear configuration helped in two ways. First, it allowed for a much longer non-linear crystal (and by extension a much higher effective non-linearity) to be used since walk-off effects are vastly reduced in a collinear configuration. Secondly, the collinear configuration allowed a much higher percentage of down-converted photon pairs to be entangled, much like the sandwich source mentioned above, since I was not limited to the regions of intersection of two cones. Also, the mode of each down-converted photon is much cleaner allowing for a much better mode matching and coupling to the singlemode fibres.

One potential problem with the higher entangled photon rates generated with the new Sagnac source is the increase in the probability of double pair emission events where two

entangled photon pairs are created in the crystal within one coincidence window. When used in a QKD system double pair emission events increase the measured QBER either by causing multiple detectors to fire which must then be recorded as a random result for security to hold, or when due to loss Alice measures a photon from the first pair while Bob measures a photon from the uncorrelated second pair. Indeed, this is the main cause for the dropping visibilities and increasing QBERs in Table. 3.6 as the pump power is increased. A higher QBER will in turn decrease the final key rate generated using such a source. The only method for combating this problem is to decrease the size of the coincidence window by using electronics with a higher temporal accuracy and lower jitter allowing the coincidence algorithm to discern the photons as two separate pairs.

3.3 Improving Entangled Free-Space QKD in the Turbulent Atmosphere with a Signal-to-Noise Ratio Filter

The basis biasing idea, discussed earlier, is a very useful tool to have in one's QKD toolbox in order to increase the efficiency of the secure key generation rate in a QKD system from the same amount of raw key material. I now move on to the investigation of a second useful tool for increasing the secret key generation rate specific to a free-space QKD system. The rationale for research focused on a tool which can only be used in a free-space system is that while fibre implementations have produced some of the fastest systems to date [40], until reliable quantum repeaters are realized, fibre implementations will remain limited to a transmission distance of ≤ 200 km. Even with expected future advances in fibre, source, and detector technology, secure key distribution will still be limited to ≤ 400 km using fibres. However, free-space QKD links with orbiting satellites have long been proposed as a solution for global key distribution, as evidenced by the growing number of feasibility studies that have been conducted [114, 126, 12, 9, 26].

QKD with low earth orbit (LEO) satellites likely represents the most feasible solution since they will have the shortest free-space transmission distance with the lowest losses.

However, LEO satellites travel quickly with short orbital periods limiting the time available to perform QKD during a single pass to the order of 300 sec [26]. Thus, it is important to have a thorough understanding of the transmission properties of the free-space channel which the photons will travel through in order to properly evaluate the feasibility of such a system. As well, with such a short time to exchange a key, it is important to get the most from the relatively small number of signals sent and received during a pass.

To investigate these two points, I begin by reviewing some recent theoretical work on the transfer of quantum light and entanglement through the turbulent atmosphere (Sec. 3.3.1); then experimentally determined free-space transmission efficiency curves measured with an entanglement based free-space QKD system are examined (Sec. 3.3.2); a method for improving free-space QKD key rates in the turbulent atmosphere through the use of a signal-to-noise ratio (SNR) filter is then put forward (Sec. 3.3.3); followed by the experimental results of implementing such a filter and their implications for the security of the system (Sec. 3.3.4). A paper on this work is currently being prepared [50].

I worked on the free-space link statistics theory and measurement in collaboration with Bettina Heim from the Max Planck Institute for the Science of Light in Erlangen, Germany and Prof. Thomas Jennewein at the Institute for Quantum Computing in Waterloo, Canada. Bettina and I jointly collected the data that was subsequently analyzed for the statistics of IQC's free-space link transmission efficiency. Bettina performed an initial analysis of the data to get some of the first transmission distributions and I subsequently wrote analysis software capable of more accurately ascertaining the free-space link statistics making use of the timing information collected. Both methods are described in Sec. 3.3.2. I also include Bettina's analysis of the 144 km Tenerife free-space experiments to compare with the measurements from my system. The signal-to-noise ratio filter is an idea from Prof. Jennewein. Again, the data used in its study is the same data used for the link statistics analysis and was jointly collected by Bettina and myself. I then wrote all of the custom analysis software and used it to analyze the usefulness of the SNR filter idea. Lastly, I benefitted from a number of helpful discussions with E. Meyer-Scott and J.P. Bourgoin on satellite QKD simulations while completing this project.

3.3.1 Free-Space Link Statistics

The propagation of classical light through turbulent atmosphere has long been of interest in theoretical investigations, including such diverse phenomena as diffraction, scintillation, and the absorption of light by molecules in the atmosphere which produce beam wander and broadening. This has been thoroughly studied (see e.g. Refs. [152, 52, 53, 7]) following previous work on the description of turbulence by Kolmogorov [82]. The "strength" of optical turbulence due to random variations of the refractive index in the atmosphere can be described in terms of the refractive index structure parameter, $C_n^2(h)$, which depends on the wavelength, atmospheric pressure, and atmospheric temperature and varies strongly with the height, h, above ground. Typical values of $C_n^2(h)$ lie in the range of 10^{-17} m^{23} for weak turbulence up to 10^{-12} m^{23} for strong optical turbulence (see e.g. Ref. [8]).

Satellite based communication has also been investigated in the context of a turbulent atmosphere, see for example the first theoretical study of scintillation for ground-to-space laser beam transmission by Fried [59] or more recent work by Shapiro [145] and Andrews *et al.* [7, 8]. Following this theory, the intensity fluctuations due to the turbulent atmosphere can be assumed to be log-normally distributed in the regime of weak fluctuations. This has also been confirmed in various experiments (see e.g. Ref. [108]). Recently, Vasylyev, Semenov and Vogel [157, 142, 141] provided a theoretical foundation for studying the influence of fluctuating loss channels on the transmission of quantum and entangled states of light. They approximate the probability distribution of the (fluctuating) atmospheric transmission coefficient (PDTC) in the case of entanglement distribution according to the log-normal distribution:

$$\mathcal{P}(\eta_{atm}) = \frac{1}{\sqrt{2\pi}\sigma\eta_{atm}} \exp\left[-\frac{1}{2}\left(\frac{\ln \eta_{atm} + \bar{\theta}}{\sigma}\right)^2\right] \tag{3.19}$$

where η_{atm} is the atmospheric transmittance, $\overline{\theta} = -\ln < \eta_{atm} >$ is the logarithm of the mean atmospheric transmittance, and σ is the variance of θ characterizing the atmospheric turbulence.

They state that this will not be a complete description of the atmospheric influence on the transmission of (quantum) light under general conditions since phase (front) fluc-

tuations must also be considered. For the most general description, they suggest an experimental method to reconstruct the PDTC by measuring its statistical moments using balanced homodyne detection [141]. However, all of the following investigations are based on experiments utilizing the direct detection of single photons, making the complex phase nature of the transmission coefficients unaccessible. Thus, it is sufficient to describe the fading channel by the distribution of the real valued $\eta_{atm} = |T|^2$, where the transmission coefficient, T, is from the operator input-output relation for an attenuating system given in Ref. [142].

3.3.2 Measuring Free-Space Link Statistics with Entangled Photons

To begin, Bettina and I measured the free-space transmission efficiency link statistics observed in my entanglement based QKD system. The system is comprised of the compact Sagnac interferometric entangled photon source (discussed fully in Sec. 3.2), a 1,305 m free-space optical link from the CEIT building to the IQC building where the outgoing/incoming beam is expanded/contracted by the use of the same telescopes (the telescopes have a 75 mm collection lens and a 25:1 magnification) and compact passive polarization analysis modules discussed in Sec. 2.4.3, avalanche photodiode (APD) single photon detectors, time-tagging units, GPS time receivers, two laptop computers, and custom written software improved upon from that described in Sec. 2.4.4. Usually there is a filter at the entrance of the polarization detector box used to reject background light; however, I removed it for these experiments in order to simulate a scenario (such as a satellite link) with a higher background noise level in order to test the usefulness of the signal-to-noise ratio filter proposal, described later.

The beauty of measuring the link statistics with the entangled photons is that the various other efficiencies of the system can be measured, by first performing a local experiment with the same equipment (source, polarization analyzers, photon detectors). The effects of these components can then be divided out of experiments performed over the link leaving only the PDTC of the free-space channel. The method I use here for the efficiency calibration of different components in the system was first discussed by Brida *et al.* [30]

who employed two photon entangled states for the absolute quantum efficiency calibration of photodetectors. The number of counts per second expected for a local experiment at Alice's detector (N_A) and Bob's detector (N_B) are given by

$$N_A = N\eta_A = N\eta_{A_{source}}\eta_{A_{pol}}\eta_{A_{det}} \tag{3.20}$$

$$N_B = N\eta_B = N\eta_{B_{source}}\eta_{B_{pol}}\eta_{B_{det}} \tag{3.21}$$

where N is the total number of pairs produced at the source per second, η_A is Alice's total transmission efficiency (comprised of the source coupling efficiency, $\eta_{A_{source}}$, polarization analyzer efficiency, $\eta_{A_{pol}}$, and detector efficiency, $\eta_{A_{det}}$), and similarly for Bob. Additionally, the expected number of observed coincidences per second (N_{coin}) between Alice's and Bob's measurement lists, which represent the detection of entangled photon pairs, is given by

$$N_{coin} = N\eta_A\eta_B. \tag{3.22}$$

Dividing the measured coincidence count rate (N_{coin}) by the observed singles rate at Alice (N_A) yields an estimate for the total loss caused by Bob's optics (η_B) including the source coupling, polarization analyzer, and photon detectors.

For experiments performed over the free-space link, the equation for Bob's singles rate gets modified to

$$\begin{aligned} N_B &= N\eta_B + N_{background} \\ &= N\eta_{B_{source}}\eta_{B_{link}}\eta_{B_{pol}}\eta_{B_{det}} + N_{background} \end{aligned} \tag{3.23}$$

where his total transmission efficiency, η_B, now includes a term for the link transmission efficiency, $\eta_{B_{link}}$, and an additional term, $N_{background}$, is added representing background photons which are collected and measured by Bob's receiver. The equation for the coincidence rate is similarly modified to

$$N_{coin} = N\eta_A\eta_B + N_{accidental} \tag{3.24}$$

where again η_B includes a link efficiency term, $\eta_{B_{link}}$, and there is an additional term, $N_{accidental}$, representing accidental coincidences of Alice's measurements with the background photons measured by Bob. Fortunately, the accidental coincidence rate, given to good approximation by

$$N_{accidental} = N_A N_B \Delta t_{coin} \tag{3.25}$$

where Δt_{coin} is the coincidence window used to identify entangled photon pairs, is negligible ($< 1\%$) when a sufficiently short coincidence window ($\Delta t_{coin} \leq 5$ ns) is used. Further, the accidental rate can be estimated by finding the number of coincidences between Alice's measurements and Bob's measurements shifted by a few coincidence windows and then subtracted from the results.

One method to estimate the PDTC of the free-space channel from the measured rates is to divide Bob's singles rate (N_B) measured over the link by the mean value of Alice's singles rate ($\bar{N_A}$) leaving the link efficiency, $\eta_{B_{link}}$. The validity of this method assumes that Alice and Bob's detection setups are equal in terms of fluctuations and losses and that Alice's local detection events are Poissonian distributed, which is the case. However, one remaining problem is that Bob's singles rate will be inflated by any background photons entering his telescope, ie. $N_{background}$, resulting in the PDTC being artificially shifted towards higher transmission values. By carefully estimating the background photon detection rate one can subtract it from Bob's singles rate and arrive at a fairly good estimate for the free-space link PDTC

Without the results of a local experiment to measure the efficiencies of the system optics minus the free-space channel this is the only method available to estimate the free-space PDTC from the count rates. However, with a local experiment in hand to calibrate out the efficiencies of all the system components, it is possible to perform the more accurate estimation technique alluded to above. To do so, I divide the coincidence rate (N_{coin}) observed during a link experiment by Alice's local single photon count rates (N_A) which gives the total PDTC for Bob including all of the losses in his equipment. Then, using the estimate from the local experiment, I divide out the losses from Bob's equipment leaving only the contribution from the free-space channel. This is more accurate than using just the singles rates since the only source of error is the accidental coincidence rate ($N_{accidental}$) which I have already argued is negligible and can be estimated and removed if necessary.

For each of these methods, the data is broken up into blocks of a certain duration which we call the block duration and then the efficiency is estimated for each block using one of the two methods above. These results are then summed up into a histogram, normalized, and displayed as the PDTC for that link. For the data taken with my entanglement based free-space QKD system I applied the more accurate method using the measured coincidence

rate since I had access to a local experiment estimating Bob's optical efficiencies without the free-space link. However, for the Tenerife data shown subsequently, Bettina had to make use of the estimation method using the singles rates as we did not have access to a local experiment. The Tenerife data, analyzed by Bettina, is included since it shows the results for a much longer free-space link (144 km) to compare with the results from IQC's free-space link (1.3 km).

I studied three different scenarios with my system for the distribution of entangled photons over free-space channels with the following conditions: a maximum free-space transmission with optimized pointing and focusing parameters (Fig. 3.8 (a)), a transmission with artificially increased turbulence using a heat gun placed under the sending telescope (Fig. 3.8 (b)), and a defocused transmission as a way to simulate larger losses (Fig. 3.8 (c)). In all cases, the distributions are shown with a block duration of 10 ms since it has been shown that this is the typical timescale for atmospheric turbulence [108]. All measurements were performed on August 24, 2011 between the hours of 12 and 1am, with a total data acquisition time for each experiment of 3 minutes.

Fig. 3.8 (a) shows that we experienced extremely good atmospheric conditions during the experiments since the observed transmission coefficient for the well aligned link was very close to a Poissonian distribution. The defocussed transmission case, Fig. 3.8 (c), is also very close to a Poissonian distribution only narrowed with a decreased overall transmittance compared to Fig. 3.8 (a). This is expected since defocusing the beam increased it to a size larger than the receiver telescope thus causing fluctuations in the transmission efficiency experienced over the free-space link to be smoothed out (ie. causing it to be even closer to a Poissonian distribution) while at the same time lowering the overall transmittance since many more photons missed the receiver telescope and consequently were not collected and measured. For the experiment where turbulence was artificially added by letting the beam pass over hot air produced by a heatgun, Fig. 3.8 (b), the distribution indeed changes towards one which starts to resemble a log-normal distribution as predicted, albeit an imperfect one owing to the imprecise technique of using a heat gun to increase the turbulence.

In addition to the experiments performed with the IQC free-space QKD system, Bettina also analyzed the 2008 entanglement-based quantum communication experiment performed

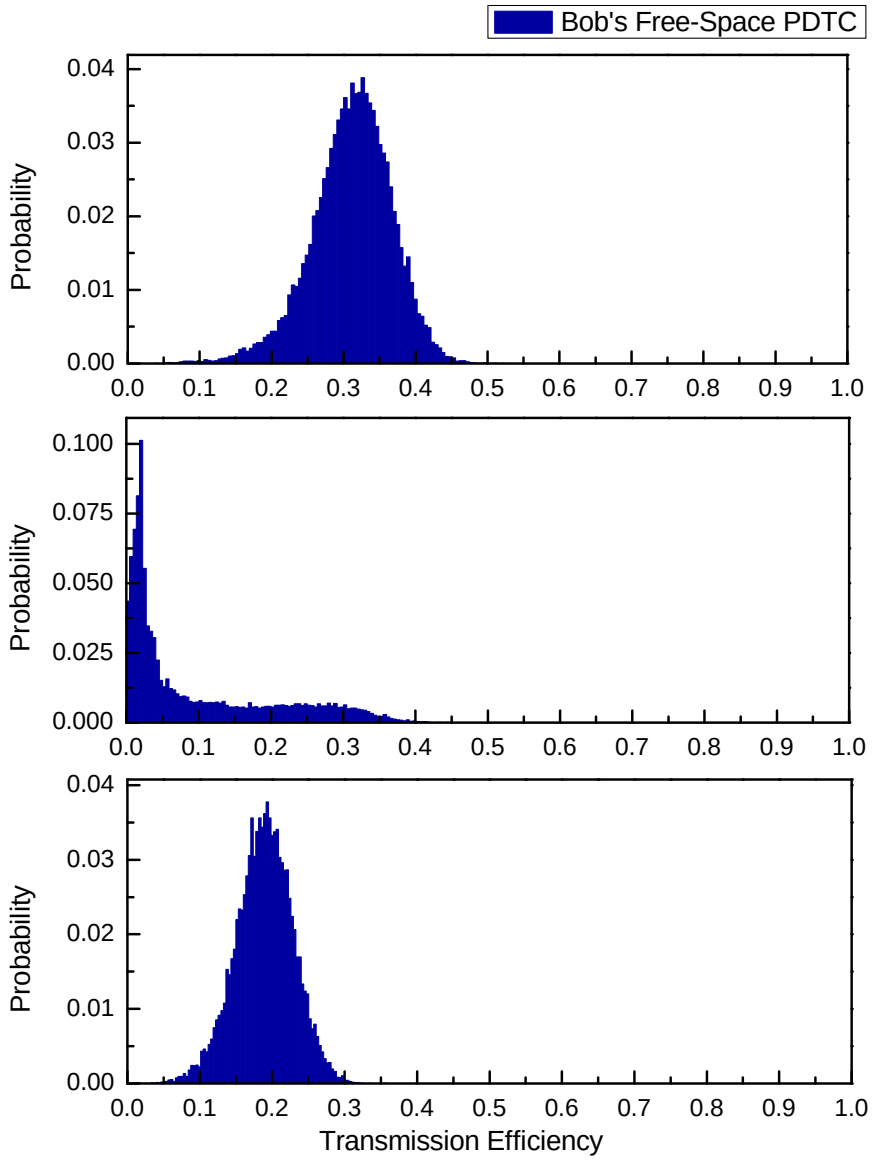

Figure 3.8: Probability distribution of the transmission coefficient (PDTC) for the case of (a) an optimized free-space channel, (b) a free-space channel with artificially increased turbulence using a heat gun placed under the sending telescope, and (c) a free-space channel where the beam is defocused in order to simulate larger losses. The block duration was 10 ms.

over a 144 km free-space link between the two islands of La Palma and Tenerife in the Canary Islands [55, 139]. Here an optical ground station of the European Space Agency (ESA), initially developed for standard optical communication between the Earth and satellites, was used as the receiver telescope. It was oriented horizontally allowing it to be adapted for earth-based quantum communication between the islands. Polarization-entangled photon pairs were produced with an efficient Sagnac interferometric down-conversion source, similar to the one employed in my system.

The experiment demonstrated a violation of Bell's inequality [16, 35] while enforcing the freedom of choice condition. Here, one photon from each pair was transmitted across the 144 km free-space quantum channel, collected by the large receiving telescope and analyzed with an active polarization analyzer, while the other photon was detected locally, after having passed through 6 km of optical fibre in order to ensure space-like separation between the two measurement events. The mean total free-space link attenuation was estimated at 35 dB, where 3 dB was due to the analyzer module. The attenuation due to losses and scattering of the photons transmitted through the fibre was estimated at 20 dB (again including a 3 dB loss from the analyzer module).

Fig. 3.9 shows the corresponding free-space channel PDTC, measured during the night of July 4, 2008. Since we neither had access to coincidence data nor to data from a local calibration experiment Bettina had to estimate the PDTC using the first singles rate method described above, summing Alice's single count rates for a block duration of 2 ms and then normalizing by the mean value of Bob's single count rates. In addition, before calculating the histograms, Bettina carefully corrected the data for the losses from the analyzer module and 6 km fibre mentioned above. The mean background photon detection rate at Alice was also estimated and subtracted from her singles counts. One can clearly see that the PDTC in Fig. 3.9 is very close to an ideal log-normal distribution as predicted and smoother than the data gathered with our inner-city link in Waterloo. The smoothness can be explained by the fact that the atmosphere would have been very calm and homogeneous at those large altitudes above a relatively stable ground consisting mostly of the ocean's surface between the two islands, and the data sample size was larger than our experiments with my system. It is useful to compare this figure with Fig. 3.8 to observe how a short free-space link initially starts out with a Poissonian PDTC and slowly transforms into a

log-normal PDTC as the turbulence is increase either artificially or by adding distance to the free-space link.

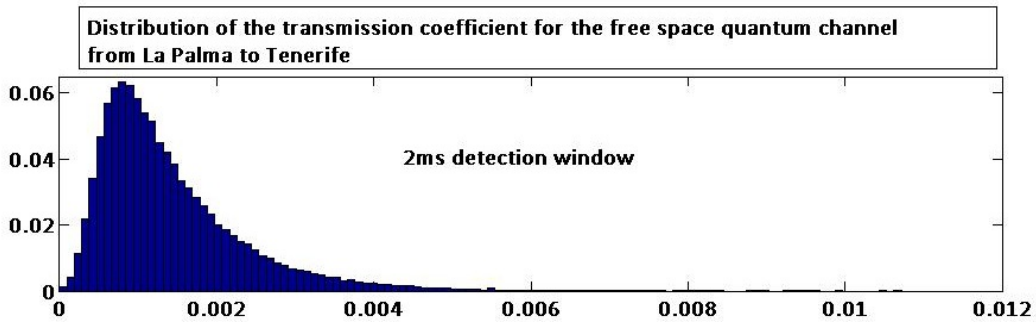

Figure 3.9: Probability distribution of the transmission coefficient (PDTC) for the 144 km quantum channel between the islands of La Palma and Tenerife during a Bell inequality violation experiment performed while enforcing the freedom of choice condition [55, 139]. The block duration was 2 ms.

3.3.3 Improving QKD with a Signal-to-Noise Ratio Filter

Using the link statistics analysis and the data from the experiments above, I then investigated the use of a signal-to-noise ratio (SNR) filter in order to increase the final key rate in QKD systems with a turbulent quantum transmission channel. The idea of the signal-to-noise ratio filter is that during a block of data where the free-space transmission happened to be quite low, the relative proportion of accidental background coincidences (carrying a 50% error rate) to coincident events from real entangled photon pairs is quite high. However, with no way of knowing that they were accidental uncorrelated events they get lumped together with the real entangled photon pair measurements and consequently the quantum bit error rate (QBER) for these blocks is much higher than was actually the case for the real entangled photon pairs. This leads to a higher measured QBER and lower overall secret key rate. However, using an SNR filter which throws away those data blocks where the signal-to-noise ratio is lower than some preset threshold might actually improve the overall secret key rate even though the raw key rate will be lower.

Fig. 3.10 shows (a) Alice (red curve) and Bob's (blue curve) singles count rates measured over the link along with the coincidence count rate (green curve) and (b) the corresponding QBER in the Z (blue curve) and X (green curve) bases when no SNR filter is used for the artificially increased turbulence experiment of Fig. 3.8 (b). Whereas, Fig. 3.10 (c) shows Alice and Bob's singles and coincidence rates when the optimum SNR threshold of 95,000 counts/sec (discussed below) is applied, and (d) shows the corresponding QBER. The data points are grouped using the optimum block duration of 30 ms and a coincidence window of 5 ns for all graphs. Here one can clearly see the high background detection rate experienced by Bob (a situation that will be typical of a QKD link performed to an orbiting satellite) as the flat bottom of his singles rate graph (Fig. 3.10 (a) blue curve), as well as the wildly varying coincidence rates (Fig. 3.10 (a) green curve) where the points close to the x-axis largely consist of accidental coincidences. The SNR idea is neatly illustrated here by looking at the many high QBERs in Fig. 3.10 (b) associated with Bob's low singles and coincidence rates from the top graph. For the experiment corresponding to Fig. 3.8 (a) for the well aligned link I measured the real QBER as $\sim 2.34\%$; however; the QBER observed for the turbulent link corresponding to Fig. 3.8 (b) and Fig. 3.10 (a) and (b) was instead $\sim$5.51%. This increase in the measured QBER over the actual QBER of the system will lower the final secret key rates. However, one can see that when the high loss regions are removed from the singles and coincidence graph (Fig. 3.10 (c)) using the optimum SNR filter, many of the corresponding over-estimated QBERs (Fig. 3.10 (d)) are also removed. Thus, I was able to lower the measured QBER from $\sim$5.51% to $\sim$4.30%, a value closer to the intrinsic error rate of the system, allowing the system to generate many more secret key bits than would otherwise be possible.

The secret key rate formula for my system expressed in secret key bits per raw key bit is given by [97] (see Sec. 2.4.4)

$$R = \frac{1}{2}(1 - f(e)h(e) - h(e)) \tag{3.26}$$

where $f(e)$ is the error correction inefficiency as a function of the error rate, normally $f(e) \geq 1$ with $f(x) = 1$ at the Shannon limit, and $h_2(e) = -e \log e - (1 - e) \log(1 - e)$ is the binary entropy function. For the clarity of the argument I have used the infinite key limit formula; however, the insights gained transfer to the finite key limit in suitable

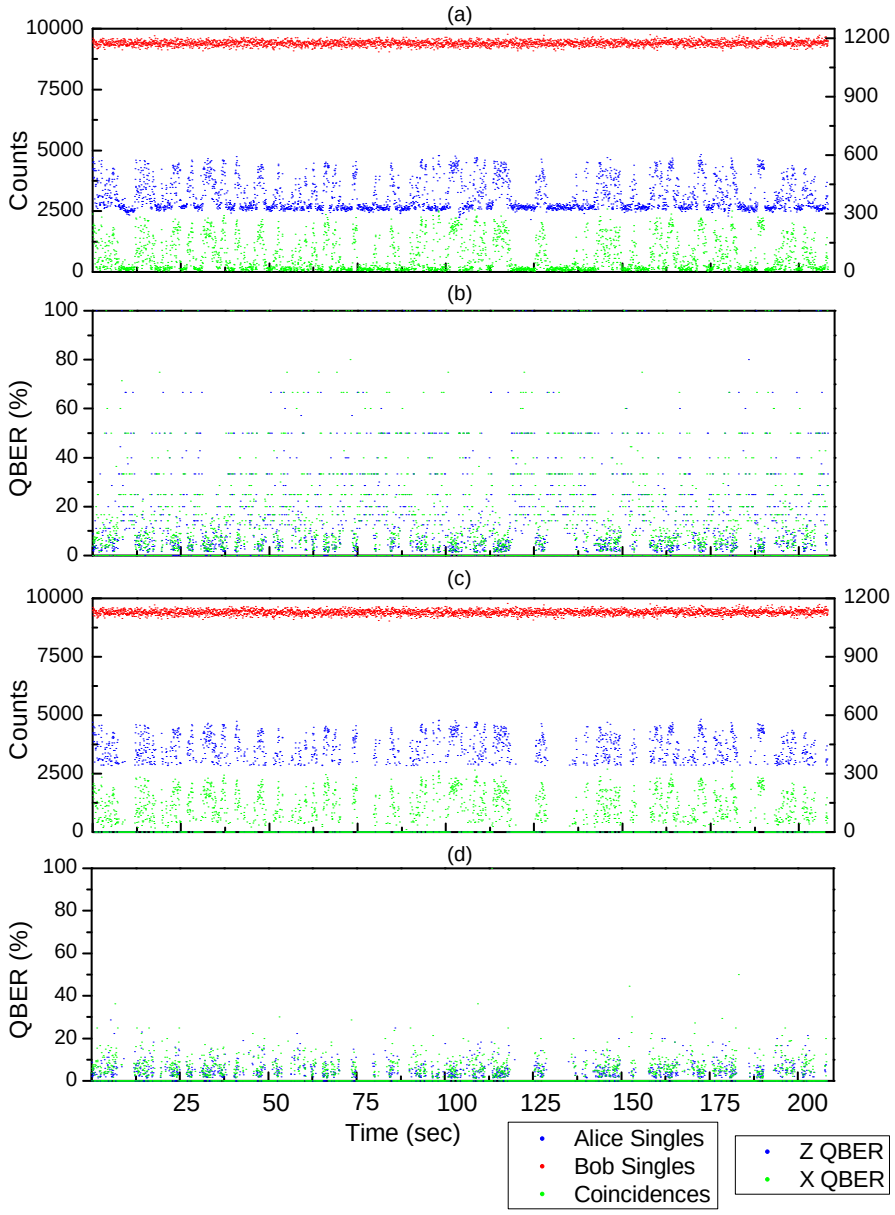

Figure 3.10: Alice's single count rate (red curves), Bob's single count rate (blue curves), the coincidence rate (green curves), and QBER in the Z (blue curve) and X (green curve) bases for the high free-space turbulence experiment of Fig. 3.8 (b) for the case of (a-b) no SNR threshold filter and (c-d) the optimum threshold filter of 95,000 singles/sec. The optimum block duration of 30 ms and a coincidence window of 5 ns were used.

scenarios. Looking at Eq. 3.26, one can see that a higher QBER is detrimental to the final key rate for two reasons (a) increased error correction and (b) increased privacy amplification. The Cascade algorithm [29, 150] and low density parity check (LDPC) codes [61, 100, 117, 104] mentioned previously are the two most commonly employed error correction algorithms used in QKD systems. Both of these algorithms are most efficient, and by that I mean they reveal the least amount of information about the key, for lower error rates. As the QBER climbs the number of parities revealed (and correspondingly the information about the key which has to be accounted for in privacy amplification) increases. Privacy amplification is used after error correction to squeeze out any potential eavesdropper and ensure that the probability that anyone besides Alice and Bob knows the final key is exponentially small at the cost of shrinking the size of the final key. Privacy amplification is commonly accomplished by applying a two-universal hash function [33, 83] to the error corrected key and then using Eq. 3.26 to determine how many bits from this operation may be kept for the final secret key. Both the number of bits exposed during error correction and the measured QBER are used to determine the final size of the key. Additionally, the secure key rate formula is a non-linear function of the QBER so that decreasing the QBER does better than a linear improvement in the final key rate. Thus, the more efficient I can make the error correction algorithm and the lower I can make the measured QBER, the larger the final key will be.

The use of an SNR filter could potentially open a loophole in the security proofs for QKD since I am now throwing away data (which is typically not allowed by the proofs) depending on Bob's measured singles rates. However, I implement the SNR filter on Bob's singles rate which is a sum over all of his detectors during a block of data, so the SNR filter is detector independent. Additionally, throwing away data should be equivalent to a decrease in the channel transmission efficiency (which could happen anyways due to atmospheric effects) and thus should not affect the security proof. Therefore, for this work I assume that using an SNR filter does not compromise the security of my system; however, it remains an open question whether security can be proven for this scenario.

3.3.4 Experimental Results and Discussion

After performing some initial simulations which showed the promise of the SNR idea, I proceeded to implement the idea using the data gathered during the artificially increased turbulence experiment of Fig. 3.8 (b). There are three main parameters which affect the total secret key length using the SNR filter idea: the block duration, the SNR threshold, and the coincidence window. The block duration refers to the time-scale on which the SNR idea is applied and its optimum should be related to the time-scale of the atmospheric turbulence. The optimum SNR threshold should be related to the mean background count rates observed during the experiment. Fig. 3.11 shows the results of this analysis, with the total secret key length plotted against the block duration and the SNR threshold, for a coincidence window of 5 ns.

The key lengths for the lower SNR thresholds in Fig. 3.11 essentially show the secret key length one would expect without implementing the SNR idea (since little if any raw key is thrown away). As the SNR threshold increases though (moving to the right in Fig. 3.11), one can clearly see that the total secret key length also increases until reaching a maximum at which point it quickly falls off since the SNR threshold cuts out too much raw key. Less obvious from the figure, but still important, there is a gradual improvement in the secret key length as the block duration shrinks until a maximum is reached at which point the secret key length gradually decreases once again. The optimum parameters for this data set were to use a block duration of 30 ms and a SNR threshold of 95,000 counts/sec which increased the total secret key generated to 97,678 bits from the 78,009 bits generated when no SNR threshold was used. This represents an increase of 25.2% in the total secret key generated from the *same* amount of raw key.

As mentioned earlier, the secret key rate given by Eq. 3.26 is improved due to two effects. First, the intrinsic error rate in the data is smaller causing the efficiency of the Cascade error correction algorithm [29, 150] used here to be improved from 1.2631 for the case of no SNR threshold to 1.2202 when a SNR threshold is used. This increased efficiency translates into fewer bits revealed during error correction and thus fewer bits sacrificed during privacy amplification. Secondly, the QBER measured during error correction is smaller, 4.30% with an SNR threshold versus 5.51% with none. This translates into less privacy amplification

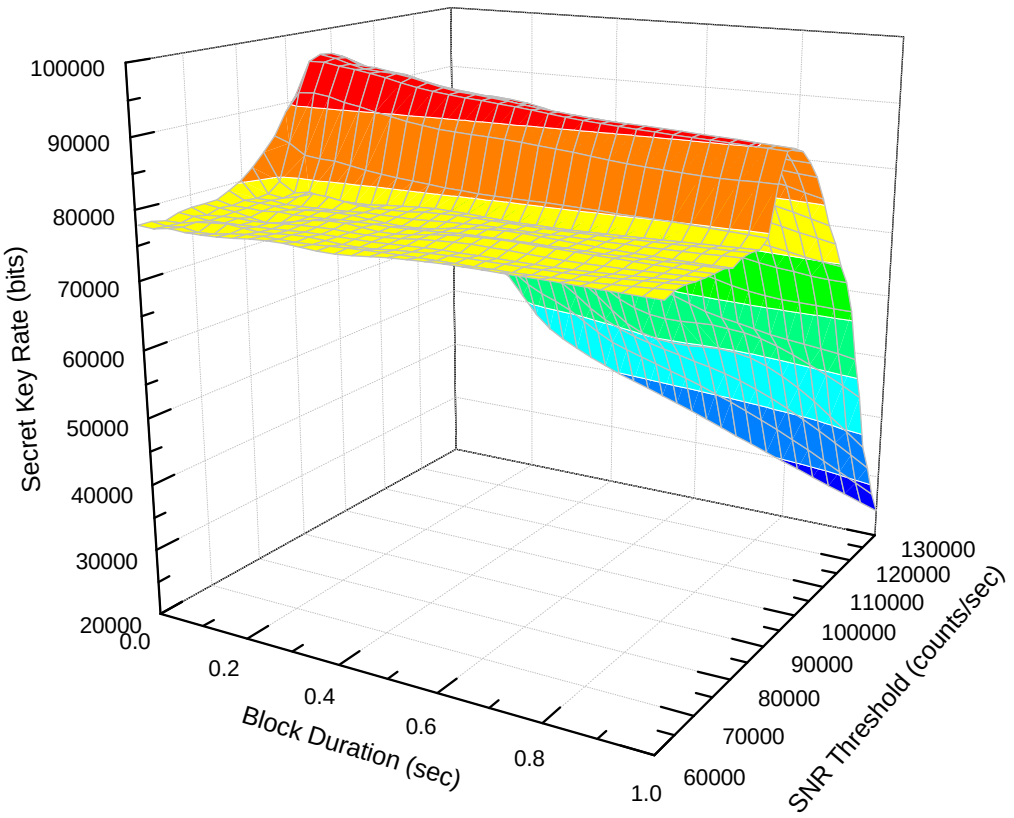

Figure 3.11: The final secret key length for the high free-space turbulence experiment of Fig. 3.8 (b) plotted versus the block duration and the SNR threshold, using a coincidence window of 5 ns.

needed to ensure that the final secret key is secure against an eavesdropper.

Scenario	raw key	sifted key	secret key	f	qber
No SNR filter	535,530	259,855	78,009	1.2697	5.51%
Above SNR filter	466,441	226,279	97,678	1.2202	4.30%
Below SNR filter	69,089	33,576	-	-	13.77%

Table 3.7: Measured values for: directly generating key, using the SNR threshold filter to generate key, and data discarded by the SNR threshold filter, for the high free-space turbulence experiment of Fig. 3.8 (b). The optimum SNR threshold of 95,000 singles/sec, optimum block duration of 30 ms, and a coincidence window of 5 ns were used.

In order to aid a potential future security analysis of the SNR threshold idea, I also document a few other measured values pertinent to its implementation which are summarized in Tab. 3.7. For the data set shown in Fig. 3.11 (using the optimum SNR threshold of 95,000 singles/sec, optimum block duration of 30 ms, and a coincidence window of 5 ns) the SNR algorithm kept 466,441 coincidences which made up the raw key while rejecting 69,089 coincidences generated from data blocks that were below the SNR threshold. The size of the sifted key, where both Alice and Bob measured in the same basis, was 226,279 bits while 33,576 bits were rejected by the SNR thresholds. As mentioned before, the QBER in this sifted key was 4.30% while the QBER in the rejected data was 13.77%. Here one can clearly see how utilizing the SNR threshold was able to increase my overall secret key rate by rejecting this small subset with a much higher QBER.

While the preceding discussion nicely illustrated the usefulness of using the SNR filter idea to produce a larger final key length from the same raw key rates, there are at least two other possibilities for future work to augment the protocol. The ideas are similar with the first being to use an adaptive block duration which expands and contracts depending on the single photon rates being observed. The optimum block duration of 30 ms found in this experiment was in a way a compromise since there will be blocks for which the first part of it had high fluctuations while in the second part of it the fluctuations settled down. With an adaptive algorithm it would be possible to match the block duration more closely to the actual physical SNR variations during an experiment and thus increase the

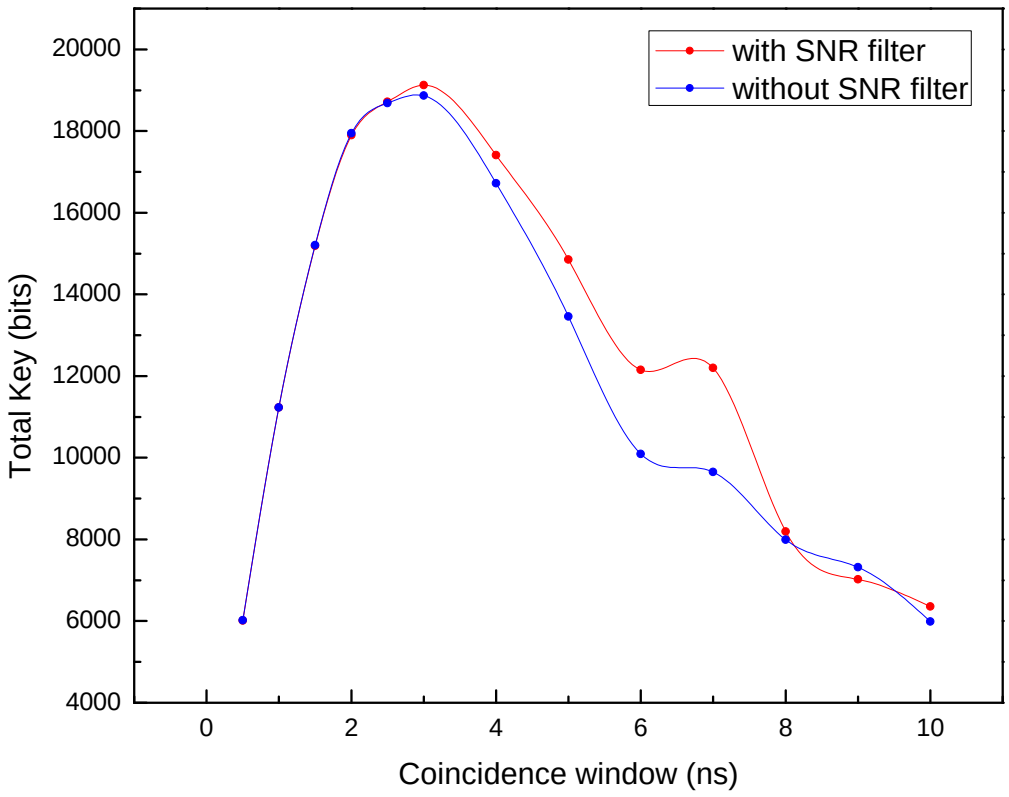

Figure 3.12: The final secret key length for the high free-space turbulence experiment of Fig. 3.8 (b) plotted versus the coincidence window using the optimum detection window for the case of the optimum SNR threshold filter (red curve) and no SNR filter (blue curve). While a narrower coincidence window of 3 ns actually would have produced the highest secret key length, with minimal help from an SNR filter. I used a larger coincidence window in the data above to simulate the higher background environment which a satellite QKD mission will experience. Also, the system currently operates close to the lower limit for possible coincidence windows due to detector jitter and GPS clock accuracy and these limitations will only increase in a satellite mission.

proportion of good transmission periods kept even more. The second idea would seek to examine how the signal (singles rates) are correlated with the QBER (for instance, by plotting a 3D frequency (z-axis) histogram of signal (x-axis) versus QBER (y-axis)). With this correlation plot, one could try to predict what the most likely QBER would be for a given signal level. Then one could apply a finer filtering scheme, for instance, grouping data blocks into the three classes: low QBER, medium QBER ($< 11\%$), and high QBER ($> 11\%$). Certainly the high QBER blocks should be discarded because they actually cost key. But while the medium QBER blocks may still have a QBER higher than that of the intrinsic system due to background light, they would still contribute positively to the key. Processing them separately from the low QBER blocks however would allow one to optimize the algorithms used for each subset to make them as efficient as possible[12].

Lastly, while fairly obvious, it is important to note that the SNR filter idea is only helpful in cases with a high background where the accidental coincidence rate approaches the same order of magnitude as the QKD signal. This is in fact why Fig. 3.11 is plotted for a coincidence window of 5 ns. By using a slightly longer coincidence window I essentially artificially increased the relative size of the accidental coincidence rate in order to illustrate the usefulness of the SNR threshold idea in a situation with a larger background. Fig. 3.12, which plots the secret key lengths obtained with (red curve) and without (blue curve) an SNR filter, shows that decreasing the coincidence window to 3 ns actually produced the highest secret key length with minimal help from an SNR filter. However, recent work for the case of performing QKD with an orbiting satellite[26] has shown that one will indeed be operating in a high background regime where the SNR threshold idea will prove very useful.

Further to this point, depending on the level of the background noise, the simulations I performed (see Fig. 3.13) demonstrate that the SNR threshold idea can be used to produce

[12]For example, in the Cascade error correction algorithm, the algorithm chooses the best block sizes and is most efficient when the actual QBER stays close to the assumed QBER. In my implementation I usually used the last recorded QBER or an average of, say, the last five QBERs as an estimate to choose the block size. But in a situation where the QBER can vary so wildly, it would likely be extremely advantageous to split up the data into two subsets (low and medium QBER) and run error correction on each subset separately.

a secret key when the background would otherwise have prevented it. Fig. 3.13 plots the secret key rate for a QKD experiment performed with an orbiting LEO satellite (simplifying the losses into one log-normal PDTC distribution with a mean loss of 30 dB and a variance of $\sigma = 1.8$ dB) carrying a 100 MHz entangled photon source with a link duration of 10 mins for various background counts. Here, the SNR filter idea would allow me to generate secret key from many more satellite passes that would otherwise have been useless due to the high free-space link fluctuations and low SNR experienced. Additionally, my system already operates close to the lower limit of roughly 1-2 ns for possible coincidence windows due to detector jitter and the accuracy of my GPS synchronized clocks, and I would only expect these limitations to increase in a satellite experiment. Thus, I am very confident that the SNR threshold idea will prove extremely useful in high background situations such as in satellite QKD, long distance terrestrial free-space links, or daylight QKD experiments.

3.4 Conclusion

To conclude this chapter, I have detailed three projects focused on increasing the key rate of my free-space QKD system in order to extend its capabilities into a more practically interesting regime. I began by describing the implementation of the idea of Lo *et al.* [92] to use a biased basis choice in order to increase the efficiency of the secret key generation from 50% (due to a symmetric basis choice) asymptotically towards 100%. While one can only truly reach a 100% efficiency for the case of an infinite key length, I was able to improve the efficiency from 50% to 89.5% for key sizes that will be comparable to those generated in satellite QKD experiments. Thus, the biased basis idea will indeed be extremely useful in future satellite QKD missions to extract as much key as possible from the same amount of raw data. In addition to the efficiency improvement, during this experiment I also made one of the first attempts at a security proof which took into account finite size key statistics for the biased basis idea. Improvements and optimizations to the Cascade error correction algorithms were also implemented and studied, information that will be very useful for future systems.

The second project focused on the construction of a new entangled photon source based

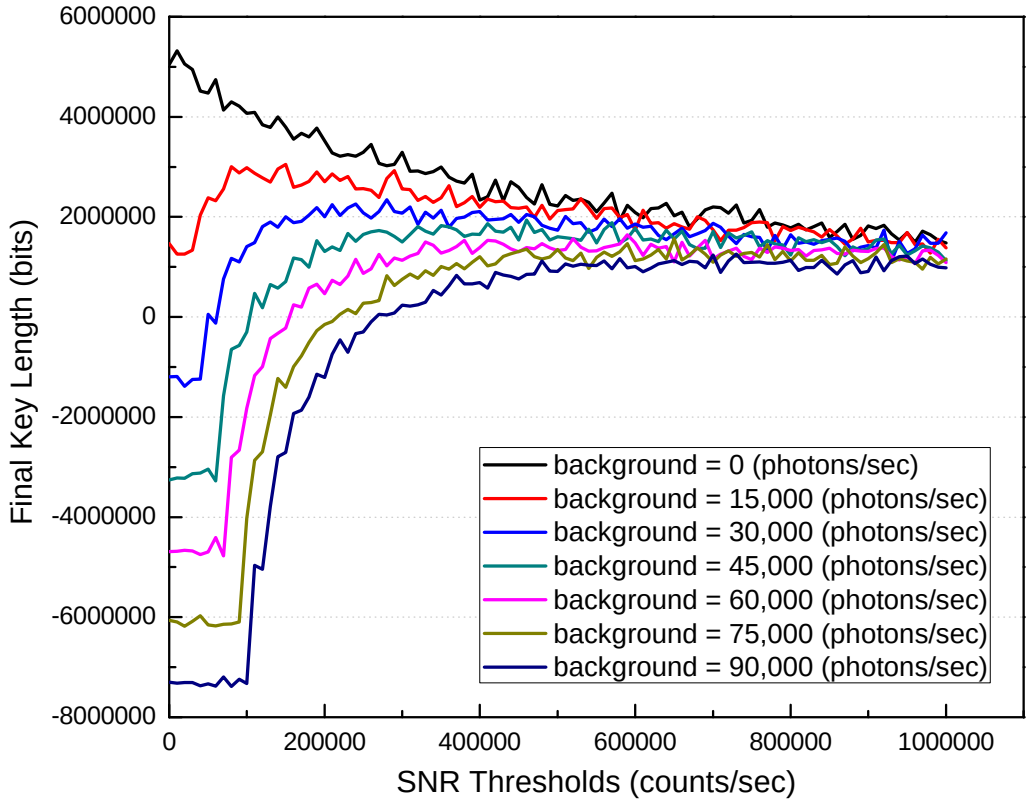

Figure 3.13: The simulated final secret key rate for a satellite QKD experiment (simplifying the losses into a single log-normal PDTC) for various background count rates. I assume the entangled source on the satellite operates at 100 MHz and a free-space PDTC curve for the satellite transmission with a mean loss of 30 dB and $\sigma = 1.8$ dB (typical of a LEO satellite experiment).

on a Sagnac interferometer invented by Shi and Tomita [146] and further developed and optimized by Kim *et al.* [77, 164] and Fedrizzi *et al.* [54]. I gave a general description of parametric down-conversion (the physical process used to generate correlated photon pairs) and quasi-phase matching (a technique used to achieve phase matching in non-birefringent crystals) before briefly mentioning work on previous entangled sources. I then detailed the design of my source and all of the setup and alignment procedures necessary to optimize its operation. Lastly, I discussed some of the performance metrics for the new source showing that it was almost two orders of magnitude brighter than my first generation source (see Sec. 2.4.1). Further it had a much narrower bandwidth of 0.23 nm allowing for the possibility of much stronger spectral filtering in order to operate the QKD system under twilight and daylight conditions. One potential drawback I noted with the higher photon rates was an increase in the QBER due to the production of many more double pair emissions when the source was run at high powers.

The last project I completed had two objectives: the first was the study of the free-space channel through which the entangled photons travel and the second was the investigation of utilizing a signal-to-noise ratio filter in order to improve the efficiency of the key generation much like the biasing idea. For the first objective, I measured the probability distribution of of the (free-space) transmission coefficient (PDTC) for my system for the cases of optimal alignment, artificially increased turbulence, and defocused alignment. I showed that as the turbulence increases, the PDTC curve does in fact transition towards a log-normal distribution as theoretically predicted. For the second objective, I implemented an SNR filter on the data from the artificially increased turbulence experiment to determine whether it could increase the key generation efficiency by removing blocks where a low SNR was observed, thus lowering the overall QBER and increasing the amount of final key generated. I was able to show that for a coincidence window of 5 ns, the optimum block duration of 30 ms, and the optimum SNR threshold of 95,000 counts/s I could increase the final key generated 25.2% from the *same* amount of raw data. This has obvious implications for improving the secret key rate in many satellite QKD missions. Additionally, I showed through simulations that the SNR idea has the potential to allow many more successful key distributions during passes where high background and turbulence are experienced.

Chapter 4

Implementing Oblivious Transfer in the Noisy-Storage Model

As I have shown with my own work in Chs. 2 and 3, and with the multitude of references therein; quantum cryptography is a very active area of research. It has come a long way both in the theory of its security [105, 149, 64, 133] and its experimental implementations [31, 102, 140, 66, 48, 104, 118, 132]. However, almost all of the experimental work has focused exclusively on the cryptographic primitive of key distribution using quantum means. Yet there are many other cryptographic primitives which can make use of quantum mechanics to aid in their security. Oblivious transfer is just such a primitive and has the potential to be extremely useful in 21st century cryptography since, among other things, it can be used to construct a secure identification scheme [38] that might soon be used to ensure security at ATM machines and over the internet. This is a simple cryptographic task currently implemented with classical cryptography which has repeatedly been hacked and broken costing companies millions of dollars. In fact, I would argue that its incredible usefulness over such a short distance (thus avoiding many of the technological hurdles facing the distribution of quantum states in QKD) makes it *the* most important and commercially viable quantum cryptographic primitive around.

This chapter describes the first experimental implementation of oblivious transfer in the noisy storage model. As we will see, there are a number of tradeoffs and assumptions I

needed to make in order to ensure security for my system implemented with today's technology. However, my hope is that as more people recognize the importance of this protocol we will see the same explosion in experimental development as we did for QKD, helping to improve the security proofs and technology to make oblivious transfer a commercial reality. This chapter begins with some background by reviewing the noisy storage model (Sec. 4.1.1) before detailing one of the simpler oblivious transfer protocols (Sec. 4.1.2); then a description of the experimental implementation is given (Sec. 4.2) paving the way for my development of an adapted oblivious transfer protocol capable of being implemented with my system (Sec. 4.3); security of the system is then discussed starting with measurements of the relevant experimental parameters (Sec. 4.4.1) and their subsequent use in the security analysis (Sec. 4.4.2); finally the experimental results (Sec. 4.5) and a discussion of their implications (Sec. 4.6) is given followed by some conclusions (Sec. 4.7).

This work was done in collaboration with Dr. Stephanie Wehner from the Center for Quantum Technologies at National University of Singapore. Stephanie has been responsible for much of the recent work on the theoretical security of oblivious transfer in the noisy storage model. Stephanie provided me with some of her Mathematica code analyzing the security of oblivious transfer for other situations which I adapted to my particular experimental setup. I spent a lot of time investigating the security analysis in order to find a secure regime for my system. In addition to building the new Sagnac interferometric source (discussed in Sec. 3.2), which was necessary in order to decrease the QBER to a level tolerable by the security proofs, I programmed all of the classical post-processing steps necessary to implement the full oblivious transfer protocol including the one-way error correction discussed in Sec. 4.2 and the OT protocol itself. All measurements of the pertinent security parameters were performed by myself and the subsequent security analysis using these parameters was also carried out by me. Finally, I also benefitted from a number of discussions with Marcos Curty from the University of Vigo in Pontevedra, Spain.

4.1 Background

Beginning with work by Wehner *et al.* in 2008 which expanded the bounded storage model into the noisy storage model [137, 160], Koenig *et al.* developed a rigorous theory soon after for the security of various two-party protocols in the noisy storage model in 2009 [80]. Wehner *et al.* [159] and Schaffner [136] quickly used this framework to develop a number of different experimentally feasible protocols that could be implemented using today's technology. Here I layout some background by first outlining the noisy-storage model and then move to detailing one of the first proposed experimental protocols for oblivious transfer.

4.1.1 The Noisy-Storage Model

After quantum key distribution (QKD) was discovered, researchers hoped that it would be possible to use quantum means to develop other advanced cryptographic primitives such as bit commitment and two-party communication. Unfortunately, it was soon shown that almost no cryptographic two-party primitives, save for QKD, are secure if a quantum channel is available and no further assumptions or restrictions are placed on an adversary [106, 91, 90]. A simple way of understanding this is the fact that in QKD Alice and Bob are working together to thwart a potential eavesdropper which affords them more cryptographic power, whereas in most other cryptographic primitives Alice and Bob do not trust each other severely limiting what can be accomplished securely. Thus, one needs to find scenarios that place realistic assumptions on an adversary which allows provable security to be restored. The first such proposal was the bounded-quantum-storage model developed by Damgård *et al.* in 2005 [36] which exploits the technical difficulty of storing quantum information. In the bounded-quantum-storage model, security is ensured based on the assumption that the parties', and by extension an adversarial parties', amount of quantum memory during the execution of a quantum protocol is upper bounded.

This assumption is certainly valid with today's technology judging from the fact that building a scalable quantum memory is one of the major research goals in experimental quantum information processing. However, the hope is that one day large scale quantum

memories will be readily available; thus, one would rather their security did not rest on the fact that their adversary failed to purchase one more gigabyte of quantum RAM. This motivated Wehner *et al.* to develop the noisy-quantum-storage model in 2008 [137, 160] under the assumptions of individual storage attacks and soon afterwards Koenig *et al.* completed the security against general storage attacks [80]. The noisy-quantum-storage model allows one to obtain security under the *physical* assumption that an adversary does not possess a large *reliable* quantum memory and that the noise level of the memory must necessarily increase with the amount of time during which the quantum information needs to be stored. It should be noted that the noisy-storage-model has recently been shown to encompass the case where an adversary has a bounded amount of noise-free storage (ie. the bounded-storage model) [80].

The noisy-quantum-storage model actually captures the difficulty facing an adversary more accurately. While quantum communication can usually be accomplished with very high fidelity using photons that act as the carrier of quantum information; it is the transfer of the photonic qubit onto a different physical system for storage that is noisy. Additionally, current memories either suffer from an inability to maintain the integrity of the quantum information over time, or an inability to perform consistently. That is, the retrieval of the photons in the correct state is possible, but often the photons are lost and the memory acts as an erasure channel. In fact, with current technology, the quantum information stored in a quantum memory is usually lost within a few milliseconds. One might posit that quantum error correction could be used *within* a quantum memory to faithfully preserve the state of the quantum information; however, until an implementation with sufficient control is developed such that error correction can be performed fault tolerantly[1] it will be extremely difficult to maintain unknown quantum states without errors. Thus, security is still ensured unless the process of transferring quantum information between different physical systems can be made error free. A daunting task to be sure. I will make use of the noisy-quantum-storage model in order to ensure security for my implementation of

[1]Fault tolerance refers to the fact that the quantum operations or gates making up the error correction algorithm can themselves contain errors without sufficiently fine control. The fault tolerance threshold theorem establishes the necessary lower bound on the individual gate fidelity such that redundantly encoded qubits can be corrected fast enough to maintain reliable error correction.

oblivious transfer which I describe next.

4.1.2 The Oblivious Transfer Protocol - In Words

In a 1-2 oblivious transfer (OT) protocol we have two parties, Alice and Bob, who interact. Alice holds two secret binary strings S_0, $S_1 \in \{0,1\}^l$ of length l. Bob wishes to learn one of these two strings; the string he learns is given by his choice bit $C \in \{0,1\}$. The protocol is called oblivious transfer for two reasons: first, in learning the string of his choice, S_C, Bob should remain oblivious to Alice's other string, $S_{\overline{C}}$, and thus learn nothing about it; second, Alice should remain oblivious to which string Bob chose to learn, i.e. Alice should not learn C[2]. While the 1-2 OT protocol might at first seem rather trivial, it is in fact quite a powerful cryptographic primitive. Indeed, it can be used to construct a secure identification scheme[3] which has obvious wide ranging applications in every day life.

In order to implement 1-2 OT I actually first implement 1-2 *random* oblivious transfer (ROT) which is then converted into 1-2 OT with an additional step at the end. In the randomized 1-2 oblivious transfer protocol, rather than Alice choosing her two strings she instead receives the two strings S_0, $S_1 \in \{0,1\}^l$ chosen uniformly at random during the protocol. After the random oblivious transfer protocol is complete, Alice can use the random strings she was given as one-time pads to encrypt her original desired inputs $\hat{S}_0$ and $\hat{S}_1$ and send them both to Bob. Bob can then recover Alice's original intended string by using the S_C he learned during the random oblivious transfer protocol in order to decrypt his desired $\hat{S}_C$ and thus complete a 1-2 oblivious transfer protocol where Alice chose her two strings.

The robust ROT protocol I implement is taken from Ref. [136] (suitably modified for implementation with an entangled QKD system) which is capable of handling a practical setting where there are imperfections in both Alice's and Bob's devices as well as errors produced by the quantum communication channel connecting Alice to Bob (Ref. [136] also discusses an idealized protocol). Before starting the protocol, Alice and Bob must

[2]The 1-2 in the protocol name refers to the fact that Alice has 2 strings and Bob learns 1 of them.

[3]As the scheme for how to construct a secure identification protocol using the oblivious transfer primitive is fairly involved, please refer to Ref. [38] for more details.

agree on a security error probability, ε, which gives the maximum probability that the protocol fails (just like in QKD). This parameter can also be seen as a bound on the maximum allowable fluctuations, for example on the various count rates and probabilities, observed during the protocol in order for security to hold. For example, if $p^h_{B,noclick}$ denotes the probability that an honest Bob observes no click in his detector, the corresponding parameter $\zeta^h_{B,noclick}$ captures the observable fluctuations of $p^h_{B,noclick}$ allowed while still maintaining security. Using a $\zeta^h_{B,noclick}$ of order $\sqrt{\ln(2/\varepsilon)/(2n)}$, where n is the number of signals (photons) exchanged, one can use the Chernoff bound to argue that $p^h_{B,noclick}$ should lie in the interval $[(p^h_{B,noclick} - \zeta^h_{B,noclick}), (p^h_{B,noclick} + \zeta^h_{B,noclick})]$ except with probability ε [136]. If a value of $p^h_{B,noclick}$ is observed outside of this range (for example, because of extra loss), the protocol must be aborted (in fact we will soon see that losses are crucial to the security of the protocol).

Error correction is also necessary in the robust protocol in order to correct errors due to the quantum communication channel connecting Alice to Bob, so that Bob can faithfully recover S_C. Error correction must be done with a one-way forward error correction protocol to maintain the security of the protocol. While two-way error correction protocols have been popular in QKD experiments, such as the Cascade algorithm [29, 150], two-way error correction would open up a security loophole allowing Alice to discern Bob's choice bit C (see Sec. 4.2). The error-correcting code is chosen such that Bob can decode faithfully except with a probability at most ε_{EC}. Thus, the protocol failure probability and the error correction failure probability imply that the ROT protocol will succeed except with probability $\varepsilon + \varepsilon_{EC}$.

Now I give the 1-2 ROT protocol developed in Ref. [136] in words. The original protocol assumes Alice and Bob have synchronized clocks and well defined time slots in which Alice prepares and sends one qubit to Bob (à la BB84). We will see in the next section that I need to make a few changes to the protocol in order to adapt it to my experimental implementation with a modified QKD system using entangled states. Luckily all of the jargon described now will carry over when I describe the modified protocol.

Protocol 1: Robust 1-2 Random Oblivious Transfer

1. **Alice picks $x \in_R \{0,1\}^n$ (bit) and $\theta \in_R \{+,\times\}^n$ (basis) uniformly at random.**
   x represents an n bit long bit string which Alice starts with which will eventually be shortened (due to losses) and then divided into two subsets ($\mathcal{I}_0$ and $\mathcal{I}_1$), while θ is a vector (the same length as x) containing the basis that each bit in x was encoded in. In the adapted protocol Alice will no longer pick x and θ but rather they will be given to her by her equipment (think entangled QKD here like in BBM92).
2. **Bob picks $\hat{\theta} \in_R \{+,\times\}^n$ (basis) uniformly at random.**
   Similarly Bob picks $\hat{\theta}$, a vector (again of the same length as Alice's x) which contains the basis he will measure each qubit sent from Alice in. Just like for Alice, in the adapted protocol Bob will no longer consciously pick $\hat{\theta}$ but will rather be given it by his equipment.
3. **For i = 1,. . . ,n: in time slot t = i, Alice sends bit x_i encoded in basis θ_i to Bob. In each time slot, Bob measures the incoming qubit in basis $\hat{\theta}_i$ and records whether he detects a photon or not. He obtains some bit-string $\hat{x} \in \{0,1\}^m$ with $m \leq n$.**
   Bob measures each of the photons sent from Alice which make it to him (remember there is some loss) according to his $\hat{\theta}$ (i.e. in time slot i he measures in the basis given by θ_i) and obtains a shortened (because of the loss) version of Alice's bit string x which he stores in his $\hat{x}$ which is m bits long (where $m \leq n$). Not only will $\hat{x}$ be shortened but it will now contain errors with a probability of 50% every time Alice's preparation basis, θ_i, does not match Bob's measurement basis, $\hat{\theta}_i$, not to mention any errors that might naturally have happened due to the transmission channel.
4. **Bob reports back to Alice in which time slots he recorded a click.**
   Since there were losses Bob needs to report back to Alice in which time slots he recorded a click so that she knows what bits in her original x to keep.
5. **Alice restricts herself to the set of $m \leq n$ bits that Bob did not report as missing. Let this set of qubits be S_{remain} with $|S_{remain}| = m$. If m does not lie in the interval $[(1 - p^h_{B,noclick} - \zeta^h_{B,noclick}) \cdot n, (1 - p^h_{B,noclick} + \zeta^h_{B,noclick}) \cdot n]$ then Alice aborts the protocol**
   With the information from Bob about which qubits he received, Alice now sifts her x down to only those bits where Bob received a qubit (think of the coincidence

algorithm in the entangled QKD protocol sifting Alice and Bob's measurement results down to only coincidences). At this point Alice and Bob's strings, x and $\hat{x}$ respectively, are the same length and, if there were no errors induced by the quantum transmission channel, should match in each position where Alice's preparation basis matched Bob's measurement basis. Alice now needs to check the interval $[(1-p^h_{B,noclick}-\zeta^h_{B,noclick})\cdot n, (1-p^h_{B,noclick}+\zeta^h_{B,noclick})\cdot n]$ which puts a minimum and maximum bound on the number of photons Bob can report as missing. Remember that unlike in QKD, loss plays a much more important role in the security statements and thus it is imperative to constrain the allowable losses Bob can report in order to ensure security[4]. The probabilities which go into this statement are assumed to be measured during the characterization of the OT system. Thus, characterization of the OT equipment before its use is an important requirement which is assumed to have been done. In Sec. 4.4.1 I will characterize all of the parameters which are important for me to prove the security of my experimental implementation. Up until this point the OT protocol looks exactly the same as the BB84 protocol, this similarity will be broken in the next step.

6. **Both parties wait a time Δt.**
   This wait step is necessary to ensure the security of the OT implementation since a cheating Bob must now attempt to store the qubits sent from Alice during this time delay, Δt. However, as I have discussed during the background to the noisy storage model in Sec. 4.1.1, it is assumed that the memory of an adversarial Bob is noisy. Thus, if Δt is made long enough then we can be assured that any quantum information stored by a dishonest Bob sufficiently decoheres.
7. **Alice sends the basis information $\theta = \theta_1, \ldots, \theta_m$ of the remaining positions to Bob.**

[4]It helps to think here of the photon number splitting attack in QKD where decoy state QKD was developed to make sure that an eavesdropper could not allow only the multi-photon emissions through the quantum channel so that they could split off one photon for themselves to keep and measure in the appropriate basis later on at the cost of increasing the loss. In the case of QKD, decoy states are used to make sure an eavesdropper cannot hide their influence in the loss, while in OT a similar idea holds so that one needs to ensure that a cheating Bob cannot report losses too far outside the normal operating conditions of the system.

This is a step that would most certainly not be performed in QKD as Alice and Bob are never supposed to reveal their basis information in order to maintain security. In the setting of OT in the noisy storage model, the wait time, Δt, has allowed us to assume that a cheating adversaries stored qubits have sufficiently decohered. This implies that an adversarial Bob cannot learn both S_0 and S_1 by measuring his stored qubits each in the basis which they were encoded using θ which Alice has just sent him. The security of the protocol under these conditions will be made precise in Sec. 4.4.2.

8. **Bob, holding choice bit C, forms the sets $\mathcal{I}_C = \{k \in [m] | \theta_i = \hat{\theta}_i\}$ and $\mathcal{I}_{1-C} = \{k \in [m] | \theta_i \neq \hat{\theta}_i\}$. He sends $\mathcal{I}_0$, $\mathcal{I}_1$ to Alice.**
   Now Bob forms two index lists, the first list contains all of the indices in x and $\hat{x}$ where his measurement basis matched Alice's preparation basis (i.e. $\theta_i = \hat{\theta}_i$), while the second list contains the indices where the bases did not match (i.e. $\theta_i \neq \hat{\theta}_i$). Remember that Bob's choice bit, C, represents which one of Alice's two strings, S_0 and S_1, he wishes to learn (Alice does not yet have her two strings, S_0 and S_1, she will receive these from the protocol in the next step). Note that it is Bob's choice of labelling of the two subsets, via C, which allows him to choose which one of Alice's strings to receive. Thus, if Bob's choice bit is $C = 0$, then subset $\mathcal{I}_C = \mathcal{I}_0$ represents the subset where his measurement basis matched Alice's and thus he will be able to error correct this subset and perform privacy amplification to arrive at Alice's string S_0. Whereas, the subset $\mathcal{I}_{1-C} = \mathcal{I}_1$ represents the subset where his basis did not match Alice's and thus there will be roughly a 50% error rate between his subset and Alice's which he cannot hope to error correct (without alerting Alice to his choice bit C) and thus he will not be able to learn Alice's string S_1. If his choice bit was instead $C = 1$ the opposite would be true and he would be able to recover Alice's S_1 while remaining oblivious to her S_0. Using the two index lists, $\mathcal{I}_0$ and $\mathcal{I}_1$, Alice splits her x up into the two subsets $x|\mathcal{I}_0$ and $x|\mathcal{I}_1$, while Bob likewise splits his $\hat{x}$ up into the two subsets $\hat{x}|\mathcal{I}_0$ and $\hat{x}|\mathcal{I}_1$. Lastly, remember that Alice *always* receives the two subset lists, $\mathcal{I}_0$ and $\mathcal{I}_1$, thus there is nothing about this communication that would allow her to deduce Bob's choice bit, C.
9. **Alice picks 2 two-universal hash functions $f_0, f_1 \in_R \mathcal{F}$ and sends f_0, f_1 and**

the syndromes $syn(x|\mathcal{I}_0)$ and $syn(x|\mathcal{I}_1)$ to Bob. Alice outputs $S_0 = f_0(x|\mathcal{I}_0)$ and $S_1 = f_1(x|\mathcal{I}_1)$.

Alice encodes syndrome information (extra information about her two subsets, $x|\mathcal{I}_0$ and $x|\mathcal{I}_1$, usually in the form of parity checks) and sends it to Bob so that he can error correct the subset where his measurement basis matched Alice's preparation basis (i.e. in the example in the previous step Bob will be able to error correct subset $\hat{x}|\mathcal{I}_0$ while the syndrome information will not be enough to allow him to error correct subset $\hat{x}|\mathcal{I}_1$. This is because the error rate in the subset $\hat{x}|\mathcal{I}_1$ is much higher since their bases did not match in these cases.). Alice must also enforce a privacy amplification step by choosing a different two-universal hash function to apply to each subset. The privacy amplification step is necessary for two reasons. First, the syndrome information which she sends to Bob gives him some extra knowledge about the subset where their bases did not match (in the example in the previous step Bob learns this information about subset $\hat{x}|\mathcal{I}_1$ which the definition of secure 1-2 OT said he should remain oblivious to). Secondly, an adversarial Bob might have learned some information about this second subset through various quantum attacks which he may successfully have managed to perform sparingly during the protocol. This will show up as a non-zero error rate (QBER). This also needs to be taken into account for security. By Alice applying a different two-universal hash function to each subset and only keeping the maximum number of bits allowed by the OT security formula she can reduce the amount of information an adversarial Bob knows about the second subset to an exponentially small amount, thus fulfilling the security statement of 1-2 OT that Bob only learns one string. The output of the two-universal hash functions applied to Alice's two subsets become her two strings S_0 and S_1 described above in the 1-2 OT protocol.

10. **Bob uses $syn(x|\mathcal{I}_c)$ to correct the errors on his output $\hat{x}|\mathcal{I}_c$. He obtains the corrected bit-string x_{cor} and outputs $S_C = f_C(x_{cor})$.**

    Bob uses the syndrone information for the subset where his basis matched Alice's (in the example above, the $\hat{x}|\mathcal{I}_C = \hat{x}|\mathcal{I}_0$ subset) to correct any errors between his version of the subset and Alice's to arrive at x_{cor} (which is the error corrected version of $\hat{x}|\mathcal{I}_c$). His subset now matches Alice's such that if he applies the same two-universal

hash function (remember Alice sent him the two functions in the previous step) to x_{cor} he will arrive at $S_C = f_C(x_{cor})$, the bit string of Alice's which he wished to learn (in the example above he learns S_0).

11. **To perform 1-2 OT *without* the randomization Alice could add the extra step of using her generated S_0 and S_1 as one-time pads to encrypt her chosen $\hat{S}_0$ and $\hat{S}_1$ as $\hat{S}_0^{enc}$ and $\hat{S}_1^{enc}$ which she could then send to Bob. Bob, using the S_C which he learned in the previous step, can then decrypt $\hat{S}_C^{enc}$ to arrive at $\hat{S}_C$.**

    Remember the original protocol we wanted (so that we could, amoung other things, build a secure identification scheme) is 1-2 Oblivious Transfer with *no* randomization where Alice gets to choose her two strings $\hat{S}_0$ and $\hat{S}_1$. Thus, Alice adds the simple step of using the generated S_0 and S_1 as one-time pads to encrypt her desired $\hat{S}_0$ and $\hat{S}_1$ through the simple encryption operation of a bit-wise XOR via $\hat{S}_0^{enc} = S_0 \oplus \hat{S}_0$ and $\hat{S}_1^{enc} = S_1 \oplus \hat{S}_1$. She then sends $\hat{S}_0^{enc}$ and $\hat{S}_1^{enc}$ to Bob. Bob is then able to use his S_C, which he gained in the previous step, to decrypt $\hat{S}_C^{enc}$ through the operation $\hat{S}_C = \hat{S}_C^{enc} \oplus S_C$. Thus Bob is able to learn $\hat{S}_C$ which is the string, chosen by Alice, that he desired in the original *non*-randomized oblivious transfer protocol.

4.2 Experimental Implementation

Before continuing further, I first discuss my experimental implementation of ROT. This aids in explaining the necessary adaptations of the protocol required due to my implementation with a modified entangled QKD system and helps to outline all of the system parameters that are important when I turn to discussing the security of my system.

As Refs. [159] and [136] mention, while the security of ROT is guaranteed against adversaries that are allowed quantum memories and a quantum computer, the actual implementation of ROT does not require these devices and is possible with today's technology. In fact, it is possible to perform ROT with much of the same hardware used in various QKD setups though modifications need to be made to the classical post-processing steps. However, there are two major caveats. First, the necessary QBER needed to maintain the

security of the system must be much lower ($< 0.956\%$[5]) than typical safe QBER levels for QKD ($\sim 11\%$) which is a challenging experimental constraint. Second, while in QKD loss merely effects the overall key rate of the system, in ROT loss is integral to the security of the scheme. In fact, if not properly bounded, loss may be a show stopper for converting many of the current implementations of QKD into secure ROT devices. Thus, it is important to realize that security in QKD does *not* imply security for OT in the noisy storage model. With these requirements in mind, I proceeded to modify my existing entangled QKD system (described more fully in Chs. 2 and 3 and in Refs [48, 49]) in order to securely implement the ROT protocol.

A schematic layout of the system can be seen in Fig. 4.1. Entangled photon pairs are produced with the Sagnac interferometric entangled photon source detailed in Sec. 3.2. As has been mentioned earlier, the ROT protocol is particularly interesting since it could be useful over very short distances, such as to securely identify oneself to an ATM machine over less than one meter. One could imagine in the future the entangled photon source being part of Alice the ATM and Bob owning a small handheld detection device that he could connect to the ATM, either with a short optical fibre or over a short free-space link but placing his handheld device into a cradle for alignment, in order to authenticate his identity and take out money. To that end, Alice and Bob each locally measure their half of the entangled photon pairs while sitting next to the source connected to it with short single-mode optical fibres. The photons are measured with the same passive polarization detector boxes mentioned before consisting of: a filter to reject background light, a 50/50 non-polarizing beamsplitter (BS) to perform the measurement basis choice, a PBS in the reflected arm of the BS to separate horizontally and vertically polarized photons, and a HWP and PBS in the transmitted arm of the BS to separate photons polarized at $+45^\circ$ and -45°. Avalanche photodiode single photon detectors again convert the photons into electronic TTL pulses which are fed into time-tagging hardware which stamps the electronic signals with the polarization measurement and a highly accurate time of arrival. This information is then transferred into Alice's and Bob's laptops where custom written

[5]The maximum tolerable QBER is dependent upon a number of the parameters going into the OT security proof, the most important of which are the loss and error correction efficiency. It is possible for the maximum tolerable QBER to be relaxed as each of these parameters is improved.

software then performs the rest of the ROT protocol including entangled photon pair identification (based on the measurement times), security checking, sifting, error correction, and 2-universal hashing of the final outputs.

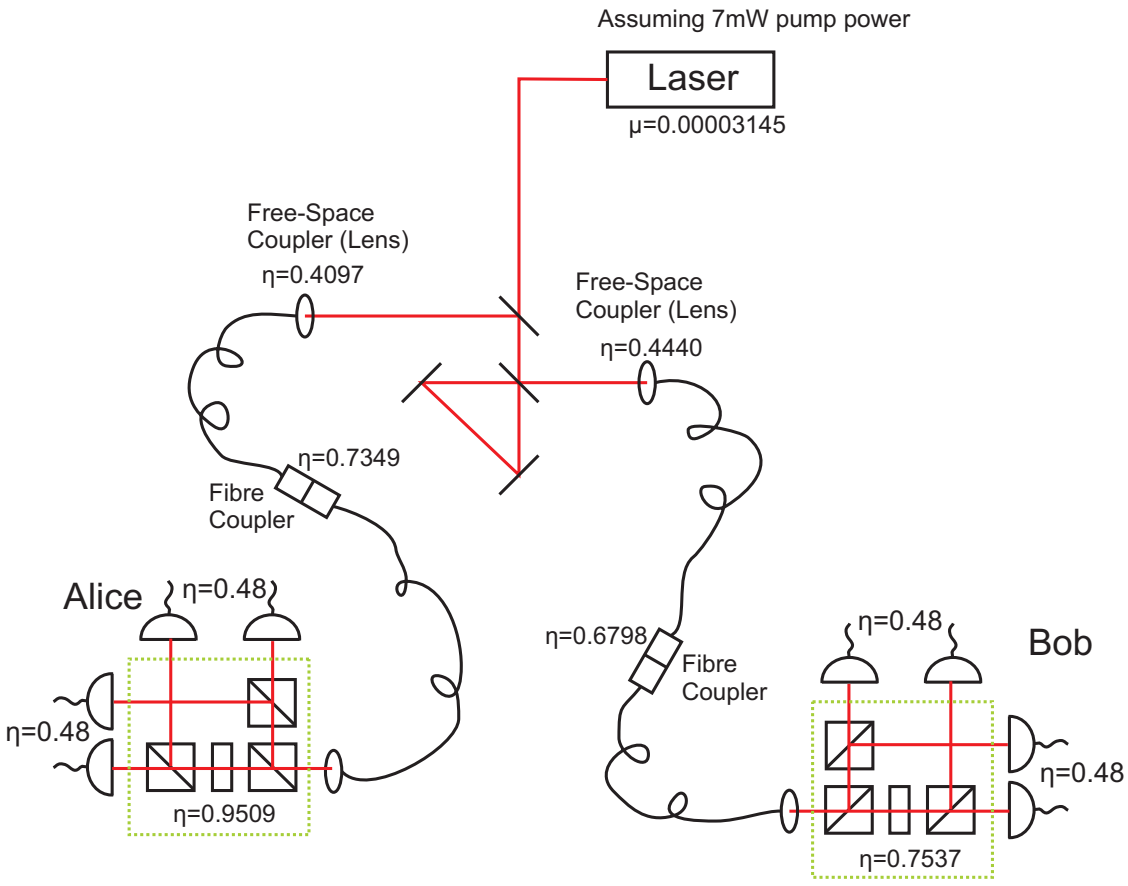

Figure 4.1: Schematic layout of the ROT experiment including all losses experienced in the system.

The biggest modification I had to make to my QKD system, apart from how the ROT protocol differs from a QKD protocol, was to the error correction algorithm used in the classical post-processing. Typically in QKD systems, the error correction is performed with an interactive procedure known as the Cascade algorithm [29, 150]. However, using

this interactive procedure for the ROT protocol would quickly negate the security of the protocol because Alice would very quickly discover Bob's choice bit, C. The reason for this is that Bob could only hope to properly error correct his subset $\mathcal{I}_C$ where his basis choice matched Alice's. If he tried to also perform error correction on the subset $\mathcal{I}_{1-C}$ where his basis choice did not match Alice's, not only would error correction prove impossible due to the number of errors, but Alice would quickly realize that this subset contained many more errors than $\mathcal{I}_C$ and thus Bob's choice bit must have been C. Therefore, in order to maintain the security of the protocol against a dishonest Alice, I needed to implement a one-way forward error correction algorithm so that no extra discerning information flowed back to Alice.

I chose to implement one-way forward error correction using low density parity check (LDPC) codes. LDPC codes were originally invented by Gallager in 1962 [61] but unfortunately were generally forgotten until MacKay and Neal re-invented them in 1997 [100]. LDPC codes have already found their way into a few QKD experiments [117, 104] since it was realized that using one-way forward error correction could relieve much of the classical communication bottleneck that interactive error correction algorithms posed when QKD systems are run at high rates over long distances. For my experiment, I based my LDPC algorithms on Chan's implementation of LDPC codes in a fibre-based QKD system [34, 104] which updates the original LDPC algorithms by MacKay and Neal [100] for the case of QKD according to Pearson [117].

The algorithm is comprised of the following steps. A parity check matrix, $\mathbf{H}$, is used to encode redundant syndrome information[6], $syn(x|\mathcal{I}_C)$ and $syn(x|\mathcal{I}_{1-C})$, about Alice's measurements of her half of the entangled photon pairs split up into the subsets $\mathcal{I}_C$ and $\mathcal{I}_{1-C}$ as defined by Bob. This syndrome information is then sent to Bob as part of the ROT protocol. Bob also calculates the syndrome of his own measurements, $syn(\hat{x}|\mathcal{I}_c)$, where his basis choice matched Alice's. Using the syndrome information sent from Alice, $syn(x|\mathcal{I}_C)$, for the subset of measurements in which Bob's bases choices matched Alice's, $\mathcal{I}_C$, and his own calculated syndrome information, $syn(\hat{x}|\mathcal{I}_c)$, Bob runs Gallager's decoding algorithm

[6]The syndromes are calculated by applying the parity check matrix, $\mathbf{H}$, separately to Alice's measurements in each subset, $x|\mathcal{I}_C$ and $x|\mathcal{I}_{1-C}$ (where the two measurement lists are each grouped into a column vector), according to the normal rules of matrix multiplication, ie. $syn(x|\mathcal{I}_C) = \mathbf{H} \cdot \tilde{\mathbf{x}}_{|\mathcal{I}_C}$.

[61, 100] which is essentially a maximum likelihood estimation using the two syndromes and Bob's measurements as inputs. The decoding algorithm is an iterative procedure that updates the most likely guess of Alice's string, $x|\mathcal{I}_C$, after each iteration. The algorithm stops once the syndrome of the latest guess of Alice's string matches the syndrome Alice sent, or after a specified number of iterations at which point it gives up. Work on good parity check codes is a field in its own right, with randomly generated codes following a few simple rules seeming to perform the best [93]. However, as this is not the focus of this work, I chose to use a hand constructed code with acceptable performance metrics.

After the error correction step is performed, the last thing required is for Alice and Bob to use shared 2-universal hash functions to perform privacy amplification on their outputs. This privacy amplification step is necessary for two reasons. First, to take care of the extra information about the string Bob chose *not* to learn leaked by Alice through the syndrome information sent to Bob; and second, to take care of any information a cheating Bob might theoretically have gained, based on the error rate, about Alice's second string. For this, I make use of the same 2-universal hash functions used in my QKD system developed by Carter and Wegman in 1979 [33]. It is important to note that my implementation of the 2-universal hash functions operates sequentially on blocks of 1022 bits of ROT key, rather than on the whole ROT key at once. It is already known that to maintain security in QKD, an implementation must perform privacy amplification on the *entire* error corrected key of 10^6 bits or more. It is assumed that the same holds true for the security of ROT. However, as this is a first implementation, for simplicity I use my existing algorithms and assume that security still holds for my implementation of 2-universal hashing. It should be noted that currently *no* experimental or commercial QKD systems meet this security requirement for their implementation of privacy amplification [2]; however, an algorithm by Krawczyk [83] does exist which is capable of efficiently hashing large quantities of key at once. This could be used in any future implementations of ROT and QKD.

4.3 The Adapted Oblivious Transfer Protocol

In order to implement ROT by modifying my QKD system, I had to adapt the ROT protocol given in Refs. [136, 159] to my experimental implementation in a number of different ways. Most significantly since I use a continuously pumped entangled photon source, there is no notion of well defined time slots in which Alice and Bob should measure a photon. Additionally, since both Alice and Bob are using passive polarization detector boxes, neither one of them needs to pick a $\theta \in_R \{+, \times\}^n$ uniformly at random which defines how they will measure each photon, instead the protocol gives this to them as one of its outputs. Here I first give the adapted protocol which I implemented, followed by a few words on any additional assumptions necessary to maintain the security of the system and how it reduces to the original protocol given above.

Protocol 2: Robust 1-2 Random Oblivious Transfer Adapted to an Entangled Source Implementation

1. For each photon pair $i = 1, \ldots, n$: if Alice gets a click in one of her detectors, Alice records the basis information as an entry in $\theta \in_R \{+, \times\}^{m_A}$, the bit information in $x \in_R \{0, 1\}^{m_A}$, and the measurement time in $t \in \{\Re\}^{m_A}$.

2. For each photon pair $i = 1, \ldots, n$: if Bob gets a click in one of his detectors, Bob records the basis information as an entry in $\hat{\theta} \in_R \{+, \times\}^{m_B}$, the bit information in $\hat{x} \in \{0, 1\}^{m_B}$, and the measurement time in $\hat{t} \in \{\Re\}^{m_B}$.

3. Bob sends Alice his timing information $\hat{t}$. Alice performs a coincidence search between t and $\hat{t}$ using a coincidence window, Δt_{coin}, which generates a list of indices which she sends to Bob allowing them to sift down to only those measurements where they both detected a photon. Alice and Bob now obtain the bit and basis strings $x \in \{0, 1\}^m$ and $\theta \in_R \{+, \times\}^m$, and $\hat{x} \in \{0, 1\}^m$ and $\hat{\theta} \in_R \{+, \times\}^m$ respectively, with $m \leq n$.

4. Alice has already restricted herself to the set of $m < n$ bits where both she and Bob reported a photon detection. Let this set of qubits be S_{remain} with $|S_{remain}| = m$.

Alice checks whether m lies in the interval $[(1-p^h_{B,noclick}-\zeta^h_{B,noclick})\cdot n, (1-p^h_{B,noclick}+\zeta^h_{B,noclick})\cdot n]$, if it does not then Alice aborts the protocol.

5. Both parties wait a time Δt. This ensures security by causing any quantum information stored by a dishonest party to sufficiently decohere.

6. Alice sends her basis information $\theta = \theta_1, \ldots, \theta_m$ of the remaining positions to Bob.

7. Bob, holding choice bit C, forms the sets $\mathcal{I}_C = \{k \in [m] | \theta_i = \hat{\theta}_i\}$ and $\mathcal{I}_{1-C} = \{k \in [m] | \theta_i \neq \hat{\theta}_i\}$. He sends $\mathcal{I}_0$, $\mathcal{I}_1$ to Alice.

8. Alice picks 2 two-universal hash functions $f_0, f_1 \in_R \mathcal{F}$ and sends f_0, f_1 and the syndromes $syn(x|\mathcal{I}_0)$ and $syn(x|\mathcal{I}_1)$ to Bob. Alice outputs $S_0 = f_0(x|\mathcal{I}_0)$ and $S_1 = f_1(x|\mathcal{I}_1)$.

9. Bob uses $syn(x|\mathcal{I}_c)$ to correct the errors on his output $\hat{x}|\mathcal{I}_c$. He obtains the corrected bit-string x_{cor} and outputs $S_C = f_C(x_{cor})$.

The change from active polarization detector boxes to passive ones should not represent a security threat, as security has been proven for QKD using both techniques. However, it will add to the complexity of the security statement for ROT as the security proofs in Refs. [136, 159] assume active polarization detection with identical detectors (ie. one variable η_D). I make the simplifying assumption that security still holds even though eight detectors, each with slightly different characteristics, are used. Strictly speaking the security proof could be redone with a different variable for each detector; however, special care needs to be taken so that other loopholes [101, 125] are not exposed as a result of the different detectors.

Whereas the original protocol given by Ref. [136] assumes synchronized clocks and well defined time slots in which Alice prepares and sends one qubit to Bob; in my setup a continuously pumped entangled photon pair source is used which emits pairs at random times. Thus, Alice now measures one half of each entangled photon pair to receive her two strings S_0 and S_1 while the other half is sent on to Bob. The biggest difference now is that Alice herself has some loss in her own setup (both from the entangled source and her

polarization detector box). This has no influence on the protocol other than to randomize the strings S_0 and S_1 which were assumed to be random in the first place. However, it does have implications for the security of the scheme.

As a few last comments, it is assumed that Bob learning which photon pairs Alice did not measure does not gain him any security advantage since he must already have chosen which photons to interact with (and possibly store in a memory) before learning which photon pairs Alice missed. Further, Ref. [159] also suggests that a quantum non-demolition (QND) measurement on the photon number in Alice's arm could also be used to conclude whether no photon or too many photons (multi-pair emission) were emitted, allowing Alice to safely discard that round in order to obtain tighter security bounds. Unfortunately, reliable optical QND measurements do not yet exist without introducing additional losses, but they are a theoretical possibility and could be used in future implementations to obtain higher OT rates and better security.

4.4 Theory of Security

I now turn to describing the theory behind the security of ROT. To begin with I layout all of the important experimental security parameters (Sec. 4.4.1) that I need to measure. This is the information I will need to know in order to evaluate the various security statements of ROT (Sec. 4.4.2).

4.4.1 Experimental Security Parameters

In order to prove security for my system I need to characterize the parameters that will be important to me in the security proof. Figure 4.1 shows all of the losses experienced in my experimental implementation. These will be important to define Bob's acceptable reported loss.

To begin with, the security proofs for ROT [136, 159] assumed that the states emitted

by a PDC source can be written as [81]

$$|\Psi_{src}\rangle_{AB} = \sum_{n=0}^{\infty} \sqrt{p_{src}^n} |\Phi_n\rangle_{AB} \tag{4.1}$$

where the probability distribution p_{src}^n is given by

$$p_{src}^n = \frac{(n+1)(\mu/2)^n}{(1+(\mu/2))^{n+2}}, \tag{4.2}$$

the states $|\Phi_n\rangle_{AB}$ are given by

$$|\Phi_n\rangle_{AB} = \sum_{m=0}^{n} \frac{(-1)^m}{\sqrt{n+1}} |n-m, m\rangle_A |m, n-m\rangle_B \tag{4.3}$$

(where the states are written in the basis $|H, V\rangle$), and $\mu/2$ is directly related to the amplitude of the pump laser resulting in a mean photon pair number per pulse of μ. Using this assumption and a few other measured parameters, the authors of Refs. [136, 159] derived all of the other necessary quantities used in their proofs of security. While a good starting point, we shall see later that one might be able to gain much from measuring all of the necessary quantities rather than relying on the model given above.

The first thing that I need to know for security is the parameter μ. For the experimental implementation detailed here, I choose to use 7 mW of pump power. Since I have a continuously pumped source which creates pairs at random times rather than the pulsed source assumed in the model, it is a little more roundabout to estimate μ. To begin with, I measure Alice and Bob's single photon count rates, N_A and N_B, as well as their coincident detection rate, N_{coin}, measured with a coincidence window of $\Delta t_{coin} = 3$ ns (see Table 4.1). I then estimate Alice and Bob's total transmission efficiency (including their source coupling, polarization analyzer, and detectors) using the formula $\eta_{A/B} = N_{coin}/N_{B/A}$ which yields $\eta_A = 0.1374$ for Alice and $\eta_B = 0.1092$ for Bob (see Ref. [30] and Sec. 3.3.2 for more discussion on this method of estimating efficiencies). Using these numbers I can back out the loss and estimate the total number of pairs produced at the crystal with the formula $N = N_A/\eta_A$, which yields $3,145,331$ pairs/sec. Finally to calculate μ, I define my "pulse length" as the coherence time of my laser. The reasoning behind this is that in the security statements μ is used with Eqs. 4.1, 4.2, and 4.3 in order to determine a

bound on the possible double pair emission contributions which might expose additional information to a dishonest party. It is well known with PDC sources that pairs separated by more than a coherence time are independent and thus would not give a dishonest party additional information. It is only those pairs generated within the same coherence time (or equivalently within a coherence length) which might pose a security risk. Thus, with a coherence length of $\Delta l_c = 3$ mm for my laser and a corresponding coherence time of $\Delta t_c = 1.0 \times 10^{-11}$ sec, I can calculate μ using the formula

$$\mu = 3,145,331 \frac{\text{pairs}}{\text{sec}} \left(\frac{1 \text{ sec}}{1 \times 10^{11} \text{ coherence times}} \right) \tag{4.4}$$

where again I have defined my "pulse length" as one coherence time (ie. with $\Delta t_c = 10$ ps there are 10^{11} coherence times per second). This estimation yields $\mu = 0.00003145$.

Experimental Parameter	Value
N_A	432,148
N_B	343,470
N_{coin}	47,197
η_A	0.1374
η_B	0.1092
N	3,145,331

Table 4.1: Source parameters for ROT where N_A and N_B are Alice and Bob's single photon count rates per second, N_{coin} is their coincident detection rate per second, η_A and η_B are estimates for Alice and Bob's total transmission efficiencies, and N is an estimate for the total number of pairs produced at the crystal per second. The source is pumped with 7 mW of power.

There are three other measured parameters that are necessary for the security statements: the total transmission efficiency, η, which can be obtained from Fig. 4.1, the intrinsic error rate (QBER) of the system, e_{det}, and the probability of obtaining a dark count in one of Alice's or Bob's detectors, p_{dark}. The dark count probability is defined similarly to μ (ie. by multiplying the dark count rate per second by $1/10^{11}$ coherence times), and Alice

takes for p_{dark} her average value for her four detectors. the transmission efficiency, η, and the QBER, e_{det}, are measured over the course of the experiment but are needed to discuss the security statements. Their values are summarized in the top half of Table 4.2.

Experimental Parameter	Value
μ	0.00003145
η	0.0150
e_{det}	0.0093
p_{dark}	5×10^{-9}
n	2.704×10^{10}
f	1.5
δ	0.0386
d	2
r	0.01
ν	0.01

Table 4.2: Experimental parameters for ROT where μ is the mean photon pair number per coherence time, η is the total transmission efficiency, e_{det} is the intrinsic error rate (QBER) of my system, p_{dark} is the probability of obtaining a dark count per coherence time, n is the total number (before losses) of entangled photon pairs exchanged, f is the error correction efficiency, δ is a security parameter which must be chosen according to the constraints given in Sec. 4.4.2, d is the dimension of the assumed depolarizing channel (a qubit channel is assumed), r is the probability that the memory (assumed to be a depolarizing channel) faithfully stores the state, and ν is the storage rate of the quantum memory (where a storage rate of $\nu = 0$ means that none of transmitted qubits can be stored, while a storage rate of $\nu = 1$ means that all of the transmitted qubits can be stored). The source is pumped with 7 mW of power.

Next, I turn to the security statements themselves. For these, there a number of quantities (for example: p^1_{sent}, which is the probability only one photon pair is sent; $p^h_{B,noclick}$, which is the probability that an honest Bob receives no click; and $p^d_{B,noclick}$, which is the minimum probability that a dishonest Bob receives no click) which are important. All of these are derived from the PDC model given by Eq. 4.1 with the experimental parameters

given in Table 4.2. For the derivations see Ref. [159]. Additionally, it should be noted that security has been proven for channels[7] which satisfy the strong-converse property, which essentially states that the success probability of decoding a randomly chosen n-bit string sent over the quantum channel decays exponentially for rates above the classical channel capacity, ie. the classical channel capacity is bounded. In order to explicitly evaluate the security statements for ROT one needs to pick a particular channel to analyze. Refs. [136, 159] chose to analyze the d-dimensional depolarizing channel, given by

$$N_r(\rho) = r\rho + (1-r)\frac{\mathcal{I}}{d} \quad \text{for} \quad 0 \leq r \leq 1 \tag{4.5}$$

which successfully transmits the quantum state ρ with probability r and otherwise replaces it with the completely mixed state $\frac{\mathcal{I}}{d}$ with probability $1-r$, as the "typical" channel action of a quantum memory. They specialize to the case of qubits where $d = 2$. I pick the same channel since I use their security analysis for my implementation of oblivious transfer. For a quantum memory, one needs to also define a storage rate, ν, which represents the number of qubits that can be stored in the memory relative to the number sent from Alice to Bob. Thus, $\nu = 1$ means that all qubits sent to Bob can be stored in the memory, while $\nu < 1$ means that Bob can only store a fraction of the qubits sent from Alice. Finally, one must also pick the number of entangled pairs, n, that Alice will attempt to send to Bob, and know the efficiency of the one-way error correction code, f. The assumed parameters are summarized in the bottom of Table 4.2.

4.4.2 Security Analysis

There are a number of different conditions that play a role in determining the security of the experimental implementation of the ROT protocol given earlier in Sec. 4.3. The first is the acceptable security parameter or security error, ϵ, which represents the probability that the protocol might fail. Failure in this context means that the OT key was not distributed securely and an eavesdropper might have significant knowledge of it. From Ref. [136], we

[7]Here, the definition of the strong-converse property is given in terms of the usual language of quantum channels (over which information would pass). To relate back to our setting with a memory the reader can merely replace the language "sent over a quantum channel" with "stored in a quantum memory".

have that the error for ROT is given by

$$\epsilon(\delta) \leq 2\exp\left(-\frac{\delta^2}{512(4+\log\frac{1}{\delta})^2}\cdot m^1\right) \tag{4.6}$$

where $m^1 = (p^1_{sent} - p^h_{B,noclick} + p^d_{B,noclick})n$ (the minimal number of single photon pair rounds). The δ that arises in this formula comes from the conditional smooth min-entropy[8] being lower bounded through the use of a special case of the quantum uncertainty relation [136, 37]. From Eq. 4.6 we can clearly see that the larger we make δ the smaller the security error, ϵ, becomes. However, there is an additional constraint on δ that I need to consider due to a security condition on the classical capacity of the quantum channel representing an adversary's quantum memory which needs to be enforced. Again from Ref. [136], the security condition is given by

$$C_N \cdot \nu < \left(\frac{1}{4} - \delta\right)\cdot(p^1_{sent} - p^h_{B,noclick} + p^d_{B,noclick}) \tag{4.7}$$

where C_N is the classical capacity and ν is the storage rate. From Eq. 4.7 we can immediately see that one requires $\delta < \frac{1}{4}$ to have any hope of finding a secure region. In fact, I would like to choose δ as small as possible so as to make this security condition as easy as possible to fulfill. Thus, to fulfill these two competing conditions I want to choose δ to be the minimum necessary to meet the chosen security error requirement while at the same time assuring security for the largest possible region of parameters.

With these conditions in mind, the first step I need to take in order to start to analyze the security of my implementation is to first choose an acceptable security error, ϵ, that I am willing to tolerate. As seems to be the standard in QKD, I choose $\epsilon = 10^{-6}$ as my security parameter. From Fig. 4.2 we can see that choosing $\delta = 0.0386$ will ensure that $\epsilon < 10^{-6}$, as desired.

Next, I need to check for which parameter regions I can ensure security. For this I require that

$$(p^1_{sent} - p^h_{B,noclick} + p^d_{B,noclick}) > 0 \tag{4.8}$$

[8]The smooth min-entropy is an entropy measure that finds application in many of the latest classical and quantum cryptographic security proofs. For more information please refer to Refs. [136, 37].

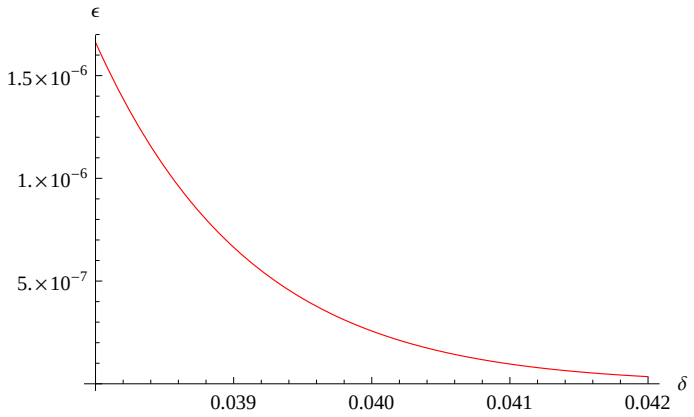

Figure 4.2: Plot of the security error, ϵ, versus δ for ROT.

in order to ensure that the exponent in Eq. 4.6, which gives the security error, is negative so that ϵ becomes sufficiently small. Figure 4.3 (left) shows the possible regions where Eq. 4.8 can be fulfilled and secure ROT can be implemented. Additionally, security requires that I fulfill the condition given by Eq. 4.7. Figure 4.3 (right) shows the possible regions where Eq. 4.7 can be satisfied and security for ROT can be established (shaded region) assuming that an adversary has a noisy memory that acts as a qubit depolarizing channel. Therefore, as long as I implement an experiment with parameters contained in the shaded regions of Fig. 4.3 and I can safely assume that an adversary has a noisy quantum memory that acts as a depolarizing channel, the security of my system will be ensured.

Finally, I am now in a position to explore the ROT length rate formula from Ref. [136] given by

$$l \leq \frac{1}{2}\nu \cdot \gamma^N\left(\frac{R}{\nu}\right) \cdot n - f \cdot h(p^h_{B,err}) \cdot (1 - p^h_{B,err})\frac{n}{2} - \log\left(\frac{1}{\varepsilon}\right) \tag{4.9}$$

where $R = (\frac{1}{4} - \delta)\frac{m^1}{n}$ is the rate at which a dishonest Bob would need to send information through storage, $m^1 = (p^1_{sent} - p^h_{B,noclick} + p^d_{B,noclick})n$ is the minimal number of single entangled photon pair rounds, $m = (1 - p^h_{B,noclick})n$ is the number of accepted rounds, and f is the error correction efficiency relative to the Shannon limit. The next important thing to do is to graph this ROT length rate versus some of the various experimental parameters which I can tune to see what kind of rates I can expect from the system. As it turns out

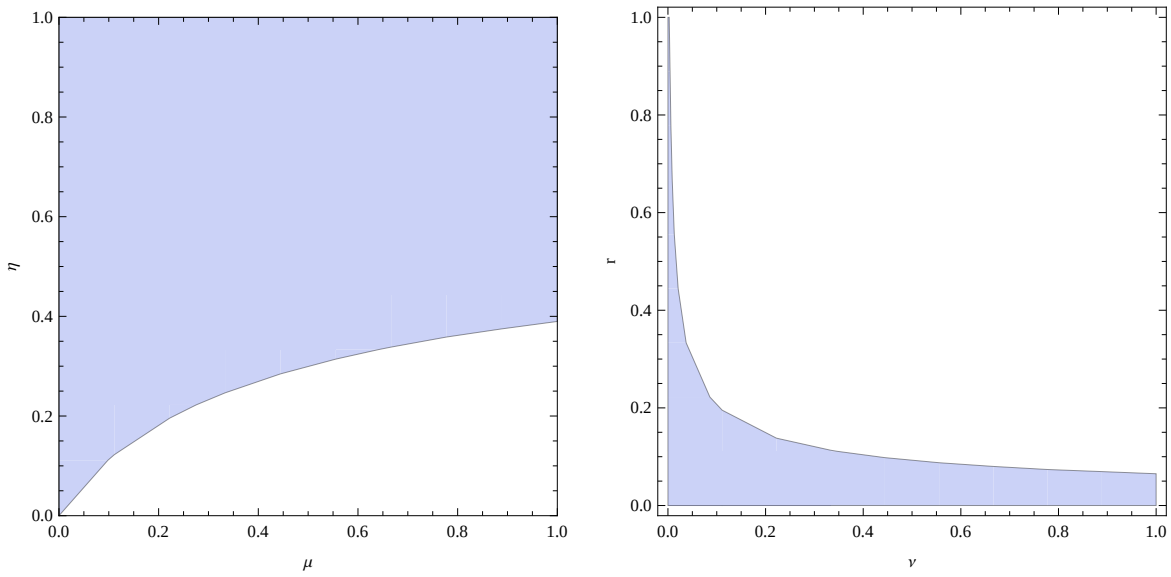

Figure 4.3: Plot of the security conditions given by Eq. 4.8 (left) and Eq. 4.7 (right) assuming an adversary has a noisy quantum memory that acts as a depolarizing qubit channel with noise parameter, r, and a quantum memory storage rate, ν. Security for ROT can be shown for the shaded region.

the ROT length rate is sensitive to four parameters[9]: the depolarizing noise, r; the storage rate, ν; the intrinsic error rate of the system, e_{det}; and the transmission and detection efficiency, η.

Firstly, looking at Figure 4.4, which shows the ROT rate versus the loss, we can see now why the loss is so crucial to the security of ROT. The secure ROT rate quickly drops as the transmission efficiency decreases. Indeed, for certain values of the other parameters (r, ν, and e_{det}) the ROT rate can quickly become negative for relatively large transmission efficiencies, e.g. $\eta > 0.2$.

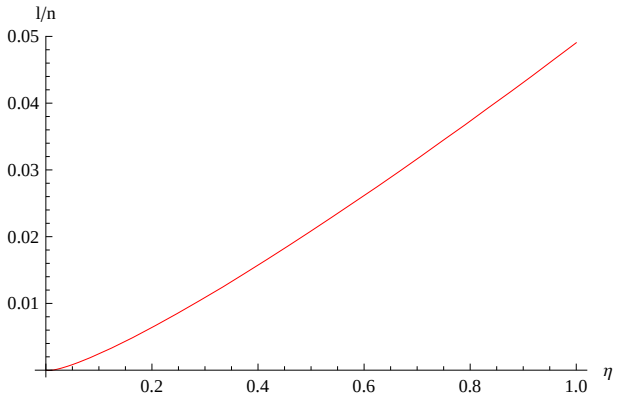

Figure 4.4: Plot of the ROT rate, l, versus the loss, η.

Next I look at the ROT rate plotted against the depolarizing noise, r, and the storage rate, ν, which is shown in Fig. 4.5 (left) and (right). Here we see that a positive ROT rate can be obtained only for a select range of these parameters. The choices in Table 4.2 are made so as to yield reasonable ROT rates for my experimental implementation. However, in general r and ν should typically be set as estimates for the best quantum memories available. I should also mention that the secure range of each of these parameters depends quite sensitively on the values of the other parameters.

[9]Actually, the rate is also sensitive to a fifth parameter, namely, the error correction efficiency, f. I mention it because while it technically is a function of the QBER, it is usually chosen at the beginning of an experiment through the choice of a particular LDPC code, and it has important consequences for the ROT length rate.

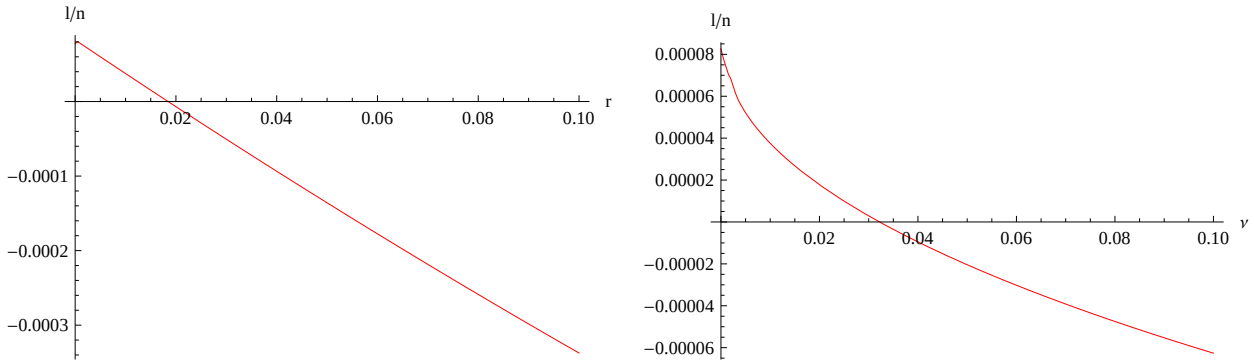

Figure 4.5: Plot of the ROT rate, l, versus the (left) depolarizing noise r, and (right) the quantum memory storage rate, ν.

Finally, looking at Figure 4.6 which plots the ROT rate versus the detection error (QBER), e_{det}, we see that in order to get a positive ROT rate, I need to observe a QBER of 0.956% or less over the course of the experiment. This represents an extremely experimentally challenging constraint, one that is much stronger than the typical safe QBER levels for QKD ($\sim$ 11%). Moreover, this fact alone prevents most of the existing QKD systems in the world today from being easily converted into a secure ROT implementation through a classical post-processing software update alone. This is a significant point of importance for this work since the original theory papers do not mention this stringent QBER requirement allowing one to naively believe that ROT could be simply implemented with some new software on any existing QKD system. Hopefully, future theoretically work on the security of ROT in the noisy storage model can alleviate this road block but for now it requires a much better source (high pair rates and low QBER) than is typically found in QKD implementations.

A few last notes to include are that the entire preceding discussion on the security of ROT was predicated on the assumption that I am dealing with optical qubits, ie. two level systems. In reality though, I have optical modes. Thus, I still need to make use of the squashing model [15, 154, 79], which was developed for QKD, in order to allow me to safely assume that I am creating and measuring qubits. Also, my security discussion has neglected vulnerabilities from a number of well known attacks in QKD [62, 96, 103, 125, 101].

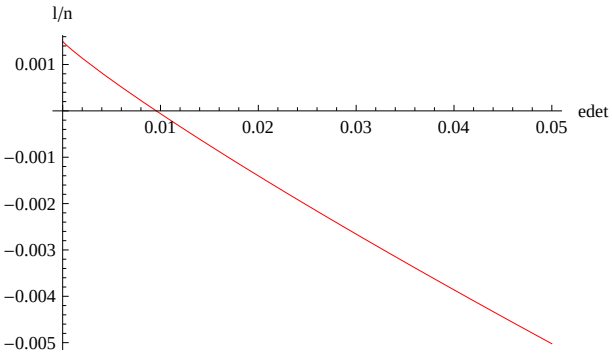

Figure 4.6: Plot of the ROT rate, l, versus the QBER, e_{det}.

4.5 Experimental Results

The ROT experiment that I now detail was performed on December 22, 2011 from 5:21pm to 9:42pm. Before starting the experiment, I fine-tuned the alignment of the source running at 7 mW of power to minimize its error rate and measured or selected all of the pertinent parameters shown in Table 4.2 in order to evaluate the length of the ROT strings, given by Eq. 4.9, which Alice and Bob could subsequently extract from their data. Over the course of the 4 hr 21 min experiment, Alice and Bob measured 405,642,088 ($= 4.06 \times 10^8$) coincident detection events which means that a total of 2.704×10^{10} pairs were sent. The timing information t and $\hat{t}$ was exchanged in real-time so that they could sort their measurements down to coincident events which were then saved. These measurements formed their raw keys (x and $\hat{x}$ respectively) combined with their record of measurement basis for each detection (θ and $\hat{\theta}$ respectively) and resulted in raw files 396 MB in size.

After collecting the necessary amount of signals for the security proof, Alice and Bob then proceeded to implement the remaining steps in the ROT protocol. First, Alice verified that a potential dishonest Bob was sufficiently bounded by checking that the number of coincident detections lay in the secure interval given by $[(1 - p^h_{B,noclick} - \zeta^h_{B,noclick}) \cdot n, (1 - p^h_{B,noclick} + \zeta^h_{B,noclick}) \cdot n] = [3.96757^8, 3.97642 \times 10^8]$[10]. Next, after waiting for a minimum time $\Delta t = 1$ sec for any stored quantum information of a dishonest party to

[10]The number of coincident detections (4.06×10^8) was actually higher than the upper bound to this interval, meaning that $p^h_{B,noclick}$ (the probability that an honest Bob got no click) was actually lower than

decohere[11], Alice then sent her basis measurement information (θ) for each detection event to Bob. Bob with his choice bit set to $C = 0$ then partitioned his data into $\hat{x}|\mathcal{I}_0$ (totalling 194,940,275 bits) where his measurement basis matched Alice's (ie. $\theta = \hat{\theta}$), and $\hat{x}|\mathcal{I}_1$ (totalling 210,701,813 bits) where his measurement basis did not match Alice's (ie. $\theta \neq \hat{\theta}$). He then sent his partitioning, $\mathcal{I}_0$ and $\mathcal{I}_1$, to Alice.

It is important to realize that it is Bob's choice of labelling the two sets according to $\mathcal{I}_C = \{k \in [m] | \theta_i = \hat{\theta}_i\}$ and $\mathcal{I}_{1-C} = \{k \in [m] | \theta_i \neq \hat{\theta}_i\}$ which allowed him to choose to receive S_C from Alice since it is the $\hat{x}|\mathcal{I}_C$ subset which he is able to error correct and subsequently recover S_C from. However, this does not reveal C to Alice since from her point of view she always receives an $\mathcal{I}_0$ and $\mathcal{I}_1$ from Bob and there is never any information in the partitioning which would allow her to deduce C.

Once Alice received the subset information from Bob, she proceeded to partition her data similarly into the two sets $x|\mathcal{I}_0$ and $x|\mathcal{I}_1$. She then chose two 2-universal hash functions, $f_0, f_1 \in_R \mathcal{F}$, and sent her choices to Bob. The next step was for Alice and Bob to perform one-way error correction on the two subsets. Alice began by encoding syndrome information on her first subset, $syn(x|\mathcal{I}_0)$, which she then sent to Bob. The term one-way error correction is slightly misleading since Alice and Bob do in fact minimally communicate during the error correction process. The reason for this is that there is a certain probability (p_{fail}) that Bob's decoding algorithm will fail to error correct a particular block of key from Alice. When this happens he needs to let Alice know that his decoding failed. In a QKD system they would have had three options: they could reveal that block of

anticipated. This was due to coarse estimation techniques used to estimate quantities, such as η, which experimentally include effects such as dark counts but which are separated in the probabilities utilized in the security proof. Additionally, the security proof relies on a model of the source which likely differs substantially from the actual experimental statistics. Luckily, Ref [159] mentions that only conservative *lower* bounds are necessary for the proof of security. And that if there are, for example, laser intensity fluctuations provided one knows a worst case estimate of the necessary parameters then the security for an experiment with finite size effects will still go through so long as a one-sided lower bound is used. Thus, since the number of detections was strictly larger than the lower bound in this formula, security can still be ensured for this experiment.

[11]This is more than long enough based on current storage times of quantum memories in the range of milliseconds. Additionally, the experiment lasted for 4.35 hrs so that Δt was actually much longer for most of the key.

key (for proper QBER estimation) and then discard it; Alice could try a different parity check matrix to calculate more parity bits, send them to Bob, have him run his decoding algorithm again and hopefully it works; or they could revert to a two-way error correction algorithm, such as Cascade, which is guaranteed to correct the errors (assuming the error rate was sufficiently small). The third possibility is not an option for Alice and Bob in this case since, as mentioned before, it would reveal Bob's choice bit, C, ruining the security of ROT.

Since error-correction was not the focus of this experiment, I chose for Alice and Bob to reveal those blocks of key where Bob's decoding algorithm failed and then discard them. It is extremely important that all failed blocks get publically revealed so that the QBER is properly measured. If these blocks were merely discarded then the QBER measured on only the successful blocks would underestimate the actual QBER that was experienced by quite a lot since the failed blocks represent sections of data where the error rate was proportionally higher. However, in future experiments concerned with the overall ROT rate, one could employ the second option and attempt error correction a second time with a different parity check matrix. Additionally, future implementations could try and optimize the efficiency of their error correction code. During error correction on the $\mathcal{I}_0$ subset, Bob observed an average quantum bit error rate of 0.93%. He relayed the observed QBER to Alice once the error correction step for the $\mathcal{I}_1$ subset was also performed so that they could both use Eq. 4.9 to determine how much key to keep after hashing their subsets.

Having finished with the $\mathcal{I}_0$ subset, Alice then proceeded to encode syndrome information on her second subset, $syn(x|\mathcal{I}_1)$, and sent it to Bob. It is important to note that Bob had to employ an additional step here, not mentioned in the protocols of Refs. [136, 159], in order to maintain security. Knowing the rough performance of the one-way error correction code that they were using, Bob randomly reported back to Alice according to the expected probability for the code (p_{fail}) whether his decoding succeeded or failed for each block of subset $\mathcal{I}_1$. He did this even though he was *not* in fact running any decoding algorithm on this subset because he needed the protocol to look identical from Alice's point of view, regardless of whether they were error correcting subset $\mathcal{I}_0$ or $\mathcal{I}_1$, in order for security to hold.

With error correction finished, Bob then reported back to Alice his observed QBER of

0.93%. In order to maintain security, he reported it to Alice without mentioning which subset it was measured in. Using this QBER in Eq. 4.9, Alice and Bob calculated the size of their secure final ROT key to be 8,939,150 bits. Using the f_0 and f_1 chosen earlier, Alice then output $S_0 = f_0(x|\mathcal{I}_0)$ and $S_1 = f_1(x|\mathcal{I}_1)$ retaining the last 8,939,150 bits from the 2-universal hash operation, as required. Having chosen $C = 0$, Bob then used f_0 to output $S_C = f_C(x_{cor})$ to obtain the bit string he desired from Alice. If Alice and Bob wanted to remove the randomness from the protocol to implement oblivious transfer with specific strings desired by Alice, she could then use S_0 and S_1 as one-time pads to encrypt her desired strings and send the results to Bob. Using his S_C he could then have decrypted Alice's last communication, recovering his desired string of Alice.

4.5.1 Security Caveat

There is one small caveat to the preceding security argument that I only recently discovered. Originally in my implementation of ROT I had to redefine my μ for the source by absorbing all of Alice's losses into it because I had not yet achieved a low enough QBER to obtain a positive ROT rate. I then claimed security, much like decoy state QKD systems, by using this redefined μ in my security analysis with the additional assumption that Bob could not influence the source and was stuck with the signals he received at the fibre he connected to. In doing so, the ROT rate I obtained was more than large enough to deal with any inefficiencies due to my error correction algorithm.

However, after much optimization work with the source, I finally managed to get a QBER of 0.93% which was just under the minimum necessary ($< 0.956\%$) to prove unconditional security. While this was a very positive step forward, removing an additional unwanted assumption from my security analysis, an unanticipated result of this was that the efficiency of my error correction algorithm, f, and its probability of failure, p_{fail}, were too high to obtain a positive ROT rate. For this experiment, Alice and Bob used an LDPC code with a block size of 92 bits revealing 32 bits of information about the key per block through the parity computation. Over the course of Bob error correcting his subset $\hat{x}|\mathcal{I}_0$ using the syndrome information sent from Alice, his decoding algorithm succeeded 2,053,535 times and failed 57,395 times thus yielding his error corrected key, x_{cor}, shortened from

194,940,275 bits to 188,925,220 bits while revealing a total of 67,549,760 bits. Thus, for this experiment the error correction algorithm operated at an efficiency of $f = 4.57$ times the Shannon limit with a probability of failure of $p_{fail} = 0.0272$.

Additionally, it was only in double checking my security arguments while proofreading this thesis that I realized the effect of the error correction efficiency on the ROT rate[12]. Since realizing this, I have gone back to the ROT rate formula to analyze the minimum error correction efficiency necessary to obtain a positive ROT rate and found it to be $f = 1.53$. This is reassuring since Pearson has reported on obtaining an error correction efficiency of $f = 1.26$ using one-way error correction with LDPC codes [117]. I am currently searching for a better code and/or decoding algorithm able to perform efficiently enough to generate an ROT key using the data collected for this chapter with unconditional security. For the purposes of my analysis in the preceding security discussion, I pessimistically assumed an achievable error correction efficiency of $f = 1.5$.

4.6 Discussion

The experiment above represents the first experimental implementation of robust oblivious transfer in the noisy storage model. It is important to notice that ROT is a fundamentally different cryptographic primitive than QKD and represents an important new tool at our disposal. Using the example mentioned in the introduction of this chapter of securing one's banking information at an ATM, it has long been suggested to use a small handheld QKD device to accomplish this [41]. However, if one were to employ ROT to build a secure identification scheme, as opposed to QKD, one's bank card number and PIN would never *physically* be exchanged over any communication line. Rather, the ATM and the user would merely be evaluating the joint equality function, $f(x) = f(y)$, on each of their copies of the login information. Thus, we can see one example of how ROT differs from QKD and ROT's potential in certain situations.

[12]Schaffner's original paper, Ref. [136], merely has a constant of 1.2 in its ROT rate formula which I only just realized represented an (optimistic) error correction efficiency which he must have gotten from somewhere.

However, before ROT is widely adopted, there are a number of shortcomings both in its proof of security and possible implementations that are currently hindering it. The situation is very similar to what was the case for QKD shortly after Mayers [105] developed his first security proof in 1996. Very few people understood the security proof, and furthermore the specifications demanded of a QKD system using this proof were so stringent as to be practically impossible for the technology of the day. However, with much work over the last fifteen years, security proofs for QKD have become much more robust, capable of tolerating much higher QBERs, of removing the need for quantum computers, and incorporating many shortcomings in actual implementations. Thus, as I discuss the current shortcomings of the theory of ROT in the noisy storage model in the following, my point is not to prove the uselessness of ROT but rather to highlight areas where more theoretical work would be very beneficial to relaxing some of the security constraints so that ROT can hopefully become as widely applicable as QKD.

The two most important issues to work on are: a relaxation of the dependence of the ROT rate on the loss of the system, and the development of security proofs to cover a wider range of quantum communication channels. As I pointed out for my system in Sec. 4.4.2, the ROT length is constrained drastically by the loss, η. Further, in order for ROT to be useful over longer distances, for instance over a future quantum communication network covering a city, the impact of loss on the security of the system has to be drastically reduced since the losses in such a network would be much higher than are currently tolerable. Since the security proofs for ROT were primarily analyzed for the case of a decoy state QKD system, there may well be improvements possible for analyzing the case using an entangled source more carefully. Analysis of QKD systems utilizing entangled sources have indeed found that they can tolerate more loss than decoy state systems, perhaps the same could be true for ROT.

Secondly, security for ROT has currently only been proven for channels that follow the strong converse property. As it happens, a lot of important channels exhibit this property, for instance, the depolarizing channel which is the channel assumed for this work. However, in order to have widespread adoption of ROT it is important to extend security to cover more, if not all, channels. A second option might be to derive an operation one might be able to perform at one or both ends of the channel in order to make it look like a channel

which follows the strong converse property. A similar idea, called "twirling", has been used in the bench-marking of quantum information processors in order to evaluate their performance versus an average noise [46]. Alternatively, in some of the quantum memory implementations the quantum states retrieved have a very high fidelity with the original quantum state, however this is always post-selected data. In other words, a second major problem for quantum memories is that they experience a lot of loss such that they act as erasure channels. Thus, an erasure channel would also be an interesting channel to study the security for.

Besides these bigger issues, there are a number of smaller issues in the security proof that would also greatly help to make ROT more practical. I worked very hard to get the error rate down in my QKD system as it severely limits the possibilities for ROT generation; indeed, it required the construction of a second generation entangled photon source (see Sec. 3.2). It would be very beneficial to relax the constraints on the tolerable QBER, especially as the distance between users increases and things like loss and dark counts cause the QBER to rise. Similarly, in order to maintain security Alice and Bob had to wait for over 10^{10} signals to be sent which in the experiment above took over 4 hrs. Obviously users wishing to authenticate themselves to an ATM do not want to have to stand there for hours in order to do so. While this might be one reason for employing decoy state prepare-and-send systems which have steadily been progressing to source rates in the GHz range [40], detectors are still not capable of GHz detection rates. Further, even if detectors capable of detection rates this high were built, the classical post-processing algorithms required to perform the rest of the protocol would become the next bottleneck. Indeed, it took 30.5 hrs for my state-of-the-art desktop computers to finish the process of one-way error correction. Thus, it would be very advantageous to lower the number of exchanged signals necessary in order to prove security.

The security proof for ROT also differs greatly from those for QKD in that it uses a number of different probabilities in its security and rate equations; whereas, the beauty of key rate formulas for QKD is that they now include only measurable quantities from experiment. Many of the probabilities for ROT are things that are not normally measured in an experiment and more importantly are quantities that are tricky to define and measure in a system with a continuous laser rather than a pulsed one. In order to prove security,

I relied on estimating a laser pump amplitude or mean photon pair number per pulse, μ, and then used it in the assumed PDC source model (given by Eqs. 4.1, 4.2, and 4.3) to generate all of the necessary probabilities. Instead, one would either like to derive formulas for all probabilities in terms of measurable quantities (such as count rates, coincidences, and QBERs) or even better convert all quantities in the key rate formula into those which are directly measured in an experiment.

Further to the point of acquiring accurate estimates of the quantities necessary for security, it is highly probable that the statistics of the assumed PDC source model differ greatly from the actual experimental distributions. This fact alone greatly undermines the confidence one has in the statements of security for ROT. Again, it would be much more secure if it relied solely on experimentally verifiable measurements for security. There are number of different techniques by Mogilevtsev [110], Rossi *et al.* [128], and Zambra *et al.* [168, 169], to name a few, which could be used to accurately measure the photon statistics output by the entangled source. A more robust proof of security could then use these measurements as inputs in order to ensure protection. Additionally, Wehner *et al.* [159] themselves point out that they simplified their security proof for ROT in the case of an entangled source, giving all information in a double pair (and higher) emission to Bob. However, not only is the double pair emission rate likely over-estimated in the assumed PDC model, but as has been pointed out in connection with QKD it is far from clear that double pair emissions give much, if anything, to an adversary. Indeed, since the probability of double pair emission is one of the key quantities limiting the acceptable QBER's, losses, and rates in ROT, there is likely much to be gained from a more detailed security analysis of an entangled system.

4.7 Conclusion

In conclusion of this chapter, I have reported on the first experimental implementation of random oblivious transfer secure under the noisy storage model. I began by describing the framework of the noisy storage model and introduced the simple ROT protocol due to Schaffner [136]. From there I moved on to describing my experimental implementation of

ROT with an entangled photon source since it had important consequences when it came to adapting the ROT protocol to my setup. Most importantly, my source of entangled photons utilized a continuous wave laser so that there were not well defined time-slots during which Alice and Bob expected a photon to be sent. Additionally, it also hindered the definition of many of the important probabilities necessary for the proof of security.

Following this, I then laid out all of the theoretical and experimental parameters needed for the proof of security. Using these I then worked through a number of security arguments in order to show that my implementation was secure. Included in this was an analysis of ROT rates depending upon a number of different parameters, the most important of which being the loss and QBER. With a proof of security complete, I then turned to examining my experimental results. Over the course of a 4 hr 21 min experimental run, Alice and Bob exchanged 2.704×10^{10} signals (before losses) which were then processed into subsets $\mathcal{I}_0$ and $\mathcal{I}_1$ containing 194,940,275 bits and 210,701,813 bits respectively. For the case of the $\mathcal{I}_0$ subset, where Bob's measurement basis matched Alice's, they observed a total QBER of 0.93%. After the necessary one-way error correction algorithms were performed (which took 30.5 hrs), Alice and Bob then used their ROT rate formula to extract 8,939,150 bits of ROT key from their exchange using 2-universal hash functions. To close I discussed the results of the experiment and highlighted many of the current short-comings in the security proofs in order to highlight important areas for future work.

Chapter 5

The Design and Implementation of Free-Space Receivers and Active Polarization Analyzers for a Space-Like Separated Svetlichny Inequality Violation

The last subject of my thesis moves away from work in quantum cryptography and instead delves into some foundational aspects of quantum mechanics. The rationale behind the project was to marry my experience and capabilities for quantum communication over free-space links with a fundamental test of quantum mechanics known as Svetlichny's Inequality. A first experiment of Svelitchny's inequality had recently been performed at the Institute for Quantum Computing in Waterloo by Lavoie *et al.* [88] in 2009; however, one of the short-comings was that it was performed locally in the lab without locality and freedom-of-choice conditions enforced. With my free-space infrastructure and expertise it made sense to extend this work to a spacelike separated experiment much like the first spacelike separate Bell inequality experiment. Additionally, having the capacity to distribute a three-photon state to separated sites opens up possibilities for a wealth of

future experiments.

This chapter describes the design and setup of new second generation free-space receivers including new active polarization analyzers capable of switching at rates over 1 MHz which are required to enforce the necessary spacetime separation between measurement sites. I begin by describing some background material (Sec. 5.1) including a proper definition for Svetlichny's inequality (Sec. 5.1.1), a brief discussion of the first experiment by Lavoie *et al.* (Sec. 5.1.2), and the theory behind the operation of a Pockels cell. I then move to the design and operation of the new free-space receivers and polarization analyzer (Sec. 5.2), followed by a description of the setup and alignment procedures necessary to obtain sufficiently high measurement contrasts in both bases. With the polarization analyzer aligned I then discuss its performance (Sec. 5.4) when measuring entangled photon pairs from an entangled Sagnac source (see Sec. 3.2). Finally I close the chapter with some conclusions about the new receiver and analyzer and comments on the future experiment (Sec. 5.5).

The whole experiment is being performed in collaboration with a large team from the Institute for Quantum Computing in Waterloo made up of students Catherine Holloway, Evan Meyer-Scott, J.P. Bourgoin, Jonathan Lavoie, Laura Richards, and Nick Gigov; postdocs Brendon Higgins, Krister Shalm, Robert Prevedel, and Zhizhong Yan; and professors Thomas Jennewein, Kevin Resch, and Gregor Weihs. During the initial setup and tests of the Pockels cell I worked closely with Robert Prevedel who is now a postdoc at the Research Institute for Molecular Pathology and Max F. Perutz Laboratories in Vienna, Austria. I also benefitted greatly from the knowledge and expertise of Prof. Kevin Resch and Prof. Thomas Jennewein. The quantum random number generator (QRNG) designed to trigger the Pockels cell's switching between measurement bases was developed by Laura Richards, Zhizhong Yan, and Prof. Thomas Jennewein and custom built electronic logic responsible for translating the signals from the QRNG into the necessary outputs required to drive the Pockels cell was developed by Zhizhong Yan and Prof. Thomas Jennewein. Beyond this, I was the sole investigator responsible for the incorporation of the Pockels cell into the new free-space receiver and polarization analyzer. I performed the setup and alignment of the Pockels cell in the new receiver and evaluated its performance by measuring entangled photon pairs with my local QKD system (see Chs. 2 and 3).

5.1 Background

Before detailing the setup and alignment of the new polarization analyzers I first take a moment to describe the details of Svetlichny's inequality. I also mention the previous local experiment performed by Lavoie *et al.* and some of their results. Finally I describe the physics behind the operation of the Pockels cell without which performing a spacelike separated version of the experiment would likely be impossible.

5.1.1 Svetlichny's Inequality

Svetlichny's inequality [151], developed in 1987, can be viewed as a generalization of Bell's equality (which is described in Sec. 1.1.3). It is an inequality that in a three-body system can detect three-body correlations that cannot be reduced to mixtures of two-body ones which are related locally to the third body. In other words, Svetlichny showed that even if one allows for unrestricted nonlocal correlations between any two particles in a three particle system, an inequality can still be found which is violated by the predictions of quantum mechanics. Thus, quantum mechanics is shown to be incompatible with a restricted class of nonlocal yet realistic theories for three particles where any two-body nonlocal correlations are allowed. Svetlichny's inequality is particularly important because while there has been an overwhelming number of Bell experiments involving two-body correlations performed, experiments on many-body systems have been few and far between. Experiments of this type are particularly valuable to explore since we live in a many-body world. Further, it is important to devise direct tests of quantum mechanics in many-body situations that are immune to any possible explanation in terms of one and two-body physics for which quantum mechanics has been well tested so far [151].

Quantum mechanics allows for an arbitrary number of qubits to be maximally entangled. Svetlichny derived his inequality for the case where only arbitrary two-body correlations are allowed and then asked the question of what restrictions this places on three-body observations. The following derivation of Svetlichny's inequality is taken from Ref. [88]. Earlier in Eq. 1.6 in Sec. 1.1.3 I wrote a particular trial for Bell's inequality as

$$S_2 = (ab) + (ab') + (a'b) - (a'b') \tag{5.1}$$

where I now use the subscript 2 to denote the fact that the inequality is for 2 particles. But the two particles also satisfy the relation

$$S_2' = (a'b') + (a'b) + (ab') - (ab) \tag{5.2}$$

equally well. Here I have taken special care not to factorize Eqs. 5.1 and 5.2 as I did earlier in Sec. 1.1.3 since we are now exploring the situation investigated by Svetlichny and allowing for arbitrary non-local correlations among the two particles. The brackets serve to emphasize this fact and remind us that we have allowed for measurement outcomes for particle a to non-locally depend on outcomes and/or measurement settings for particle b and that these quantities must now be regarded as separate and independent quantities.

If we now add a third particle, c, and assume that local realism holds with respect to this third particle, I can now write the following inequality

$$S_2c - S_2'c' = (ab)c + (ab)c' + (ab')c - (ab')c' + (a'b)c - (a'b)c' - (a'b')c - (a'b')c' = \pm 4, 0 \tag{5.3}$$

where it is understood that any of the values in brackets as well as c and c' must take on the predetermined values ± 1.

If we now average over many trials, as we did for Bell's inequality, we obtain Svetlichny's inequality

$$\begin{aligned} S_v &= |E(\mathbf{a},\mathbf{b},\mathbf{c}) + E(\mathbf{a},\mathbf{b},\mathbf{c}') + E(\mathbf{a},\mathbf{b}',\mathbf{c}) - E(\mathbf{a},\mathbf{b}',\mathbf{c}') \\ &\quad + E(\mathbf{a}',\mathbf{b},\mathbf{c}) - E(\mathbf{a}',\mathbf{b},\mathbf{c}') - E(\mathbf{a}',\mathbf{b}',\mathbf{c}) - E(\mathbf{a}',\mathbf{b}',\mathbf{c}')| \end{aligned} \tag{5.4}$$

where S_v now stands for the Svetlichny parameter. Note that although I started by allowing for nonlocal correlations amongst particles a and b while enforcing locality for c, I would get an identical expression had I allowed for b and c to have nonlocal correlations while keeping a local and similarly for the third case. Every hidden variable model that might allow for nonlocal correlations amongst any two particles but not between all three thus satisfies the Svetlichny inequality of Eq. 5.4.

Svetlichny then proceeded to show that his inequality could be violated by quantum mechanics, with a maximal violation achieved with the use of GHZ states. Using the GHZ state given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle) \tag{5.5}$$

and letting the measurement settings be those in the xy-plane of the Bloch sphere given by projecting onto the states $\frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi}|V\rangle)$ then the quantum prediction of Eq. 5.4 becomes

$$\begin{aligned} &|\cos(\phi_a + \phi_b - \phi_c) + \cos(\phi_a + \phi_b - \phi'_c) + \cos(\phi_a + \phi'_b - \phi_c) \\ &- \cos(\phi_a + \phi'_b - \phi'_c) + \cos(\phi'_a + \phi_b - \phi_c) - \cos(\phi'_a + \phi_b - \phi'_c) \\ &- \cos(\phi'_a + \phi'_b - \phi_c) - \cos(\phi'_a + \phi'_b - \phi'_c)|. \end{aligned} \tag{5.6}$$

Choosing the following angles

$$\phi_a = \frac{3\pi}{4}, \phi'_a = \frac{\pi}{4}, \phi_b = \frac{\pi}{2}, \phi'_b = 0, \phi_c = 0, \phi'_c = \frac{\pi}{2} \tag{5.7}$$

yields the maximal violation of $S_v = 4\sqrt{2} \not\leq 4$ achievable with quantum mechanics [109]. Since any possible hidden variable model describing a three-particle state where only two particles are nonlocally correlated must satisfy Svetlichny's inequality, its violation definitively rules out any local hidden variable theories of this type.

5.1.2 Previous Work

Recently, Lavoie *et al.* [88] performed the first experiment testing quantum mechanic's violation of Svetlichny's inequality. For the experiment they used the double-pair emission of a type-I noncollinear SPDC source (similar to the Kwiat source [87] developed in 1999 and mentioned in Sec. 3.2.1) following the approach of Bouwmeester *et al.* [27] to produce three-photon GHZ correlations of the form given in Eq. 5.5. Using the predictions of quantum mechanics with measurements of the form given by $\frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi}|V\rangle)$ and the angles chosen as in Eq. 5.7 they were able to measure a Svetlichny parameter of $S_v = 4.51 \pm 0.14$, violating the inequality by 3.6 standard deviations. While the maximal violation possible via quantum mechanics is $4\sqrt{2} \simeq 5.66$. Their result was in very good agreement with the state of their source, which they reconstructed with quantum state tomography, since they only measured a fidelity of their reconstructed state with the desired GHZ state of $F = \langle\psi|\rho|\psi\rangle = 0.84 \pm 0.01$.

While it was a beautiful first experiment testing Svetlichny's inequality, it had two major loopholes which weakened their result. As with a Bell inequality, it is paramount

that the measurements be made in a spacelike separated manner so that there is no possibility of signalling between the two measurement sites. Such signalling would allow Alice and Bob to collude and produce an apparent violation of Bell's inequality or Svetlichny's inequality when there really was none. While few actually believe that the measurement devices would or can conspire in such a fashion, strictly speaking spacelike separation of the measurements must be enforced in order to rule it out. Additionally, a lesser known yet equally important third assumption of Bell's inequality, called freedom-of-choice, must also be enforced. Freedom-of-choice boils down to the fact that not only must the measurements be spacelike separated from each other, but the measurements must also be spacelike separated from the source so that their settings are random and cannot be causally influenced by particle emissions and any hidden variables therein.

Without these two assumptions enforced[1], locality and freedom-of-choice, any experimental result is necessarily less convincing. The goal of this work is to build on the expertise developed in the experiment of Lavoie *et al.* for producing three-photon GHZ states and measuring the necessary quantities for Svetlichny's inequality by adding my expertise with the free-space distribution of entangled photonic quantum states in order to enforce precisely these two requirements. While daunting, improvements in the source and initial calculations with the expected loss of the free-space links have shown that we should expect rates which will make such an experiment feasible. The rest of this chapter is devoted to detailing the receiver and measurement hardware necessary to perform the experiment.

5.1.3 Pockels Cells

For the measurement hardware, it is critical to find an electro-optical modulator capable of switching between the two different measurement basis settings ($\mathbf{a}$ and $\mathbf{a}'$ for Alice, and $\mathbf{b}$

[1]There is a third assumption, namely the fair sampling assumption, which assumes that the photon triplets which are measured (remember there is a great deal of loss both during the distribution and the detection of the photon triplets) are representative of the entire sample of triplets produced and are not somehow selected in such a way as to give a Svetlichny inequality violation when really there was none if the entire sample of triplets had been measured.

and $\mathbf{b}'$ for Bob) depending on the state of a QRNG and to do so quickly enough such that the locality and freedom-of-choice conditions can be enforced. Fortunately, Pockels cells (PC) are just such devices capable of changing the refractive index of their optical crystal quickly in response to an applied voltage. This linear electro-optical effect was discovered by Friedrich Pockels [122] in 1906 and is so named after him. The following description of a Pockels cell is due to Refs. [24, 131, 138, 124].

In a birefringent crystal which exhibits the Pockels effect, the two orthogonally polarized modes of an incident beam will experience a relative phase shift given by

$$\phi = \phi_0(d, n_f, n_s) + \pi \frac{V}{V_{\lambda/2}} \tag{5.8}$$

where $\phi_0(d, n_f, n_s)$ is the phase shift induced by the crystal with no applied voltage (which depends on the length of the crystal, d, and the native indices of refraction for the fast and slow axes in the crystal, n_f and n_s, respectively), V is the voltage applied across the crystal, and $V_{\lambda/2}$ is a property of the crystal known as the half-wave voltage (which depends on the crystal material, size, geometry, and the frequency of light considered). The half-wave voltage, $V_{\lambda/2}$, is the voltage at which the fast and slow polarization components exhibit a phase-shift of $\pi/2$ allowing the Pockels cell to act as a half waveplate.

The Pockels cell used in this experiment (Leysop RTP4-20-AR800) was made by Leysop Ltd. and consists of two $4 \times 4 \times 20$ mm Rubidium Titanyl Phosphate ($RbTiOPO_4$ or RTP) crystals placed in sequence[2]. These crystals offer a high electro-optical coefficient allowing for half-wave switching within nanoseconds. With spacetime considerations on the order of μs necessary to enforce the locality and freedom-of-choice conditions, this PC is more than sufficient for our needs. The crystals are cut such that the optical path of the entangled photons through them is not along an optical axes but rather along the crystallographic y-axis, a direction that exhibits birefringence even in the absence of an applied voltage. However, the design of the PC uses a pair of RTP crystals oriented with their z-axes rotated 90° to one another thus allowing for the birefringence to be compensated. This sets $\phi_0(d, n_f, n_s) = 0$ in Eq. 5.8 and makes sure that the photons do not experience any spatial walk-off. The voltage is applied perpendicular to the direction of propagation of

[2]For more information please refer to Ref. [4]

the input photons meant to be rotated, along the z-direction (known as a transverse PC), with the opposite sign for each of the two crystals[3]. In this configuration, the PC will rotate the polarization of an incoming photon depending on the voltage applied and the orientation of the z-axis of the PC (ie. the rotation of the PC around the optical path). Suitably aligned, the PC will perform an identity on the incident photon when no voltage is applied and act as a HWP when $V_{\lambda/2}$ is applied.

5.2 Design

The setup for the new free-space receiver and polarization analyzer is shown in Fig. 5.1. The design incorporates features from Refs. [139, 138, 24]. A large 150 mm diameter receiver lens is responsible for collecting photons sent over the free-space link and a smaller lens of the appropriate focal length collimates the photons into a beam suitable for the polarization analyzer. An optional flip-mounted mirror can be inserted for local alignment of the polarization analyzer. With it in place, a local alignment laser and/or entangled single photons can be input into the polarization analyzer through the input coupler. A flip-mounted polarizer before and PBS after the PC (made up of the two RTP crystals mentioned earlier) act as two-crossed polarizers for alignment purposes (described next in Sec. 5.3).

The HWPs placed before and after the PC are used for the fine alignment of the rotation of the PC around the optical path. The HWPs are required since the RTP crystals sit in a mount which does not allow for any fine adjustment of their rotational angle with respect to the optical path. Precise rotational alignment of the PC's fast and slow axis is required in order to obtain a high switching contrast. The QWP allows the PC to be operated at its quarterwave voltage rather than its halfwave voltage, a trick first employed by Scheidl *et al.* [139, 138], which increases the maximum allowable switching rate of the PC. The switching rate of a PC is in general limited by the performance of its high voltage power

[3]The reason for opposite signs is that if the voltage was applied with the same sign the birefringence would always be compensated so that there would be no net effect on the polarization of the photon when an electric field was applied.

supply and the piezoelectric properties of the RTP crystal, but it can be increased by reducing the voltage that has to be applied. Additionally, it helps to reduce ion wandering affects (which occur when high voltages are applied for long periods of time) as well as overheating, both of which can damage the RTP crystals. The PBS behind the PC splits the incoming photons depending on their polarization according to the orthogonal basis selected by the PC. Finally, precision couplers (Metric Spatial Filter stock # NT55-475 from Edmund Optics) collect the analyzed photons into multimode optical fibres which are then connected to single photon detectors.

5.3 Setup and Alignment

The procedure for the setup and alignment of the new free-space receivers and active polarization analyzers incorporating the PC is adapted and augmented from Refs. [138, 24, 124]. For the initial tests with the PC I operated it with a Pockels cell driver, power supply, and splitter box driving electronics from Bergmann Messgeraete Entwicklung KG (BME) and a function generator. For some of the measurements of entangled photon pairs using my Sagnac source (detailed in Sec. 3.2) I also used the QRNG designed to trigger the PCs switching between measurement bases developed by Laura Richards, Zhizhong Yan, and Prof. Thomas Jennewein and custom built electronic logic responsible for translating the signals from the QRNG into the necessary outputs required to drive the PC developed by Zhizhong Yan and Prof. Thomas Jennewein.

5.3.1 Initial setup of the optical path

The large lens that collects the photons sent over the free-space link and final collimator after the polarization analyzer optics define the optical path of the new receiver in Fig. 5.1. I positioned those first along with two irises placed along the optical path for alignment purposes. The next step was for me to place the input coupler and flip-mounted mirror used to inject alignment lasers and/or local entangled photons into the polarization analyzer. These allowed me to locally align the polarization analyzer including the PC before dealing

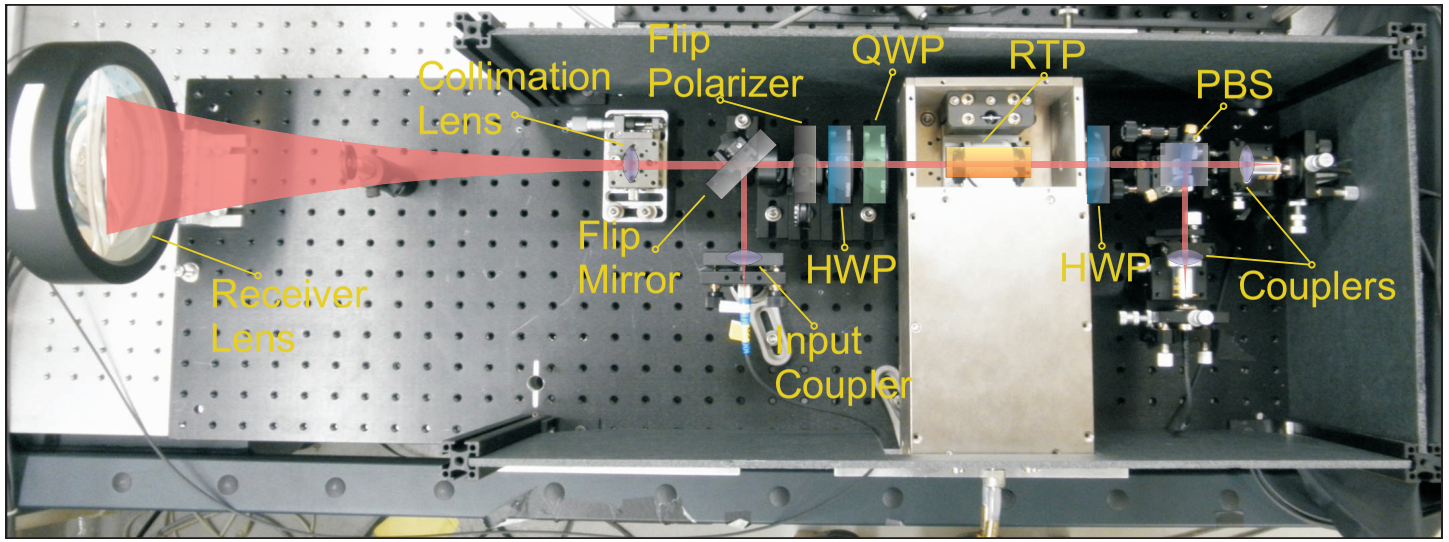

Figure 5.1: Experimental design of the free-space receiver and PC polarization analyzer. A large 150 mm diameter receivers lens collects photons sent over the free-space link and a smaller lens collimates the photons into a beam suitable for the polarization analyzer. An optional flip-mounted mirror can be used with a local alignment laser and/or entangled single photons to locally align the polarization analyzer. An optional flip-mounted polarizer before and PBS after the PC (made up of two RTP crystals) act as two-crossed polarizers for alignment purposes. The HWPs placed before and after the PC are used for fine rotational alignment of the PC around the optical path. The QWP allows the PC to be operated at its quarterwave voltage rather than its halfwave voltage, increasing the maximum allowable switching speed of the PC. Finally, the PBS splits the incoming photons into two different paths depending on their polarizations and couplers collect the analyzed photons into multimode optical fibres to be sent to single photon detectors.

with any complications arising from the free-space beam which will have an ugly mode. Using the irises, I made sure that the alignment laser followed the same optical path defined by the large lens and collimator.

With the optical path defined, I then placed the PC at the correct position on the receiver, aligned as closely as possible to the optical path, so that the alignment laser passed through the center of the PC's aperture and was back-aligned to the incoming alignment beam. Then I placed the rest of the optical components needed for the polarization analyzer including the HWP and PBS after the PC; and the QWP, HWP, and polarizer on a flip-mount before the PC. I made sure to back-align all of the components using the retro-reflected beam from their face so that the optical path was normally incident to their front surface. Also, I initially nulled the settings of each of these components so they did not have any effect on the beam.

5.3.2 Fine-tuning alignment of PC with the optical path

To obtain high contrasts and accurate operation, it is crucial that the crystallographic y-axis of the PC is aligned exactly parallel to the optical path of the receiver. To fine tune this alignment I looked at the isogyre pattern produced by divergent (or diffuse) light illuminating the PC placed between two crossed polarizers (the polarizer in front was set to V while the PBS transmitted H). Light travelling along the y-axis of the PC should exhibit no birefringence in the absence of an applied electric field and be fully reflected by the PBS with none being transmitted to the coupler. However, photons making a finite angle with the y-axis should experience a birefringence induced polarization rotation allowing some of them to be transmitted by the PBS. This change should be rotationally symmetric about the y-axis and lead to the characteristic interference pattern, shown in Fig. 5.2 (a), known as an isogyre pattern.

The PC was mounted in a four axis tip/tilt stage within the driver head, which allowed for the precise alignment of its crystallographic axis. In order to observe a high contrast with the PC it is necessary for the coupler and singlemode fibres to be looking at the center of this pattern. Since the coupler and PBS are aligned and centered on the optical path I fine-tuneed the alignment by centering the cross-hairs produced in the isogyre pattern on

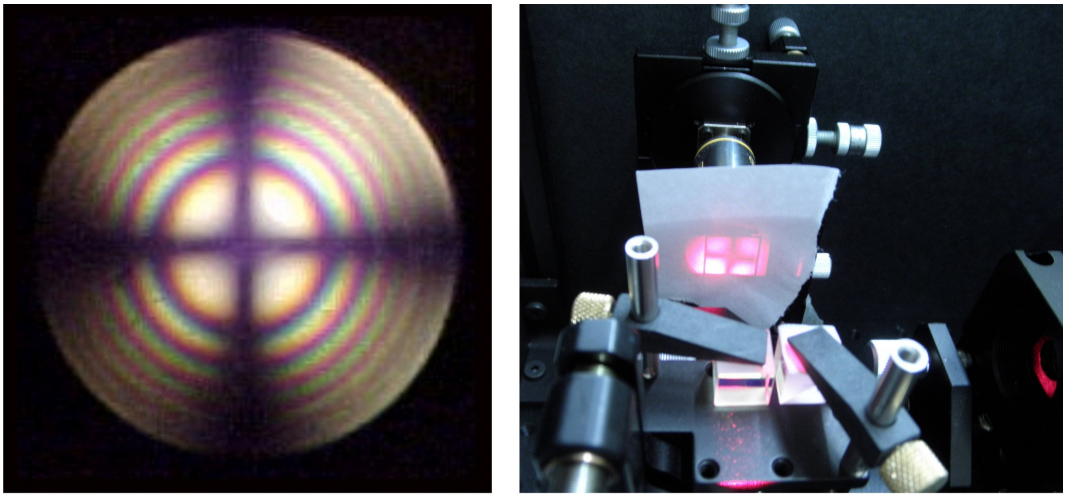

Figure 5.2: (a) A nice example of an isogyre pattern, figure taken from Refs. [138, 57], (b) the iosgyre pattern from the PC in my polarization analyzer obtained by placing the PC between crossed polarizers and a divergent lens in front of the PC.

the face of the PBS. The resulting isogyre pattern is shown Fig. 5.2 (b) where a divergent lens inserted in front of the PC was used in order to obtain a clear picture. When I actually aligned the PC it was preferable to use a piece of Scotch tape placed over the entrance to the PC since it diffused the light without causing a deviation of the beam. On the other hand, the isogyre pattern was very sensitive to the position and angular tilt of the divergent lens thus coupling the tasks of aligning the PC and the lens. The lens was used after the alignment merely to produce a stronger image that could be captured on camera.

5.3.3 Initial Measurement of the Halfwave Voltage

I implicitly aligned the PC above to be rotated 45° around the optical path (crystallographic y-axis) since the default operation of the PC at the halfwave voltage (HWV) is to flip the polarization of an incoming photon by 90°, taking H to V and vice versa. Since in my final setup I want the PC to rotate the photons by 22.5° into the diagonal basis, it was necessary to employ some additional elements to accomplish this. First, however, it was worthwhile

to ascertain an initial estimate for the HWV, $V_{\lambda/2}$, which in the initial configuration caused the PC to operate as a HWP at the angle 45° thus flipping the polarizations of the incoming photons.

I estimated the HWV by using the polarizer and PBS as parallel polarizers (always measuring photons in the transmitted arm of the PBS) setting the polarizer to transmit H photons from the alignment laser while the PBS projected onto H. I measured the output signal of the photons collected into the multimode fibre with a fast photodiode (DET10A from Thorlabs) on an oscilloscope (Agilent Infinium 54832D) as the PC was triggered with a function generator sending trigger pulses at 30 kHz to the splitter box which in turn sent the appropriate signals to the PC. I found the HWV by adjusting the high voltage power supply of the PC until the output signal was minimized during the time which the PC was on corresponding to the PC rotating the incoming photons by 90° to V. The resulting trace from the oscilloscope is shown in Fig. 5.3.

Using this method, I estimated the HWV of my PC to be 4.48 on the dial of the high voltage power supply. As the dial was supposed to represent the range of 0 to 2.2 kV, this implies that my estimated HWV was 0.986 kV. The reason this is only an estimate is that the power measured with the fast photodiode should follow a sin curve as the high voltage power supply is adjusted. The HWV corresponds to the maximum/minimum of the sin curve where there is the least sensitivity to changes in the voltage set with the high voltage power supply. Additionally, the signal from the laser, fast photodiode, and oscilloscope did not have a large contrast compared to the noise. This also contributed to a less accurate measurement of the HWV.

A second method for determining the HWV is to actually determine the quarterwave voltage (QWV) by replacing the PBS behind the PC with a second polarizer. Setting the first polarizer to pass H photons, adjusting the high voltage power supply, and rotating the second polarizer behind the PC will determine the quarterwave voltage of the PC when the midpoint of the trace during the time when the PC is on no longer changes. This is because at this point the PC is being fired at its QWV rotating H into the circular basis causing the photons to always be transmitted at the second polarizer with a probability of 50% regardless of the polarizer's linear setting. I found this method slightly more accurate for determining the QWV (and by extension the HWV which is merely the QWV multiplied

Figure 5.3: The figure shows the oscilloscope trace measured while finding the PC halfwave voltage (HWV). The PC was operated between a parallel polarizer and PBS set to transmit and project on H polarized photons. Photons were measured with a fast photodiode. The PC was triggered at a repetition rate of 30 kHz with a function generator and accompanying splitter box as the high voltage power supply was slowly adjusted. The HWV was found as the setting which minimized the trace during the time when the PC was on corresponding to the PC rotating the incoming photons by 90° to V. The yellow trace was the sync signal from the function generator while the green trace was the output of the fast photodiode.

by two) and this is how I determined the estimate for the HWV setting of 4.48 in the end. I will use these estimates for the HWV and QWV as the starting points for my optimization search in the following steps.

5.3.4 Reducing the Voltage of the Pockels Cell

Before moving on the operation of the PC with the QRNG, I first mention one last optimization made to the setup. As mentioned before, the Pockels cell can be operated at a higher switching rate with less heating and ion wandering effects, both of which can damage the RTP crystals, if the QWV is used as opposed to the HWV. In order to accomplish this, I used a trick due to Scheidl *et al.* [139, 138] and placed a QWP set to 45° in front of the PC. Now when a positive quarterwave voltage (+QWV) was applied the PC acted as an additional QWP at 45° such that the net effect was one of a HWP at 45°, rotating the polarization of light by 90°. Alternatively, when a negative quarterwave voltage (-QWV) was applied the PC acted as a QWP at $-45°$ compensating the rotation of the QWP so that the net overall rotation was 0°.

5.3.5 Verifying the Operation of the Pockels Cell at the QWV

With the addition of the QWP ahead of the PC, it was important to verify the operation of the PC while being switched with the QRNG at its QWV. When the PC logic applies a +QWV, this combined with the additional QWP in front of the PC should produce the result of flipping an input V polarized photon into an H polarized photon; whereas, when the logic applied the -QWV the PC should cancel the action of the additional QWP leaving the input V polarized photon alone. However, when testing this with correlated photon pairs produced with my Sagnac source (see Sec. 3.2) with the polarizer in front of the PC set to pass V photons while the PBS transmitted H photons, as I slowly increased the voltage to the QWV the contrast never improved beyond approximately 1:2 (for V:H) when the +QWV was applited. As it turns out, the reason for this was that operation at a switching rate of 1 MHz (programmed into the PC logic) corresponded to an unfortunate resonant frequency of the PC creating sinusoidal fringes which degraded the maximum

contrast. Fig. 5.4 (left) shows these fringes when a strong alignment laser was input to the PC.

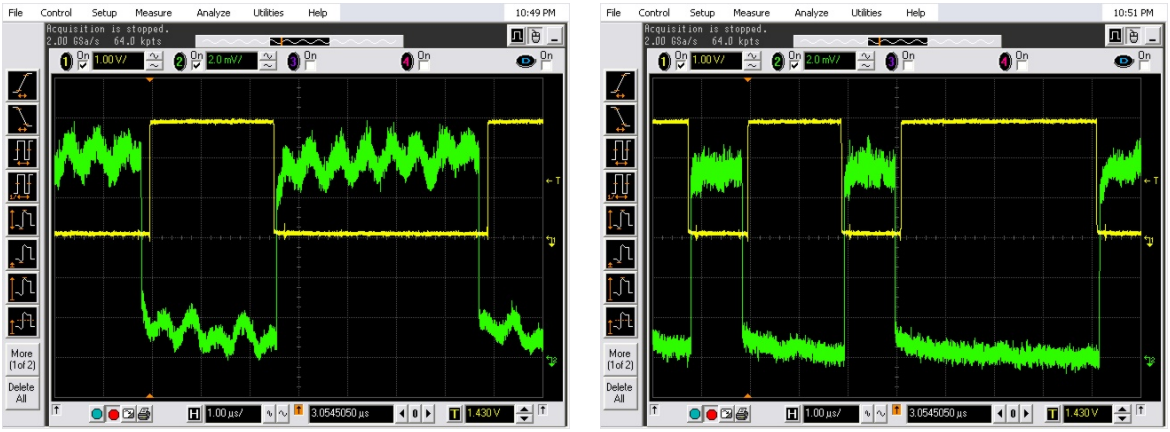

Figure 5.4: The figure shows (left) the oscilloscope trace of the unfortunate PC resonance when operating the PC at a frequency of 1 MHz and (right) the oscilloscope trace when the PC operation is moved to 0.956 MHz. The reason for the decrease in contrast of the PC between H and V from that expected is clearly visible in the sinusoidal interference fringes when the PC is operated near a resonance at 1 MHz (right); however, once its operation is moved away from the resonance the sinusoidal interference fringes are drastically reduced.

To correct for this, the logic which translates the output state of the QRNG into the signals necessary to drive the PC was augmented to allow for an external clock input. An internal frequency divider translates the external clock input into the output clock of the QRNG. For example, when a 30 MHz clock input was used, the resulting switching rate of the QRNG was 1.67 MHz. Using this additional functionality I scanned the clock frequency to move off of the PC resonance in order to recover a high switching contrast. Fig. 5.4 (right) shows the results of operating the PC with a QRNG switching frequency of 0.956 MHz where sinusoidal interference fringes are no longer seen.

5.3.6 Measuring the Duty Cycle of the Pockels Cell

With the resonance problem figured out, the next thing to measure was the duty cycle of the PC. The duty cycle is due to the non-zero rise and fall times of the PC when its state is changed. During the rise/fall time of the PC, any photons which traverse the PC will *not* have their polarizations rotated as expected. This will in turn degrade the maximum contrasts observed when analyzing the polarization of incoming photons. I measured the duty cycle by again injecting a local alignment laser into the polarization analyzer with the polarizer in front of the PC set to pass V photons while the PBS transmitted H photons and triggered the PC with its QWV (using the trick mentioned in Sec. 5.3.4) using the QRNG and logic at a switching rate of 0.956 MHz with a minimum pulse duration of 1 μs. The result was again detected with a fast photodiode.

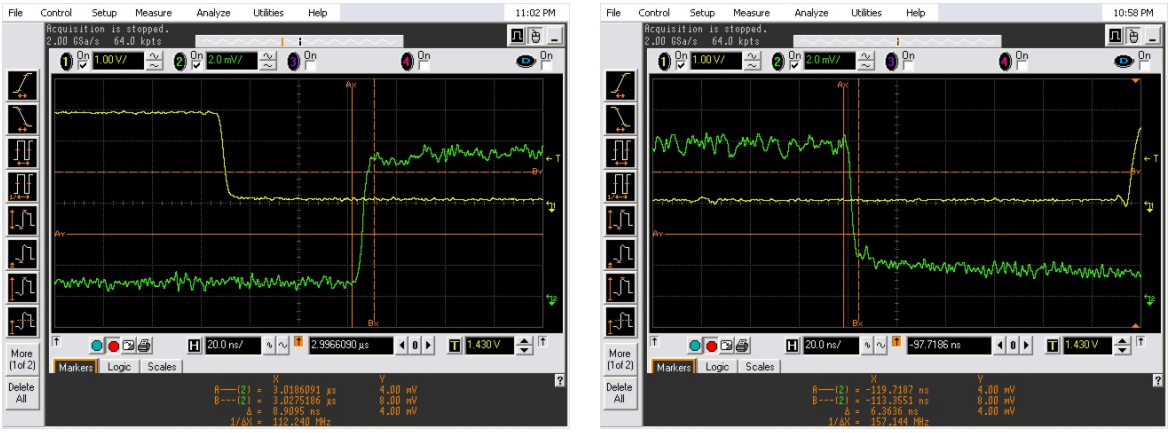

Figure 5.5: The figure shows the oscilloscope trace measuring the (left) rise time and (right) fall time of the PC as it was triggered at a rate of 0.956 MHz with a minimum pulse length of 1 μs. A rise time of 8.9 ns and a fall time of 6.4 ns were measured at the QWV leading to a duty cycle of 98.40%. The green trace is the signal from the fast photodiode, while the yellow trace is the state of the PC.

Fig. 5.5 shows the oscilloscope traces for these measurements as the PC was triggered. I measured an optical rise time for the switching process of approximately 8.9 ns using this procedure while measuring a fall time of approximately 6.4 ns, as shown in Fig. 5.5. These

results translate into a duty cycle for the PC of $(1 - \frac{8.9+6.4}{956}) = 98.40\%$ at the QWV[4].

5.3.7 Aligning the Pockels Cell for a 22.5° Rotation

With the PC characterization performed in the previous sections, the next task was to align the PC for use in the polarization analyzer. The PBS behind the PC naturally analyzes incoming photons in the H/V orthogonal basis, all that was required in order to analyze photons in the diagonal basis was to have the PC perform a rotation of 22.5°. However, as mentioned earlier in Sec. 5.3.3, the default operation of a PC is to perform a rotation of 45° and so it comes mounted with the RTP crystals inside the cell rotated 45° around the crystallographic y-axis and the electrodes facing up for easy attachment to the driver leads. In order to use the PC to perform a rotation of 22.5° it had to be physically rotated by this angle.

However, there is a more convenient method which does not waste the careful alignment of the isogyre pattern that I had already performed [24]. This is where the HWPs before and after the PC came in. As can been seen from the equation

$$HWP(-11.25°) \times QWP(45°) \times PC(45°) \times HWP(-11.25°) = HWP(22.5°) \qquad (5.9)$$

setting the HWPs before and after the PC to an angle of −11.25° makes the HWP-QWP-PC-HWP combination act as a HWP set to 22.5° when the QWV is used, up to an unimportant global phase. Additionally since the tip/tilt mount which the PC sat in had no fine adjustment of its rotation angle around the optical path, I made use of the HWPs to compensate any angular misalignment remaining in the setup of the PC. For instance, if the PC was aligned at $45° + 2\delta$, then with the HWPs set to $-11.25° + \delta$ and the QWV applied

$$HWP(-11.25° + \delta) \times HWP(45° + 2\delta) \times HWP(-11.25° + \delta) = HWP(22.5°)^5 \qquad (5.10)$$

[4]We expect to operate the PC at between 1 MHz - 2 MHz during the actual experiment, so this is an appropriate frequency to switch at for this test. Additionally, the rise and fall time of the PC did not appear to change appreciably as the switching frequency of the PC was increased towards 2 MHz. Thus, one can easily estimate the duty cycle of the PC at a switching rate of 2 MHz as $(1 - \frac{8.9+6.4}{500}) = 96.94\%$.

[5]In the equation, the action of the PC-QWP are combined for clarity, it should be understood though that $HWP(45° + 2\delta) = QWP(45°) \times PC(45° + 2\delta)$

and the angular misalignment is compensated. Alternatively, with the voltage supply off, then

$$HWP(-11.25^\circ + \delta) \times \mathbb{I} \times HWP(-11.25^\circ + \delta) = \mathbb{I} \tag{5.11}$$

and the HWPs contributed nothing.

5.4 Performance and Discussion

To fine-tune the operation of the PC, I used the coincident detection of correlated photon pairs from the Sagnac source described in Sec. 3.2. Rotating the pump laser in the Sagnac source so that it produced only HV correlated pairs, the H photons were coupled into the left fibre while the V photons were coupled into the right fibre. The H photons were directly detected with a single photon detector. The other singlemode fibre from the source was connected to the local input coupler for the PC polarization analyzer with the photons then passing through the polarizer, set to V, before proceeding to the HWP-QWP-PC-HWP combination and then on to the PBS, before finally being coupled and detected with single photon detectors. I then performed an iterative procedure to optimize both the HWP angles $-11.25^\circ + \delta$ and the QWP angle 22.5°, as well as the exact QWV used. During this optimization procedure I continued to trigger the PC using the QRNG set to the non-resonant frequency of 0.956 MHz determined above.

Solving for the optimum QWV, rotation of the QWP, and rotation of the HWPs required multiple iterations switching between searching for the optimal value for each which minimized the unexpected coincidences and maximized the contrast. I should mention that the optimum QWV found with this procedure was 1.73 on the dial (corresponding to a voltage of 0.381 kV produced with the high voltage power supply), as opposed to the 2.24 dial setting found during the initial QWV measurement. Eventually, with the optimal correction found, I measured a maximum contrast of 1:25.2 for the rectilinear basis and 1:22.6 for the diagonal basis. If the experiment were to be performed with this alignment, the PC polarization analyzer would have approximately a $\sim 4\%$ error rate. However, I should still be able to do better as Scheidl *et al.* [139, 138] were able to obtain contrasts of 1:160 and 1:170 in the rectilinear and diagonal bases respectively.

The decrease in contrasts is likely due to the duty cycle of the PC being less than 100%. Remember, during the rise and fall times of the PC the photons will not have their polarization rotated as expected thus decreasing the maximum obtainable contrast. Additionally, there is a delay between the switching signal output from the QRNG and when the PC actually switches its state. If this delay is not taken into account during the counting analysis then some photons will erroneously be recorded to have been measured in the rectilinear basis when the PC was in fact still set to measure in the diagonal basis and vice versa. In order to continue to fine-tune the alignment and operation of the PC, future work will update the measurement software to reject detection events occurring within ± 5 ns of the switching of the PC (removing measurements of photons which passed through the PC during its rise or fall time when an ambiguous rotation was implemented). As well, inputs allowing for a delay to be added to the QRNG state signal will also be added to the software.

5.5 Conclusion

In conclusion of this chapter, I have detailed the alignment of new free-space receivers incorporating an active polarization analyzer for use in a spacelike separated Svetlichny inequality experiment performed over optical links. I began by giving some background on Svetlichny's work and deriving a version of his inequality. I then mentioned the results of a previous experiment by Lavoie *et al.* [88] which was the first experimental violation of Svetlichny's inequality; albeit, in a setting which did not enforce locality or freedom-of-choice in the measurement settings. I also gave some background theory on the operation of a Pockels cell which was used to implement a fast unitary in order to switch the measurement basis between the rectilinear and diagonal bases according to the output of a QRNG operated at 1 MHz.

With the background material out of the way I then moved on to detailing my design for the new free-space receiver and active polarization analyzer. I outlined a number of steps needed to properly align the PC in the polarization analyzer including: fine tuning the alignment of the PC along the optical path, an initial measurement of the halfwave

voltage, a procedure for reducing the operating voltage of the PC from the halfwave voltage to the quarterwave voltage thus allowing the PC to be operated at a faster rate with less heating effects, verifying the proper operation of the PC at the QWV, measuring the duty cycle of the PC, a method for getting the PC to operate as a HWP at 22.5° as opposed to one at 45° with HWPs placed before and after the PC set to −11.25°, and finally a procedure for fine-tuning the operation of the PC polarization analyzer. I measured the duty cycle of the PC to be 98.40% and after aligning the PC system I was able to obtain contrasts of 1:25.2 and 1:22.6 in the rectilinear basis and diagonal basis respectively. The remaining degradation of the contrasts is likely due to the duty cycle of the PC and a delay between the QRNG state signal and the actual switching of the PC not being compensated. Future work will address both of these issues in software allowing for contrasts approaching 1:100 to be obtained in both bases.

Chapter 6

Conclusions and Outlook

One of the most fascinating recent developments in research has been how different disciplines have become incredibly interconnected. So much so that ideas as disparate as information theory and fundamental physics have combined to produce ideas for secure information technologies with far reaching consequences. Indeed, information security - be it on the personal, commercial, or governmental level - is one of the major challenges facing us in the new information age of the 21st century.

Most current classical encryption schemes rely on assumptions of computational complexity for their security. The beauty of quantum cryptography methods is that they can be *proven* secure, now and *indefinitely* into the future, relying solely on the assumptions of the laws of physics. Something impossible for all current classical cryptographic methods to claim. During my graduate career, my research focused on taking these ideas and turning them into reliable and practical methods for the next generation of security. More specifically, I designed, built, studied, and improved a system capable of performing quantum key distribution, one of the most basic cryptographic tasks, allowing the distribution of identical secret keys to two users so that they could communicate securely.

My Masters research culminated with the construction of an entangled QKD system with one 430 m free-space link connecting the Institute for Quantum Computing (IQC) with the Centre for Environmental and Information Technology (CEIT) building on the UW campus and the successful distribution of secret keys between them. The first year

of my PhD improved on this with the construction of a second 1,350 m free-space link to the Perimeter Institute (PI), automation of the free-space alignment system, and the successful distribution and analysis of secret keys to users in each building. This system was the first real-time two free-space link QKD test-bed system in the world and showed that QKD could be adapted into a practical technology servicing a university or company campus.

Focused on turning this into a practical technology, I improved the key rate of the system and thus the speed at which it could handle information. I did this in three ways. First, I experimentally investigated a theoretical proposal for biasing the measurement bases and showed a 79% improvement in secret key generated from the same raw key rates. Next, I constructed a second generation entangled photon source with rates two orders of magnitude higher and a lower quantum bit error rate (important for the security of the system). Finally, I studied the free-space link transmission statistics and the use of a signal-to-noise ratio (SNR) filter to improve the key rate. The link statistics have particular relevance for a current project with the Canadian Space Agency to exchange a quantum key with an orbiting satellite - a project that I have participated in two feasibility studies for and is now being assessed as an actual mission.

Wanting to study the usefulness of more recent ideas in quantum cryptography, I then built the first experimental implementation of a different primitive called oblivious transfer. This primitive is a very good candidate to replace secure identification schemes over short distances, such as at ATM machines, which have proven to be particularly susceptible to fraud. As the first implementer, I was able to identify some of the most pressing issues preventing the scheme from becoming more widely adopted including the need to relax the the dependence of the oblivious transfer rate on the loss of the system and the need to extend the security proof to cover a wider ranger of quantum communication channels.

Finally, I concluded my studies with the construction of a second generation free-space quantum receiver, useful for increasing the QKD key rates, but designed for a fundamental test of quantum theory namely a Svetlichny inequality violation. This receiver incorporated an active polarization analyzer capable of switching between measurement bases on a μs time-scale through the use of a Pockels cell while maintaining measurements of very high fidelity.

With my graduate studies concluding it feels like, in some sense, the future is just beginning. With such a successful base built by myself and the multitude of other quantum information researchers, it now seems like the sky is the limit to developing the next generation of quantum technologies. Things like integrated quantum sources, circuits, and measurement devices which shrink current optical setups covering many bulky optical tables down to a single chip not much bigger than a dime. Quantum memories, quantum repeaters, and quantum key distribution with orbiting satellites allowing us to finally realize a global quantum key distribution network providing security for the entire world. Quantum computers with many more qubits than are currently available using ingenious new architectures yet to be invented and perfected. And all sorts of other applications and technologies that we cannot even begin to fathom yet.

To end, I need look no further than the final comic of Calvin and Hobbes, a strip far more philosophical and thought provoking than it ought to be. Which in its end only looked to future possibilities...

Created by Bill Watterson © 1995, used with permission of Universal Uclick 2012

References

[1] N. Lütkenhaus, Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, ON, N2L 3G1, Canada, (personal communication, 2008). 28

[2] L. Lydersen and V. Makarov, Department of Electronics and Telecommunications, NO-7491, Norweigian University of Science and Technology, Trondheim, Norway, (personal communication, 2011). 54, 125

[3] Pockels cell drivers datasheet, 2011. http://www.bme-bergmann.de/pockel.htm.

[4] RTP pockels cell datasheet, 2011. http://www.leysop.com/100khz_rtp_q-switch.htm. 153

[5] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007. 16

[6] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. SECOQC white paper on quantum key distribution and cryptography. *eprint*, quant-ph/0701168, 2007. 25, 55

[7] L.C. Andrews and R.L. Phillips. SPIE Press, 2005. 92

[8] L.C. Andrews, R.L. Phillips, and P.T. Yu. Optical scintillations and fade statistics for a satellite-communication system. *Appl. Opt.*, 34(33):7742–7751, 1995. 92

[9] J. Armengol, B. Furch, C. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeier, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger. Quantum communications at esa - towards a space experiment on the iss. *Acta Astronautica*, 63:165–178, 2008. 22, 90

[10] J.A. Armstrong, N. Bloembergen, J. Ducuing, and P.S. Pershan. Interactions between light waves in a nonlinear dielectric. *Phys. Rev.*, 127:1918–1939, 1962. 75

[11] 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. 5

[12] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE J. of Selected Topics in Quantum Electronics*, 9:1541, 2003. 22, 90

[13] J. Bae and A. Acin. Key distillation from quantum channels using two-way communication protocols. *Phys. Rev. A*, 75:012334, 2007. 37

[14] T. Bartley, B. Heim, D. Elser, D. Sych, M. Sabuncu, C. Wittmann, N. Lindlein, C. Marquardt, and G. Leuchs. Enhanced free-space beam capture by improved optical tapers. In *International Conference on Quantum Communication and Quantum Networking Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering*, volume 36, pages 100–107. Springer Berlin Heidelberg, 2010. 14

[15] N.J. Beaudry, T. Moroder, and N. Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008. 28, 52, 137

[16] J.S. Bell. On the einstein podolsky and rosen paradox. *Physics*, 1:195–200, 1964. 6, 46, 98

[17] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3, 1992. 14

[18] C.H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992. 61, 67

[19] C.H. Bennett and G. Brassard. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, New York, 1984. 10, 11, 23, 50, 52

[20] C.H. Bennett, G. Brassard, C. Crépeau, and U.M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41:1915, 1995. 54, 61

[21] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992. 13, 14, 23, 50

[22] C.H. Bennett, G. Brassard, and J.M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17:210–229, 1988. 61

[23] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.P. Poizat, and P. Grangier. Single photon quantum cryptography. *Phys. Rev. Lett.*, 89:187901, 2002. 14

[24] D. Biggerstaff. Experiments with generalized quantum measurements and entangled photon pairs. Master's thesis, University of Waterloo, 2009. 153, 154, 155, 164

[25] D. Bohm. *Quantum Theory*. Prentice-Hall, Englewood Cliffs, N.J., 1957. 5

[26] J.P. Bourgoin, C. Erven, X. Ma, B. Kumar, I. D'Souza, N. Lütkenhaus, and T. Jennewein. A study on satellite quantum key distribution. *in preparation*, 2011. 22, 30, 64, 90, 91, 107

[27] D. Bouwmeester, J.W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger. Observation of three-photon greenberger-horne-zeilinger entanglement. *Phys. Rev. Lett.*, 82:1345–1349, 1999. 151

[28] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330, 2000. 27

[29] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. *Lect. Notes Comput. Sci.*, 765:410, 1994. 36, 51, 61, 67, 68, 102, 103, 116, 123

[30] G. Brida, M. Genovese, and C. Novero. An application of two-photon entangled states to quantum metrology. *J. Mod. Opt.*, 47:2099–2104, 2000. 93, 129

[31] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons. Practical free-space quantum key distribution over 1km. *Phys. Rev. Lett.*, 81:3283, 1998. 111

[32] Raymond Y.Q. Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.*, 11:045024, 2009. 25, 55, 56, 61

[33] J.L. Carter and M.N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143, 1979. 37, 54, 61, 102, 125

[34] P. Chan. Low-density parity-check codes for quantum key distribution. Master's thesis, University of Calgary, 2009. 124

[35] 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. 6, 46, 98

[36] I.B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. *Proceedings of 46th IEEE FOCS*, pages 449–458, 2005. 113

[37] I.B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A tight high-order entropic quantum uncertainty relation with applications. *Advances in Cryptology - CRYPTO '07, volume 4622 of Lecture Notes in Computer Science*, 4622:360–378, 2007. 133

[38] I.B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Secure identification and QKD in the bounded-quantum-storage model. *Advances in Cryptology - CRYPTO '07, volume 4622 of Lecture Notes in Computer Science*, 4622:342–359, 2007. 111, 115

[39] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92:271–272, 1982. 24

[40] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, and A.J. Shields. Gigahertz decoy quantum key distribution with 1mbit/s secure key rate. *Opt. Exp.*, 16:18790–18797, 2008. 21, 90, 144

[41] J.L. Duligall, M.S. Godfrey, K.A. Harrison, W.J. Munro, and J.G. Rarity. Low cost and compact quantum key distribution. *New J. Phys.*, 8:249, 2006. 142

[42] M. Dušek, N. Lütkenhaus, and M. Hendrych. Quantum cryptography. *Progress in Optics*, 49:381, 2006. 11

[43] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete. *Phys. Rev.*, 47:777–780, 1935. 5

[44] A.K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991. 14

[45] D. Elser, T. Bartley, B. Heim, Ch. Wittmann, D. Sych, and G. Leuchs. Feasibility of free space quantum key distribution with coherent polarization states. *New J. Phys.*, 11:045014, 2009. 14

[46] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D.G. Cory, and R. Laflamme. Symmetrized characterization of noisy quantum processes. *Science*, 317:1893–1896, 2007. 144

[47] C. Erven. On free space quantum key distribution and its implementation with a polarization-entangled parametric down conversion source. Master's thesis, University of Waterloo, 2007. 21, 38

[48] C. Erven, C. Couteau, R. Laflamme, and G. Weihs. Entangled quantum key distribution over two free-space optical links. *Opt. Exp.*, 16:16840–16853, 2008. 14, 21, 61, 111, 122

[49] C. Erven, D. Hamel, K. Resch, R. Laflamme, and G. Weihs. Entanglement based quantum key distribution using a bright sagnac entangled photon source. In O. Akan, P. Bellavista, J. Cao, F. Dressler, D. Ferrari M., Gerla, H. Kobayashi, S. Palazzo,

S. Sahni, X. Shen, M. Stan, J. Xiaohua, A. Zomaya, G. Coulson, A. Sergienko, S. Pascazio, and P. Villoresi, editors, *Quantum Communication and Quantum Networking*, volume 36 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 108–116. Springer Berlin Heidelberg, 2010. 71, 87, 122

[50] C. Erven, B. Heim, E. Meyer-Scott, R. Laflamme, G. Weihs, and T. Jennewein. Studying free-space transmission statistics and improving free-space qkd in the turbulent atmosphere. *in preparation*, 2011. 91

[51] C. Erven, X. Ma, R. Laflamme, and G. Weihs. Entangled quantum key disitribution with a biased basis choice. *New J. Phys.*, 11:045025, 2009. 51

[52] R.L. Fante. Electromagnetic beam propagation in turbulent media. *Proceedings of the IEEE*, 63:1669–1692, 1975. 92

[53] R.L. Fante. Electromagnetic beam propagation in turbulent media: An update. *Proceedings of the IEEE*, 68(11):1424– 1443, 1980. 92

[54] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Exp.*, 15:15377, 2007. 49, 78, 81, 88, 110

[55] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger. High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Physics*, 5(6):389–392, 2009. 98, 99

[56] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982. 1

[57] G. Finn. Isogyre pattern, 2011. http://www.brocku.ca/earthsciences/people/gfinn/. 158

[58] M. Fiorentino, G. Messin, C.E. Kuklewicz, F.N.C. Wong, and J.H. Shapiro. Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints. *Phys. Rev. A*, 69(4):041801, Apr 2004. 77

[59] D.L. Fried. Scintillation of a Ground-to-Space laser illuminator. *Journal of the Optical Society of America*, 57(8):980–983, 1967. 92

[60] C.H. Fung, K. Tamaki, B. Qi, H.K. Lo, and X. Ma. Security proof of quantum key distribution with detector efficiency mismatch. *Quant. Info. Compu.*, 9:131–165, 2009. 27

[61] R.G. Gallager. Low density parity check codes. *IRE Trans. Info. Theory*, IT-8:21–28, 1962. 102, 124, 125

[62] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Comm.*, 2:349, 2011. 11, 26, 137

[63] R. Ghosh, C.K. Hong, Z.Y. Ou, and L. Mandel. Interference of two photons in parametric down conversion. *Phys. Rev. A*, 1986:3962–3968, 34. 72

[64] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, 2002. 11, 13, 15, 111

[65] Deny Hamel. Realization of novel entangled photon sources using periodically poled materials. Master's thesis, University of Waterloo, 2010. 72, 75, 76, 81

[66] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A Tomita. Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *eprint*, quant-ph/0705.3081, 2007. 111

[67] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita. Security analysis of decoy state quantum key distribution incorporating finite statistics. *eprint*, quant-ph/0707.3541, 2007. 56

[68] B. Heim, D. Elser, T. Bartley, M. Sabuncu, C. Wittmann, D. Sych, C. Marquardt, and G. Leuchs. Atmospheric channel characteristics for quantum communication with continuous polarization variables. 98:635–640, 2010. 14

[69] C.K. Hong and L. Mandel. Theory of parametric frequency down-conversion of light. *Phys. Rev. A*, 31:2409–2418, 1985. 72

[70] C.K. Hong and L. Mandel. Experimental realization of a localized one-photon state. *Phys. Rev. Lett.*, 56:58, 1986. 14

[71] Rolf Horn. *Waveguide Sources of Photon Pairs*. PhD thesis, University of Waterloo, 2011. 75, 76

[72] 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 J. Phys.*, 4:43.1, 2002. 14

[73] D.S. Hum and M.M. Fejer. Quasi-phasematching. *Comptes Rendus Physique*, 8:180–198, 2007. 76

[74] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863, 1995. 27

[75] W.Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, 2003. 14

[76] T.D. Jennewein. *Quantum Communication and Teleportation Experiments Using Entangled Photon Pairs*. PhD thesis, University of Vienna, 2002. 15

[77] 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. 49, 78, 110

[78] Y.H. Kim, M.V. Chekhova, S.P. Kulik, M.H. Rubin, and Y. Shih. Interferometric bell-state preparation using femtosceond-pulse-pumped spontaneous parametric down-conversion. *Phys. Rev. A*, 63:062301, 2001. 77

[79] M. Koashi, Y. Adachi, T. Yamamoto, and N. N. Imoto. Security of entanglement-based quantum key distribution with practical detectors. *eprint*, quant-ph/0804.0891, 2008. 28, 52, 137

[80] R. Koenig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *eprint*, quant-ph/0906.1030, 2009. 113, 114

[81] P. Kok and S.L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61:042304, 2000. 129

[82] A.N. Kolmogorov. The local structure of turbulence in incompressible viscous fluid for very large reynolds numbers. *Doklady ANSSSR*, 30:301–304, 1941. 92

[83] H. Krawczyk. Lfsr-based hashing and authentication. *Advances in Cryptology - CRYPTO '94 - Lecture Notes in Computer Science*, 839:129–139, 1994. 54, 102, 125

[84] 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. 14

[85] P.G. Kwiat, P.H. Eberhard, A.M. Steinberg, and R.Y. Chiao. Proposal for a loophole-free bell inequality experiment. *Phys. Rev. A*, 49:3209–3220, 1994. 77

[86] 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. 30, 76, 89

[87] P.G. Kwiat, E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A*, 60:773–776, 1999. 77, 151

[88] J. Lavoie, R. Kaltenbaek, and K.J. Resch. Experimental violation of svetlichny's inequality. *New J. Phys.*, 11:073051, 2009. 147, 149, 151, 166

[89] M. Lindenthal. *Long-Distance Free-Space Quantum Communication with Entangled Photons*. PhD thesis, University of Vienna, 2006. 14

[90] H.K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154–1162, 1997. 113

[91] H.K. Lo and H.F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410–3413, 1997. 113

[92] H.K. Lo, H.F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18:133–165, 2005. 48, 50, 52, 108

[93] M.G. Luby, M. Mitzenmacher, M.A. Shokrollahi, and D.A. Spielman. Improved low-density parity-check codes using irregular graphs. *IEEE Trans. Inf. Theory*, 47:585–598, 2001. 125

[94] N. Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59:3301, 1999. 56

[95] N. Lütkenhaus. Security against invidual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000. 50

[96] L. Lydersen, M. Akhlaghi, H. Majedi, J. Skaar, and V. Makarov. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New J. Phys.*, 13:113042, 2011. 26, 137

[97] X. Ma, C.H. Fung, and H.K. Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, 2007. 15, 25, 27, 37, 39, 50, 52, 54, 56, 100

[98] X. Ma, F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.K. Lo. Decoy-state quantum key distribution with two-way classical postprocessing. *Phys. Rev. A*, 74:032330, 2006. 55

[99] X.S. Ma, B. Dakic, W. Naylor, A. Zeilinger, and P. Walther. Quantum simulation of the wavefunction to probe frustrated heisenberg spin systems. *Nature Physics*, 7:399–405, 2011. 59

[100] D.J.C. MacKay and R.M. Neal. Near shannon limit performance of low density parity check codes. *Electronics Letters*, 33:457–458, 1997. 102, 124, 125

[101] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74:022313, 2006. 26, 127, 137

[102] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.*, 89:101122, 2006. 14, 111

[103] V. Markarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11:065003, 2009. 26, 137

[104] I.L. Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel. Proof-of-concept of real-world quantum key distribution with quantum frames. *New J. Phys.*, 11:095001, 2009. 102, 111, 124

[105] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology - Proceedings of Crypto '96*, page 343, Berlin, 1996. Springer Verlag. 111, 143

[106] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78:3414–3417, 1997. 113

[107] G.D. Miller. *Periodically Poled Lithium Niobate: Modeling, Fabrication, and Nonlinear Optical Performance*. PhD thesis, Stanford University, 1998. 76

[108] P.W. Milonni, J.H. Carter, C.G. Peterson, and R.J. Hughes. Effects of propagation through atmospheric turbulence on photon statistics. *J. Opt. B: Quantum Semiclass. Opt.*, 6:S742–S745, 2004. 92, 96

[109] P. Mitchell, S. Popescu, and D. Roberts. Conditions for the confirmation of three-particle nonlocality. *Phys. Rev. A*, 70:060101, 2004. 151

[110] D. Mogilevtsev. Diagonal element inference by direct detection. *Opt. Commun.*, 156:307–310, 1998. 145

[111] G. Moore. Cramming more components onto integrated circuits. *Electronics*, 38:114–117, 1965. 1

[112] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000. 2, 3, 7

[113] NIST. NIST timing software, 2008. http://tf.nist.gov/service/its.htm. 36

[114] J.E. Nordholt, R.J. Hughes, G.L. Morgan, C.G. Peterson, and C.C. Wipf. Present and future free-space quantum key distribution. *Proc. SPIE*, 4635:116, 2002. 22, 90

[115] Z.Y. Ou and L. Mandel. Violation of bell's inequality and classical probability in a two-photon correlation experiment. *Phys. Rev. Lett.*, 61:50–53, 1988. 76

[116] Z.Y. Ou, L.J. Wang, and L. Mandel. Vacuum effects on interference in two-photon down conversion. *Phys. Rev. A*, 40:1428–1435, 1989. 72

[117] D. Pearson. High-speed qkd reconciliation using forward error correction. In *QCMC*, 2004. 102, 124, 142

[118] M. Peev, C. Pacher, R Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T Debuisschert, E. Diamanti, M. Dianati, J.F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A.W. Sharpe, A.J. Shields, D. Stucki, M. Suda C. Tamas, T. Themel, T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.L. Yuan, H. Zbinden, and A. Zeilinger. The secoqc quantum key distribution network in vienna. *New J. Phys.*, 11:075001, 2009. 111

[119] C.Z. Peng, T. Yang, X.H. Bao, J. Zhang, X.M. Jin, F.Y. Feng, B. Yang, J. Yang, J. Yin, Q Zhiang, N. Li, B.L. Tian, and J.W.Pan. Experimental free-space distribution of entangled photon pairs over 13km: Towards satellite-based global quantum communication. *Phys. Rev. Lett.*, 94:150501, 2005. 14

[120] J. Perdigues, B. Furch, C. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger. Quantum communications at esa - towards a space experiment on the iss. In *58th International Astronautical Congress*, Hyderabad, India, 2007. 22

[121] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, The Netherlands, 1995. 7

[122] F. Pockels. *Lehrbuch der Kristalloptik*. Leipzig, 1906. 153

[123] A. Predojevic, S. Grabher, and G. Weihs. *in preparation*, 2012. 86

[124] R. Prevedel. *Experimental All-Optical One-Way Quantum Computing*. PhD thesis, Universität Wien, 2008. 153, 155

[125] B. Qi, C.H. Fung, H.K. Lo, and X. Ma. Time-shift attack in practical quantum cryptosystems. *Quant. Info. Compu.*, 7:73, 2007. 26, 127, 137

[126] J.G. Rarity, P.R. Tapster, P.M. Gorman, and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New J. Phys.*, 4:82, 2002. 22, 90

[127] 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. 14

[128] A. Rossi, S. Olivares, and M. Paris. Photon statistics without counting photons. *Phys. Rev. A*, 70:055801, 2004. 145

[129] 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. 5

[130] M.H. Rubin, D.N. Klyshko, Y.H. Shih, and A.V. Sergienko. Theory of two-photon entanglement in type-ii optical parametric down-conversion. *Phys. Rev. A*, 50:5122–5133, 1994. 72

[131] B.E.A Saleh and M.C. Teich. *Fundamentals of Photonics*. John Wiley & Sons Inc., Hoboken, N.J., second edition, 2007. 153

[132] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Exp.*, 19:10387–10409, 2011. 111

[133] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. A framework for practical quantum cryptography. *Rev. Mod. Phys.*, 81:1301–1350, 2009. 11, 14, 25, 111

[134] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way processing. *Phys. Rev. Lett.*, 100:200501, 2008. 56

[135] V. Scarani and R. Renner. Security bounds for quantum cryptography with finite resources. *eprint*, quant-ph/0806.0120v1, 2008. 55, 56

[136] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phys. Rev. A*, 82:032308, 2010. 113, 115, 116, 121, 126, 127, 128, 129, 132, 133, 134, 140, 142, 145

[137] C. Schaffner, B. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *eprint*, quant-ph/0807.1333, 2008. 113, 114

[138] T. Scheidl. *A Fundamental Test and an Application of Quantum Entanglement*. PhD thesis, Universität Wien, 2009. 153, 154, 155, 158, 161, 165

[139] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. Langford, T. Jennewein, and A. Zeilinger. Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences of the United States of America*, 107:19708–19713, 2010. 98, 99, 154, 161, 165

[140] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J.G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144km. *Phys. Rev. Lett.*, 98:010504, 2007. 111

[141] A.A. Semenov and W. Vogel. Quantum light in the turbulent atmosphere. *Phys. Rev. A*, 80:021802, 2009. 92, 93

[142] A.A. Semenov and W. Vogel. Entanglement transfer through the turbulent atmosphere. *Phys. Rev. A*, 81:023835, 2010. 92, 93

[143] C.E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948. 41

[144] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:657, 1949. 41

[145] J.H. Shapiro. Scintillation has minimal impact on far-field bennett-brassard 1984 protocol quantum key distribution. *Phys. Rev. A*, 84:032340, 2011. 92

[146] B.S. Shi and A. Tomita. Generation of a pulsed polarization entangled photon pair using a sagnac interferometer. *Phys. Rev. A*, 69(1):013803, Jan 2004. 78, 110

[147] Y.H. Shih and C.O. Alley. New type of einstein-podolsky-rosen-bohm experiment using pairs of light quanta produced by optical parametric down conversion. *Phys. Rev. Lett.*, 61:2921–924, 1988. 76

[148] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pages 124–134, Los Alamitos, CA, 1994. IEEE Computer Society. 1

[149] P.W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441, 2000. 50, 52, 111

[150] T. Sugimoto and K. Yamazaki. A study on secret key reconciliation protocol "cascade". *IEICE Trans. Fundamentals*, E83A No. 10:1987, 2000. 43, 45, 51, 56, 61, 67, 102, 103, 116, 123

[151] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a bell-type inequality. *Phys. Rev. D*, 35:3066–3069, 1987. 149

[152] V.I. Tatarskii. US Department of Commerce, Springfield, VA, 1971. 92

[153] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.*, 84:4737, 2000. 71

[154] T. Tsurumaru and K. Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78:032302, 2008. 28, 52, 137

[155] 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. 14

[156] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144km. *Nature Physics*, 3:481–486, 2007. 14

[157] D.Y. Vasylyev, A.A. Semenov, and W. Vogel. Towards global quantum communication: Beam wandering preserves quantumness. *eprint*, quant-ph/1110.1440, 2011. 92

[158] G.S. Vernam. Cypher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elec. Eng.*, 55:109, 1926. 24

[159] S. Wehner, M. Curty, C. Schaffner, and H.K. Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, 2010. 113, 121, 126, 127, 128, 129, 132, 139, 140, 145

[160] S. Wehner, C. Schaffner, and B.M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, 2008. 113, 114

[161] G. Weihs and C. Erven. Entangled free-space quantum key distribution. *Proceedings of SPIE - Quantum Communications Realized*, 6780:1–9, 2007. 21

[162] 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. 5, 14

[163] S. Wiesner. Conjugate coding. *Sigact News*, 15:78–88, 1983. 10

[164] F.N.C. Wong, J.H. Shapiro, and T. Kim. Efficient generation of polarization-entangled photons in a nonlinear crystal. *Laser Physics*, 16:1517–1524, 2006. 78, 110

[165] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982. 15, 24

[166] M. Yamada, N. Nada, M. Saitoh, and K. Watanabe. First-order quasi-phase matched $LiNbO_3$ waveguide periodically poled by applying an external field for efficient blue second-harmonic generation. *Appl. Phys. Lett.*, 62:435–436, 1993. 76

[167] Z.L. Yuan, J.F. Dynes, and A.J. Shields. Avoiding the blinding attack in qkd. *Nature Photonics*, 4:800–801, 2010. 26

[168] G. Zambra, A. Andreoni, M. Bondani, M. Gramegna, M. Genovese, G. Brida, A. Rossi, and M. Paris. Experimental reconstruction of photon statistics without photon counting. *Phys. Rev. Lett.*, 95:063602, 2005. 145

[169] G. Zambra and M. Paris. Reconstruction of photon-number distribution using low-performance photon counters. *Phys. Rev. A*, 74:063830, 2006. 145