Polarization Entangled Photon Sources for Free-Space Quantum Key Distribution

by

Ramy Tannous

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Masters of Science
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2018

AUTHOR'S DECLARATION

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the 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.

ABSTRACT

Free-space quantum key distribution has recently achieved several milestones, such as the launch and results of the first quantum satellite, Micius. The emergence of quantum satellites has certainly made progress towards the realization of a global quantum cryptographic network.

In this thesis, two challenges in the development of an optical quantum ground station for a free-space quantum satellite link are studied. The first is the development of a high brightness, fiber pigtailed waveguide that is to be used as a polarization entangled photon source. The high pair production rate is required in order to meet the requirements for a satellite up-link configuration. The portability, robustness and ease of alignment were motivations for choosing a fiber pigtailed source. Certain challenges that are fundamental to the source design were characterized and several solutions to these challenges were investigated.

The other main investigation in this thesis, is the development of a passive polarization compensation using polarization maintaining fibers. The birefringence in standard single mode optical fibers causes random polarization rotations to the light passing through the fiber. Polarization maintaining fibers, though very high in birefringence, are used with entangled photons and techniques from reference frame independent quantum key distribution protocols are shown to compensate for random polarization rotations while preserving the entanglement. In addition, the feasibility of the protocol using the polarization maintaining fibers is investigated.

Through various studies, experiments, and component design, the feasibility of a pigtailed waveguide entangled photon source has been shown to need further investigation, while the feasibility of implementing polarization maintaining fibers to the ground station has been shown to be effective. It is particularly effective as a passive polarization compensation system that uses entanglement, however a similar concept is effective for non-entangled single photons. This work contributes to a long line of achievements leading towards satellite implementations of quantum key distribution for an eventual global quantum cryptographic network.

STATEMENT OF CONTRIBUTIONS

This thesis contains work done in collaboration with others but to which I made the major contribution. The contributions are listed below.

Chapter 1:

Ramy Tannous wrote the introductory chapter.

Chapter 2:

Jean-Philippe Bourgoin and Thomas Jennewein designed and purchased the waveguide SPDC source.

Ramy Tannous conducted the characterization and construction of the polarization entangled photon source.

Chapter 3:

Jeongwan Jin built and characterized the 6-state and 4-state analyzer.

Thomas Jennewein, Patrick Coles and Jeongwan Jin provided background theory.

Ramy Tannous and Thomas Jennewein developed the simulation models.

Ramy Tannous performed the alignment, conducted the experiments and analyzed the data.

ACKNOWLEDGMENTS

To start, I would like to thank my supervisor Thomas Jennewein for giving me many opportunities during this degree. I feel I have truly been given a great variety of experiences and have had many insightful discussions on not only the research at hand but on science in general. I would also like to thank my Advisory Committee members: Michele Mosca, Norbert Lutkenhaus for their guidance and the filling of various forms. I would also like to thank Raymond Laflamme for joining my Examining Committee.

I would also like to thank all the Quantum Photonics Laboratory group members, past and present, for all the truly helpful discussions, fun, hard work and advice. The people you work with have a great influence on your experience, so thank you for making it a good one. Thank you to the Fun Office past and present, Chris Pugh, Aimee Gunther and Sebastian Slaman, you all made waking up, coming into school and being in the office worth it. So many shenanigans, so many rude squash shots, so much fun happened in that office, for us and the IQC. Thank you for making this degree experience so great.

A special thanks to my good friend Matthew Brown for all the interesting discussions, great times and good food shared, you have helped me tremendously throughout this degree. To all the good friends I have met during this degree, there are way too many of you to list here but you all know who you are, thank you. I am truly thankful for all the good times, discussions and late nights that were shared. IQC connects so many people from so many places and I am happy to have met you all. I would also like to thank the IQC and physics staff, students and faculty, who have no idea how many times they have been super helpful and a joy to be around.

Thank you to my friends back home for supporting me and randomly asking me how I am doing. To my rock, Shandelle Stroeder, thank you for being a listening ear, supportive and encouraging through this entire degree. And last, but most definitely not the least, I would like to thank my family, my parents Victoria and George, and my brothers Fouad and Waseem for supporting me and encouraging me from afar. I am truly lucky and could not have achieved this degree without so many wonderful people helping me along the way.

I would also like to acknowledge the National Science and Engineering Council of Canada, which funded me personally during my Master's.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Quantum Information

The emerging field of quantum information provides many exciting grounds of study. From developing quantum computers [1], to simulating quantum field theories on quantum computers [2],[3],[4], to making novel sensors [5], to providing secure communication [6]. The latter, which is most relevant to this thesis and more specifically quantum key distribution that enables users to transfer an encryption key with minimal information being leaked to an eavesdropper. The security stems from the physical security of the protocol which is the fundamental laws of quantum mechanics.

1.1.1 Quantum Key Distribution

In 1984, Charles Bennett and Gilles Brassard introduced the world to their now famous quantum cryptography protocol known as BB84 [7]. This was the first protocol of quantum key distribution (QKD), which utilizes the fundamental laws of nature to provide security. These fundamental laws are the quantum mechanical notions of the Heisenberg uncertainty principle [8] and the no-cloning theorem [9, 10].

The Heisenberg uncertainty principle is most commonly seen as:

$$\delta_x \delta_p \geq \frac{\hbar}{2} \tag{1.1}$$

which is saying that the smaller the uncertainty in the position of a particle, the larger the uncertainty of its momentum. This relationship applies to any two complementary variables such as angular momentum along different axes, etc. In a more general sense,

the more one knows about one aspect of a given state, the less one knows about its complementary aspect of the same state.

The no-cloning theorem states that one cannot copy an unknown quantum state without disturbing the original state [1]. This can be shown with a simple example: Consider that a user has a quantum machine that has two slots, H_A and H_B, and suppose the user wants to copy the state of H_A to H_B, [11]. Let $|\psi\rangle$ be the state that is initially in H_A and $|i\rangle$ be initially in H_B such that the initial state of the system is

$$|\psi\rangle \otimes |i\rangle. \tag{1.2}$$

Now suppose the user has some means of applying a unitary U[2] such that it can copy the state from H_A to H_B, i.e. $U(|\psi\rangle \otimes |i\rangle) = |\psi\rangle \otimes |\psi\rangle$. Now let us apply this to two arbitrary states $|\psi\rangle$ and $|\phi\rangle$.

$$\begin{aligned} U(|\psi\rangle \otimes |i\rangle) &= |\psi\rangle \otimes |\psi\rangle \\ U(|\phi\rangle \otimes |i\rangle) &= |\phi\rangle \otimes |\phi\rangle \end{aligned} \tag{1.3}$$

If the user now decides to take the scalar product[3] of the two equations in Eq. (1.3), assuming the $|i\rangle$ is normalized, the result is

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2. \tag{1.4}$$

This is equivalent to saying $x = x^2$ which has only two solutions: $x = 1$ or $x = 0$. Therefore, $|\psi\rangle$ and $|\phi\rangle$ are either the same state ($x = 1$), or they are orthogonal ($x = 0$). This, thus shows that one cannot copy any unknown state and that a general quantum cloning device is not possible [11].

The most common QKD protocols use photons to encode their information. These photons are individual quanta of light that, due to the no-cloning theorem, cannot be reproduced without being disturbed. Different photon degrees of freedom provide the basis where the information can be encoded. One of the degrees of freedom used to encode information is the geometric polarization of a photon, this is discussed in more detail below, however, there are many others such as time-bin encoding [12, 13], and orbital angular momentum [14, 15], to name a few.

[1] If the state is fully known then one can create a clone.

[2] The reader may be wondering what happens if something that is not unitary is chosen? According to [11], the cloning using non-unitary devices is still not possible unless the user is willing to sacrifice errors in the cloning process, such as a loss in fidelity (see Sec. 1.1.4 and Eq. (1.23)).

[3] Note that the scalar product here can also be referred to as the inner product and is not limited to discrete variables but can also apply to continuous functions.

Photon Polarization as a Qubit

A quantum bit (qubit) is the fundamental unit in the field of quantum information. A qubit can be a discrete two state system, but this is not necessary as it can be a subsystem of a multi-state system or a continuous system. The difference between a qubit and a classical bit is that the qubit can take on the value of 0 or 1 or some linear combination (superposition) of the two. Qubits that are orthonormal form a basis for a two dimensional Hilbert space and, thus form the basis for any quantum state. A good visualization tool of a qubit space is a unit sphere called the Bloch sphere [11], Fig. 1.1. The quantum states are depicted by a vector on this sphere, the poles of the sphere represent conventional bases. For example, the poles along the Z-axis depict the computational basis of $|0\rangle$ and $|1\rangle$. Any unitary operation done on a qubit, such as a Pauli Z gate[4], is equivalent to rotations along the Bloch sphere [11].

For photon polarization[5], we can classify any polarization as being the $|0\rangle$ state, the orthogonal polarization being the $|1\rangle$ state, and the superposition states are any superposition of these two polarizations. A good question to ask is,"what makes polarization a qubit, since polarization is not a quantum property?" The polarization itself does not make the qubit but rather the single photon with a polarization can be a qubit. Single photons cannot be measured without disturbing the initial state of the photon, while classical light can be measured while keeping the initial polarization state intact. The polarization analog for the Bloch sphere is the Poincaré sphere [17] and can be used for single photons. Therefore, it is convenient to use a polarized single photon in the sense of a qubit.

A common convention is for the $|0\rangle$ to be $|H\rangle$, or the horizontal polarization state, and $|1\rangle$ to be the $|V\rangle$, or the vertical polarization state. However, no one is limited to this convention. A complete list of the common convention that is followed in this thesis can be found in Tab. 1.1.

Entangled Photons

For this work and in quantum information in general, some of the most interesting algorithms and protocols arise from the quantum phenomena known as entanglement. To explain entanglement, let us consider a system made of two subsystems that can be repre-

[4]For those unfamiliar with the typical quantum information gates please see [11] for a good explanation.

[5]For those unfamiliar with polarization, it is simply the direction in which the transverse electric field oscillates with respect to some reference.

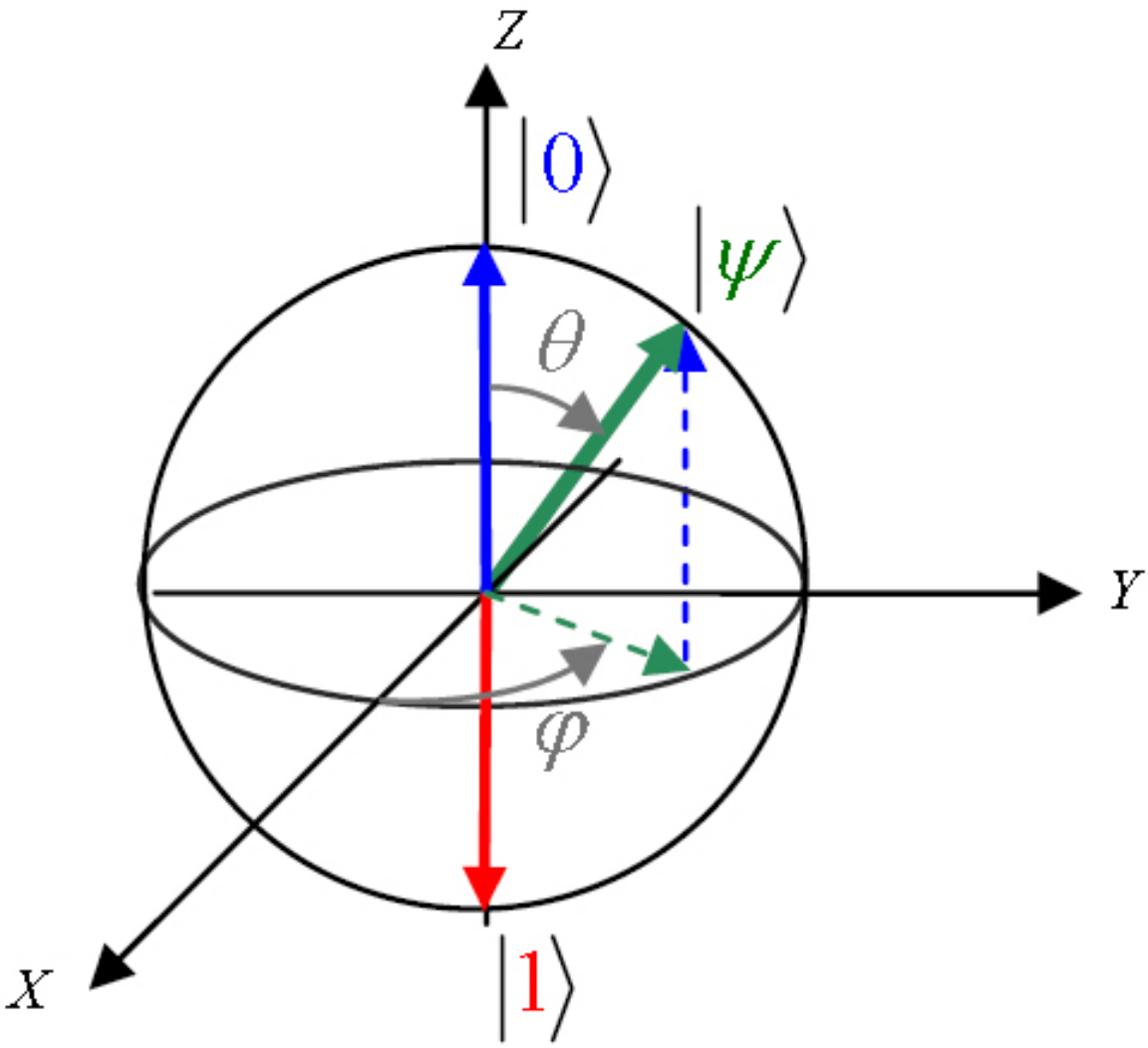


Figure 1.1: Depiction of the Bloch sphere. Image is taken directly from [16].

Polarization	Axis on Bloch Sphere	Computational Basis
$\|H\rangle$	$+\hat{z}$	$\|0\rangle$
$\|V\rangle$	$-\hat{z}$	$\|1\rangle$
$\|D\rangle$	$+\hat{x}$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
$\|A\rangle$	$-\hat{x}$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
$\|R\rangle$	$+\hat{y}$	$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$
$\|L\rangle$	$-\hat{y}$	$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$

Table 1.1: Definitions of the various polarization states in the computational basis and as their pole on the Bloch sphere.

sented by the Hilbert space:

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \tag{1.5}$$

Now suppose we have a state $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, there exists a product state $|\psi_1\rangle \otimes |\psi_1\rangle \in \mathcal{H}$. This is called a separable state because the total state can be described as a product of two states and can be separated into its individual parts. However, it is know that quantum mechanics allows for superposition states, which can create states that are not separable. It is these states that are called entangled states. Examples of non-separable states are the well known Bell states:

$$\begin{aligned} |\psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \\ |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \end{aligned} \tag{1.6}$$

If only one of the two qubits is measured, the measurement results of this qubit will be random. However, if both qubits are measured, the results when measured in the computational basis, will be anti-correlated and correlated for the $|\psi\rangle$ and $|\phi\rangle$ states respectively. As a consequence of entanglement, the correlations are not limited to the computational basis, but the correlations seen in any basis provided that both qubits are measured in the same basis. Entangled photons are used and examined throughout this work and several entanglement QKD protocols have been developed [18],[19]. The entanglement helps to prevent unintentional information leaks through the unused degrees of freedom [20]. In practical implementations, entanglement provides a robustness against multi-photon emissions, since the visibility, (Eq. (1.9)), of the state is reduced if the source emits too many photon pairs. If interested, the reader is encouraged to see [6] and [21] for security proofs of entanglement based QKD.

In this thesis, one of the key ingredients to complete the reference frame independent QKD work done in Chap. 3 is entanglement based QKD. Entanglement based QKD differs from standard QKD in that the sender and receiver can ensure the quality of the quantum channel by checking both the correlations between the two parties and also via other methods such as Bell- or CHSH-test, (particular for device independent QKD implementations [22, 23]). For more information on entanglement based protocols, see [6] and [21].

Basic QKD Concepts

In every transmission of photons, there will be N number of bits that are transferred. Of these N bits only N_c are correct while N_i will be the incorrect results. Given the number of correct and incorrect results, we can define the quantum bit error ratio (QBER) Eq. (1.7), which is a very important metric in determining the success of key transfer.

$$\text{QBER} = \frac{R^w}{R} \tag{1.7}$$

where R is the total detection rate and R_n^w is the error rate amongst R. The visibility of the correlations can also be used when expressing a minimally attainable QBER.

$$\text{QBER}_{\text{min}} = \frac{1 - \text{vis}}{2} \tag{1.8}$$

where the visibility in terms of a wave interference maximum (I_{max}) and minimum (I_{min}) is given by,

$$vis = \frac{I_{\text{max}} - I_{\text{min}}}{I_{\text{max}} + I_{\text{min}}}. \tag{1.9}$$

In theory, most protocols can withstand an eavesdropper if the QBER remains less than a threshold from which classical security algorithms can take over, this has historically been $\approx$ 11% for the BB84 protocol [24]. However, most practical applications require a more strict conditions that are dependent on the implementation, i.e. QBER$<$ 7% [25]. Knowing the limit for the QBER also tells the implementor what minimum value of visibility is needed in order to successfully transfer a key.

BB84 Protocol

Below I will discuss the steps of the BB84 protocol [7]. The main protocol will involve two polarization bases, the horizontal and vertical basis (Z basis), and the diagonal and anti-diagonal basis (X basis). For each photon sent:

- Alice (the sender) and Bob (the receiver) agree on which geometric polarization corresponds to which bit and measurement outcome.
- Alice then randomly selects a bit to send and records it.
- Alice selects a basis to send this bit to Bob and records it.

- Alice sends the properly polarized photon to Bob.
- Bob randomly selects a basis to measure the photon and records it.
- Bob measures the photon and records the bit outcome.
- Alice and Bob then compare the basis that they randomly selected and keep only the bits that correspond to the event where they selected the same basis.
- The raw key is formed from the bits that were kept during the basis comparison step above.
- Alice and Bob then compare a subset of the bits that are randomly selected and check to see how many agree. If a sufficient amount agree (based on error tolerances), Alice and Bob keep the raw key, if not it is discarded

After the steps above are complete, the protocol moves to what is referred to as classical post processing. This involves steps where the raw key undergoes error correction and privacy amplification. The error correction step involves Two of the most common forms of Error Correction are the Low Density Parity Check (LDPC) [26–28] and CASCADE algorithms [29]. These codes, check the parities between blocks of Alices and Bobs sifted keys which means they sum blocks of the raw key and perform a sum modulo 2 (XOR), keeping only the blocks that whose parities match. With the matching parities, one bit from the block is kept while the rest are discarded. If the parities do not match, all the bits are discarded. If enough bits are kept, Alice and Bob now share a secret key know as an error corrected key. The next step is to perform the privacy amplification which ensures the security of the key. One common method of privacy amplification is to use what are called universal hash functions [30]. Alice and Bob will reduce the size of their key during the privacy amplification step. The reduction in key size depends on how much information they assume Eve to have obtained during the key transfer. Once Complete, Alice and Bob share a secret key that can be used in a symmetric algorithm such as the One-Time-Pad [31] or other encryption algorithms.

1.1.2 Reference-Frame-Independent QKD Protocols

For reference frame dependent protocols such as standard BB84 and other entanglement protocols, both Alice and Bob need to agree on fixed measurement bases as this is essential for state discrimination and thus key generation. However, in reference frame independent (RFI) protocols, one basis or none of the bases are aligned. There are several papers in

the literature that use multi-photon state protocols (i.e. GHZ states) [32–34]. However, these protocols are not practical, particularly for transmission losses. In free-space QKD, the transmission probability of the state scales with the number of photons, thus the more photons required, the lower the transmission probability and consequently, a lower keyrate. There is also the additional complexity of state preparation and measurement. In this thesis, we use the simpler case of a two qubit entangled state where, ideally one photon is transmitted across the free-space link. In our protocol, we restrict the computational basis, the bases from which a key will be extracted, to be fixed, while the others are free to rotate by some rotational phase ϕ [35]. In the conventional single photon QKD the arbitrary rotation of reference frame significantly affects QBER since its measurement outcome directly becomes a raw key, and therefore a post-process for the compensation of the rotation is necessarily required to keep the QBER in check. However, one can carefully choose the correlation terms to form a good parameter that is independent of the frame rotation yet sensitive to the information leakage [35], acting like a CHSH-parameter in the conventional entanglement based QKD [18]. The CHSH-parameter is given by:

$$S = E(a,b) - E(a',b) - E(a,b') + E(a',b') \tag{1.10}$$

$$S \leq 2\sqrt{2} \tag{1.11}$$

where the $E(a,b)$ is the correlation coefficient of the measurements performed by Alice along a or a' and Bob along b or b' [36]. Now using a carefully selected "good" parameter, similar to the CHSH-parameter, one can implement a QKD protocol under an arbitrary frame rotation. The payment is to add one more basis in the state analyzer. These, RFI protocols are useful in many settings such as free-space satellite links and time-bin encoded QKD. Below, I will present one form of entanglement based protocol where Alice and Bob share some state that is ideally a maximally entangled Bell state.

One example of an RFI protocol is to set the rotational polarization basis as in [35], as being fixed or well defined for both Alice and Bob. The other two bases are not required to be well defined or fixed. The rotational basis is thus the computational basis, while the other two linear bases are free to rotate by some phase angle β. For the remainder of this document, the Pauli matrices $[\sigma_x, \sigma_y, \sigma_z]$, will correspond to the D/A, R/L and H/V polarization bases, respectively and be known as $[X, Y, Z]$, see Tab. 1.2. Thus, in our example, $Y_A = Y_B$ [6]. The other two bases will drift as a function of β and can be written as the relations $X_B = \cos(\beta)X_A + \sin(\beta)Z_A$ and $Z_B = \cos(\beta)Z_A - \sin(\beta)X_A$. Alice and Bob both independently and randomly select a basis to measure their half of the entangled

[6] Subscript A corresponds to Alice's measurement while subscript B corresponds to Bob's measurement.

state and record the measured quantum signal. After the transmission of the quantum signal is complete, they share their basis measurement choices and the raw key will consist of the times where they both measure in the Y basis. With the QBER being measured as:

$$Q_Y = \frac{1 - \langle Y_A Y_B \rangle}{2} \tag{1.12}$$

while the information known to an eavesdropper will be measured using the results of the other bases. More specifically, using the parameter,

$$C = \sqrt{\langle X_A X_B \rangle^2 + \langle Z_A X_B \rangle^2 + \langle X_A Z_B \rangle^2 + \langle Z_A Z_B \rangle^2} \tag{1.13}$$

which, for maximally entangled states, is independent of the phase and rotation angle β. See Appendix B for more details. Now, due to Pauli algebra, $C \leq \sqrt{2}$ where the equality of $C = \sqrt{2}$ is when Alice and Bob share a maximally entangled state, which is also the case when $Q_Y = 0$ [35]. However, for any value of $C < \sqrt{2}$, Alice and Bob can attribute this to be noise caused by an eavesdropper, Eve. Thus, Alice and Bob can use this C parameter to bound Eve's knowledge [35]. I will not go into a formal security proof here, however, a proof can be found in [35].

Table 1.2: Polarization basis with the corresponding Pauli spin matrix. The symbols used in this work are in the last column

Basis	Pauli Spin Operator	Symbol
H/V	σ_z	Z
D/A	σ_x	X
R/L	σ_y	Y

1.1.3 QKD Ground Station

To achieve a global QKD network, the combination of fiber-based and free-space QKD systems are necessary [37, 38]. Fiber-based implementations are limited to the order of 100 km range due to the intrinsic losses within optical fibers [37, 38]. However, free-space implementations, particularly satellites, provide the capabilities of connecting users separated by great distances. The Quantum Photonics Laboratory is particularly interested in developing an up-link satellite QKD system known as QEYSSat [39]. An up-link means that the satellite will be used as a receiver while a ground station on Earth is used as a sender. There are several advantages to an up-link, one of which is that the satellite

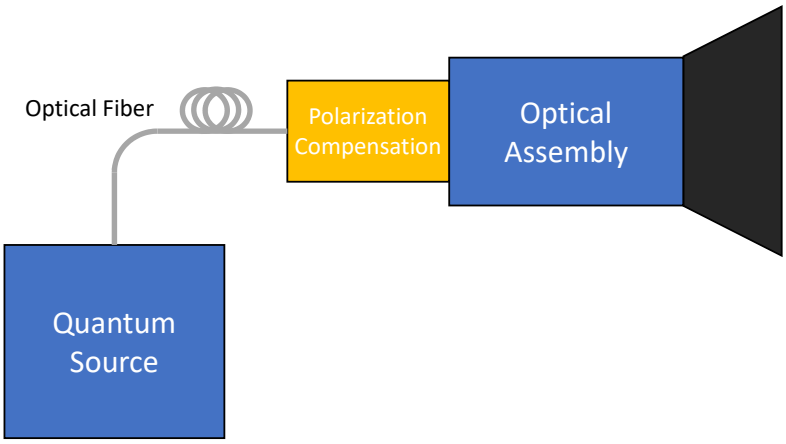


Figure 1.2: Optical quantum ground station suitable for an up-link satellite implementation. The quantum source can be easily exchanged for emerging technologies as well as the optical assembly. Here, the optical fiber can be a single mode fiber, or as seen in Chap. 3, a polarization maintaining fiber.

design complexity is reduced and that the quantum source can be easily maintained and exchanged with new emerging technologies [38].

Though there are many components with challenges for the QEYSSat mission, the ground station is of interest for this work. At a high level of abstraction, the ground station consists of a quantum source that prepares a state to be sent (in our case a polarization state), an optical assembly to enable the transmission of the photon such as a telescope, and a polarization compensation system that corrects any errors obtained going from the source to the optical assembly, see Fig. 1.2.

For an up-link QKD ground station, there are two main challenges that are addressed by this work. One is that the source must be able to produce photons at a high rate and have other requirements that are outlined in Sec. 1.2.2. Chapter 2 provides the work done on a proposed high rate entangled photon source that can meet the requirements of Sec. 1.2.2.

The other challenge is that the fiber which connects the quantum source to the optical assembly, causes birefringent polarization rotations, as outline in Sec. 3.1. The birefringence rotations are results of manufacturing defects and small amounts of stress in the

core of the fiber that can alter the relative index of refraction of the different polarization modes, which can cause power mixing [40]. This problem is amplified further when the fiber is bent or moved while the optical assembly is moving in order to track a satellite. Therefore, the need for a polarization compensation system is very important. However, the current system on the QEYSSat ground station is quite complex and consists of moving parts, active state reconstruction and active feedback controlling compensatory wave plates [38]. However, the work done in Chap. 3 demonstrates a passive polarization compensation system that does not require moving parts or adaptive feedback.

1.1.4 Quantum State Tomography

In many quantum information experiments, it is useful to perform quantum state tomography. Tomography is effectively a reconstruction or estimation of a quantum system based on measurements that are performed on the quantum system [11]. With a series of repeated measurements on an ensemble of states, one can sufficiently estimate an arbitrary state of a quantum system. With a limited and well defined set of measurements, quantum tomography can determine the entire state of a system prior to its measurement. Many techniques of tomography require the measurement of the four Stoke's parameters (or Pauli measurements) [41]. The Stoke parameters can be linked to experimentally measurable quantities such as coincidence counts.

Matrix Inversion Method

Most tomography techniques require the inversion of a linear system and what is known as a tomographically complete set of measurements. Tomographically complete measurements means that the positive-operator valued measurements (POVM) are selected such that they form an operator basis on the entire Hilbert space, which provides all the information about the system [11]. If a system contains n qubits, it is represented by a 2^n by 2^n normalized, complex, hermitian matrix which only needs $4^n - 1$ real free parameters to describe it. For example, in the one qubit case, the normalized density matrix can be written as,

$$\rho = \begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & 1 - x_1 \end{pmatrix} \tag{1.14}$$

where x_i are real parameters. Now in most experimental settings that includes experimental noise and imperfect detectors, we need one more parameter to determine the normalization

due to the noise and detector efficiencies. [41]. Now, in the two qubit case, there are 16 data points that are needed to be determined and therefore projections onto 16 state vectors $|\phi_\nu\rangle$. These $|\phi_\nu\rangle$ are tomographically complete if and only if the matrix with elements:

$$B_{\nu\mu} = \langle\phi_\nu|\Gamma_\mu|\phi_\nu\rangle \tag{1.15}$$

is invertible, i.e. nonsingular, which means that the POVM's that correspond to each $|\phi_\nu\rangle$ measurement form a basis of the Hilbert space. The Γ_μ are the set of matrices $\sigma_i \otimes \sigma_j$, where $i, j = 0, 1, 2, 3$ and the σ_i are the 2×2 Pauli matrices. Now from the matrix given in Eq. (1.15), a reconstructed density matrix can be calculated via[7]

$$\rho = \frac{1}{N}\sum_{\nu=1}^{16}\left[\sum_{\mu=1}^{16}(B^{-1})_{\nu\mu}\Gamma_\mu\right]n_\nu \tag{1.16}$$

where N is a normalizing factor defined by taking the trace of the unnormalized Eq. (1.16)

$$N = \sum_{\nu=1}^{16}\mathrm{Tr}\left(\sum_{\mu=1}^{16}(B^{-1})_{\nu\mu}\Gamma_\mu\right)n_\nu$$

and n_ν is the counts obtained when making the projective measurement $|\phi_\nu\rangle$.

This method works well in reconstructing most quantum states, however, there are some downfalls to this method. The first is that it requires a tomographically complete set of projective measurements in order to invert the matrix in Eq. (1.15), [41], otherwise the Moore-Penrose pseudo-inverse [42] can be used. However, a complete set of measurements is not always available for every experiments. In fact, the experiments discussed in Chap. 3 do not have a complete set of measurements, hence this method cannot be used. Another issue with this method is that it is possible that the resulting matrix violates the condition that all density matrices are positive semidefinite, meaning that their eigenvalues are positive and that $\mathrm{Tr}\,(\rho) = 1$. One can create density matrices with this method that are unphysical i.e. $\mathrm{Tr}\,(\rho) \neq 1$ or a negative eigenvalue. The reason this is possible is due to the imperfections in the detectors and experimental noise as well as the constraints that were used to calculate the density matrix. The matrix inversion method does not constrain the resulting matrix to be a physical density matrix. We are simply inverting a linear system to which can have a solution that is nonphysical given the experimental noise and detector imperfections. However, there is another tomography procedure that constrains the resulting density matrix to always be physical and is discussed below.

[7] In [41], there is an error in the indices their equation 3.15

As mentioned above, the matrix inversion method can create unphysical density matrices. The maximum likelihood method uses the same measurements $|\phi_\nu\rangle$, however, it constrains the final density matrix to being positive semidefinite. To do this, we parametrize the density matrix as:

$$\rho = \frac{T^\dagger T}{\mathrm{Tr}\{T^\dagger T\}} \tag{1.17}$$

this will limit the ρ to being positive semidefinite because any matrix that can be written as $G = T^\dagger T$ is must be positive semidefinite for any matrix T [41]. In addition, $T^\dagger T$ is Hermitian and the trace in the denominator of Eq. (1.17) is a normalization factor, thus we have all the constrains needed for a physical density matrix. T is thus a square matrix of dimension d that can be written as a triangular matrix with real numbers on the diagonal such that it only has d^2 free parameters. For the two qubit case, this would be 16 free parameters and the matrix would take the form of:

$$T = \begin{pmatrix} t_1 & 0 & 0 & 0 \\ t_5 + it_6 & t_2 & 0 & 0 \\ t_{11} + it_{12} & t_7 + it_8 & t_3 & 0 \\ t_{15} + it_{16} & t_{13} + it_{14} & t_9 + it_{10} & t_4 \end{pmatrix}. \tag{1.18}$$

There is also a way to express T by the elements of ρ which is useful when using numerical methods to find results, this is outlined in [41].

The next steps in deriving the equation for the maximum likelihood method are to determine how well the calculated density matrix fits the measured data. To do so we assume that the counts collected have an expected value of

$$\bar{n}_\nu = \mathcal{N}\langle\phi_\nu|\rho|\phi_\nu\rangle \tag{1.19}$$

and that they follows a Gaussian probability distribution. $\mathcal{N}$ is a parameter that is dependent on the detector efficiency and photon flux. Thus, the probability of measuring a set of κ counts $\{n_\nu\}$ is given by:

$$P(n_1, n_2, ..., n_\kappa) = \frac{1}{N_{\mathrm{norm}}} \prod_{\nu=1}^{\kappa} \exp\Big[- \frac{(\bar{n}_\nu - n_\nu)^2}{2\bar{n}_\nu} \Big] \tag{1.20}$$

with N_{norm} being a normalizing factor. Now substituting Eq. (1.19) into Eq. (1.20), we get the probability, or likelihood, that ρ could produce the measured data $\{n_\kappa\}$.

$$P(n_1, n_2, ..., n_\kappa) = \frac{1}{N_{\mathrm{norm}}} \prod_{\nu=1}^{\kappa} \exp\Big[- \frac{(\mathcal{N}\langle\phi_\nu|\rho(t_1, t_2, ..., t_\kappa)|\phi_\nu\rangle - n_\nu)^2}{2\mathcal{N}\langle\phi_\nu|\rho(t_1, t_2, ..., t_\kappa)|\phi_\nu\rangle} \Big] \tag{1.21}$$

Now rather than maximizing the value of Eq. (1.21), we can simplify the problem by finding the maximum of its logarithm [41], which reduces the problem further to minimizing the value of Eq. (1.22) [41].

$$\mathcal{L}(t_1, t_2, ..., t_\kappa) = \sum_{\nu=1}^{\kappa} \frac{(\mathcal{N}\langle\phi_\nu|\rho(t_1, t_2, ..., t_\kappa)|\phi_\nu\rangle - n_\nu)^2}{2\mathcal{N}\langle\phi_\nu|\rho(t_1, t_2, ..., t_\kappa)|\phi_\nu\rangle} \tag{1.22}$$

As already mentioned, the advantage of this method is that the resulting density matrix is physical since we constrain and assume it to be a representation of a physical system. The other major advantage of this technique is that it works with an arbitrarily large number of measurements. Indeed, κ can be much larger than $d^2 - 1$ which gives an over-complete tomography. In addition, one does not need a tomographically complete set of POVM's to get an outcome. One simply needs $d^2 - 1$ measurements to obtain a density matrix that occupies the subset of the Hilbert space spanned by the POVM's. The maximum likelihood method is used to reconstruct the states produced in Chap. 3.

To determine the error of the maximum likelihood method, one must be able to quantify how well the resulting density matrix fits the set of measurement data. In Chap. 3, I use a Monte Carlo method to determine the errors in values derived from the resulting density matrix, i.e. fidelity Eq. (1.23). The Monte Carlo method involves adding random Poissonian noise to the data, then performing tomography using the adjusted measurement data. Doing this n-times yields a set of density matrices that can give bounds for the errors of any values derived from the tomography.

Quantifying State Quality

After reconstructing a state via the aforementioned tomography methods, it is convenient to be able to quantify the quality of the state created in an experiment. I will now outline and briefly explain the various measures.

One means to do this is to compare the measured state ρ to a known state σ and measure their "closeness". This effectively means comparing how close one state is to being equal to another state that is desired. Calculating the "closeness" of two quantum states is know as the fidelity and is given by:

$$\mathcal{F}(\rho, \sigma) = \left[\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right]^2 \tag{1.23}$$

where for the positive semidefinite matrix M, $\sqrt{M}$ is the unique positive square root given by the spectral theorem [43]. The fidelity has a couple nice properties namely it is bound

by $0 \leq \mathcal{F}(\rho, \sigma) \leq 1$ and it is symmetric, i.e. $\mathcal{F}(\rho, \sigma) = \mathcal{F}(\sigma, \rho)$ [43]. The two states are deemed to be equivalent if $\mathcal{F}(\rho, \sigma) = 1$ and orthogonal if $\mathcal{F}(\rho, \sigma) = 0$. Thus, one can use the value of the fidelity to quantify the quality of the prepared state as compared to a desired state.

Another method of quantifying the quality of a state is to calculate what is know as the purity of a quantum state. The purity is a measure of how much a state is mixed. It is given by:

$$\text{Pur} = \text{Tr}(\rho^2) \tag{1.24}$$

and has bounds of $\frac{1}{d} \leq \text{Pur} \leq 1$, where d is the dimension of the Hilbert space where the state is defined [11]. The upper bound when $\text{Pur} = 1$, is obtained from the fact that for any system $Tr(\rho) = 1$ and $\text{Tr}(\rho^2) \leq \text{Tr}(\rho)$. However, for a pure state, $\text{Pur} = \text{Tr}(\rho^2) = 1$. While the lower bound is found by calculating the purity of a completely mixed state of a d dimensional Hilbert space, i.e. $\rho = \frac{1}{d} I_d$ [11]. Thus, any tomography that results in a calculated purity that is close to 1 can be regarded as almost a pure state.

In Chap. 3, the state of interest is an entangled state. There are several measures of entanglement [44]. In Chap. 3, we use concurrence and tangle to define the quality of the entanglement. Though they are measurements of the entanglement of a mixed state [41], they can also be convenient in measuring the entanglement of a pure state of a two qubit system [45]. Hence, we use them as a factor for the quality of entanglement.

We start with showing the definition of the concurrence of a two qubit state. First, we must define the spin flipped state operator for a two qubit system,

$$\tilde{\rho} = (Y \otimes Y)\rho^*(Y \otimes Y) \tag{1.25}$$

where ρ^* is the conjugate transpose of ρ and Y the Pauli matrix as per Tab. 1.2. The formula for the concurrence is,

$$\mathcal{C}(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\} \tag{1.26}$$

where λ_i are the eigenvalues of the matrix R where

$$R = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}} \tag{1.27}$$

which is positive semi definite [45]. The tangle of a system is simply defined as [41],

$$T = \mathcal{C}(\rho)^2 \tag{1.28}$$

Both the tangle and concurrence are bounded by $0 \leq T, \mathcal{C}(\rho) \leq 1$ where the upper bound indicates good entanglement and the lower bound indicating a separable state. Therefore, it is easy to verify the quality of the entangled quantum system one is using.

1.1.5 Quantum Illumination

Quantum illumination is an emerging quantum protocol that has direct implications for radar and LIDAR applications. The protocol includes the creation, via a quantum source, of photon pairs that are entangled in energy and time. One photon will be sent to a target, while the other is measured locally at the source. Bouncing the sent beam off a target and measuring the returned signal correlated against the locally measured signal, can, in principle, allow for the detection of targets with very faint signals.The signal, because of the correlations to the locally measured photon, is distinguishable above the background, which itself will have no correlation to the local photon. Thus with good timing analysis, the returned faint correlated signal will be sufficiently distinct compared to any uncorrelated background. These low signal levels allow for the detection of the source of the photons to be difficult compared with current LIDAR applications that use much brighter sources. Another benefit is that any adversary that attempts to intercept the signal will only receive one half of the photon pairs. The statistics of a source, that is one half of an entangled pair, is similar that of a thermal source which makes it difficult to determine the origin of the source. These benefits allow for the application to be relevant in defense type application as outlined in [46]. The source presented in Chap. 2 and the protocol in Chap. 3 could be utilized for quantum illumination applications. However, the realization of such applications is far in the future and were only partial motivators of the creation of the source in Chap. 2.

1.2 Spontaneous Parametric Down-Conversion

One of the most commonly used methods to generate an entangled photon pair has be to use a process known as spontaneous parametric down-conversion (SPDC). It can be described by a pump field (E_p) interacting with a nonlinear medium to split into two fields of lesser energy known as the signal (E_s) and idler (E_i). The down-conversion photons are called signal and idler for historical reasons, with the higher frequency photon being the signal. SPDC is a quantum effect and cannot be described classically. SPDC is used in this work to create entangled photon pairs and I will show a brief summary of its derivation, though if the reader desires a more comprehensive derivation see [47] and [48]. First, we

begin with the multimode quantized electric field[8].

$$\hat{E}_j^{(-)}(\bar{\mathbf{r}},t) = -i\sqrt{\frac{\hbar\omega_j}{2V\epsilon_0}}\int d^3\bar{\mathbf{k}}_j\, d\omega_j\, \bar{\mathbf{e}}_j\, \hat{a}_j^\dagger\, e^{-i(\omega_j t+\bar{\mathbf{k}}_j\cdot\bar{\mathbf{r}})} \quad [9] \tag{1.29}$$

where $\hat{a}_j^\dagger$ is the raising operator, $\bar{\mathbf{e}}_j$ is the polarization vector and $j = i, s$. We now restrict the field to propagate in the z-direction. This is not a necessary step but it makes the derivation simpler.

$$\hat{E}_j^{(-)}(z,t) = -i\sqrt{\frac{\hbar\omega_j}{2V\epsilon_0}}\int d^3\bar{\mathbf{k}}_j\, d\omega_j\, \bar{\mathbf{e}}_j\, \hat{a}_j^\dagger\, e^{-i(\omega_j t+k_{jz}z)} \tag{1.30}$$

We need the Hamiltonian that describes the quantum process of SPDC and apply it to the vacuum state $|vac\rangle$ via the interaction picture.

$$\begin{aligned} |\Psi_{\text{SPDC}}\rangle &= e^{\frac{1}{i\hbar}\int_0^t \hat{H}_{SPDC}(t')dt'}|vac\rangle \\ &= |vac\rangle + \frac{1}{i\hbar}\int_0^t \hat{H}_{SPDC}(t')dt'|vac\rangle + ... \end{aligned} \tag{1.31}$$

Note that we are only interested in the first-order term of this perturbation since the higher-order terms in the expansion yield double pair, triple pair, N-pair down conversions. We have to now address the Hamiltonian itself which can be derived by taking the classical field density of a nonlinear material and quantizing the electric field[10]. The resulting Hamiltonian is:

$$\hat{H}_{SPDC} = \epsilon_0\chi^{(2)}\int_{\mathcal{V}} d^3\bar{\mathbf{r}} E_p^+(z,t)E_s^-(z,t)E_i^-(z,t) + \text{h.c.}, \tag{1.32}$$

where ϵ_0 is the vacuum permittivity, h.c. is the hermitian conjugate, s and i are the indices representing the signal and idler modes, respectively, $\mathcal{V}$ is the volume of the nonlinear crystal that is interacting with the pump beam, and $\chi^{(2)}$ is the nonlinear tensor susceptibility. It is assumed that only the $\chi^{(2)}$ term of the tensor be considered even though other terms exist, their interactions can be considered weak. The derivation of this Hamiltonian will not be explicitly done in this work, but there are several nice derivations available in [48]. We also assume that the pump is monochromatic and can be treated as a classical plane

[8] It has been suggested that the electromagnetic displacement field $\bar{\mathbf{D}}$ be quantized rather than the electric field. This is since quantizing $\bar{\mathbf{D}}$ preserves Faraday's law in the nonlinear material whereas the quantization of the electric field does not [49].

[9] Bold face and $\bar{\mathbf{x}}$ denotes a vector.

[10] Again see [49] for the $\bar{\mathbf{D}}$ field expansion form.

wave beam. If the reader is not familiar with plane waves, I suggest looking at [50]. By substituting Eq. (1.30) and the plane wave monochromatic pump into Eq. (1.32), we get:

$$\begin{aligned}\hat{H}_{SPDC} =&\epsilon_0\chi^{(2)}\int_{\mathcal{V}} d^3\bar{\mathbf{r}}E_{p0}\, e^{i(k_pz-\omega_pt)}\sqrt{\frac{\hbar\omega_s}{2V\epsilon_0}}\int d^3\bar{\mathbf{k}}_s\, d\omega_s\, \bar{\mathbf{e}}_\mathbf{s}\, \hat{a}_s^\dagger\, e^{-i(\omega_st+k_{sz}z)}\\ &\sqrt{\frac{\hbar\omega_i}{2V\epsilon_0}}\int d^3\bar{\mathbf{k}}_i\, d\omega_i\, \bar{\mathbf{e}}_\mathbf{i}\, \hat{a}_i^\dagger\, e^{-i(\omega_it+k_{iz}z)} + \text{h.c.}\end{aligned} \tag{1.33}$$

Now substituting Eq. (1.33) into Eq. (1.31) and keeping only the first order non vacuum term, we get:

$$\begin{aligned}|\Psi_{\text{SPDC}}(z,t)\rangle \simeq\Big(&-\epsilon_0\chi^{(2)}\frac{1}{i\hbar}\int_0^t dt'\int_{\mathcal{V}} d^3\bar{\mathbf{r}}E_{p0}\, e^{i(k_pz-\omega_pt)}\sqrt{\frac{\hbar\omega_s}{2V\epsilon_0}}\int d^3\bar{\mathbf{k}}_s\, d\omega_s\, \bar{\mathbf{e}}_\mathbf{s}\, \hat{a}_s^\dagger\, e^{-i(\omega_st+k_{sz}z)}\\ &\sqrt{\frac{\hbar\omega_i}{2V\epsilon_0}}\int d^3\bar{\mathbf{k}}_i\, d\omega_i\, \bar{\mathbf{e}}_\mathbf{i}\, \hat{a}_i^\dagger\, e^{-i(\omega_it+k_{iz}z)} + \text{h.c.}\Big)|vac\rangle.\end{aligned} \tag{1.34}$$

Now we reduce the SPDC to being single mode and monochromatic, similar to the pump, and combine some terms.

$$\begin{aligned}|\Psi_{\text{SPDC}}(z,t)\rangle \simeq\Big(&i\chi^{(2)}E_{p0}\sqrt{\frac{\omega_s}{2V}}\sqrt{\frac{\omega_i}{2V}}\int_0^t dt'\int_{\mathcal{V}} d^3\bar{\mathbf{r}}\, e^{i(k_pz-\omega_pt)}\, \bar{\mathbf{e}}_\mathbf{s}\, \hat{a}_s^\dagger\, e^{-i(\omega_st+k_{sz}z)}\\ &\bar{\mathbf{e}}_\mathbf{i}\, \hat{a}_i^\dagger\, e^{-i(\omega_it+k_{iz}z)} + \text{h.c.}\Big)|vac\rangle.\end{aligned} \tag{1.35}$$

Now integrating over the volume of the crystal that interacts with the pump ($V = L_xL_yL_z$) and over the interaction time, and restricting each photon to one polarization, we get[11]:

$$|\Psi_{\text{SPDC}}(z,t)\rangle \simeq i\chi^{(2)}E_{p0}\,\frac{\sqrt{\omega_s\omega_i}L_xL_y}{2V}\int_0^t e^{i(\omega_i+\omega_s-\omega_p)t'}dt'\int_0^{L_z} dz\, e^{i(k_pz-k_{sz}z-k_{iz}z)}|1\rangle_s|1\rangle_i \tag{1.36}$$

and completing the integrals and taking that $\chi^{(2)}$ has no z dependence, we get:

$$\begin{aligned}|\Psi_{\text{SPDC}}(t)\rangle \simeq&i\chi^{(2)}E_{p0}\,\frac{\sqrt{\omega_s\omega_i}L_xL_y}{2V}\; e^{i\frac{(\omega_i+\omega_s-\omega_p)}{2}t}\, t\, \text{sinc}\Big(\frac{(\omega_i+\omega_s-\omega_p)t}{2}\Big)\\ &e^{i\frac{(k_p-k_{sz}-k_{iz})L_z}{2}}\, L_z\, \text{sinc}\Big(\frac{(k_p-k_{sz}-k_{iz})L_z}{2}\Big)|1\rangle_s|1\rangle_i.\end{aligned} \tag{1.37}$$

[11]Note that the h.c. term was removed because this contains two lowering operators that take the vacuum state to zero.

Now if the interaction time t is long enough, we can approximate the first sinc as a delta function.

$$|\Psi_{\text{SPDC}}(t)\rangle \simeq \frac{i\chi^{(2)}E_{p0}\sqrt{\omega_s\omega_i}}{2}\, e^{i\frac{(\omega_i+\omega_s-\omega_p)}{2}t}\, \delta(\frac{\omega_i+\omega_s-\omega_p}{2})\, e^{i\frac{\Delta kL_z}{2}}\, \text{sinc}\big(\frac{\Delta kL_z}{2}\big)|1\rangle_s|1\rangle_i \tag{1.38}$$

where $\Delta k = k_p - k_{sz} - k_{iz}$ and E_{p_0} is the amplitude of the pump. Eq. (1.38) shows that the process of SPDC only produces pairs of photons that meet the following conditions. They must first, by consequence of the delta function, have energies that add up to that of the pump,

$$\omega_p = \omega_s + \omega_i \tag{1.39}$$

which is effectively the conservation of energy. A secondly, because of the $\text{sinc}\big(\frac{\Delta kL_z}{2}\big)$ term, the signal will be maximized when,

$$\bar{\boldsymbol{k}}_p = \bar{\boldsymbol{k}}_s + \bar{\boldsymbol{k}}_i \tag{1.40}$$

this is called the phasematching relation. This condition limits the length over which the SPDC interaction may occur coherently within the crystal. This phasematching relation can be tuned and modified to create different signal and idler wavelengths, however this will not be discussed in this work.

Periodic Poling

The aforementioned phasematching is not the easiest thing to achieve. Most nonlinear crystals are dispersive which can cause Eq. (1.40) to not be satisfied, this is obviously problematic when already SPDC has a probability of about 10^{-6} per pump photon [51]. Therefore, quasi-phasematching is developed to modify the material such that the phasematching is satisfied for longer crystal lengths. There are several methods that optimize quasi-phasematching such as temperature tuning and angle of incidence tuning [52]. Both of these methods make use of the birefringence of the materials in order to compensate for the dispersion. However, these methods have some shortcomings, for instance, some nonlinear materials are not birefringent or have insufficient birefringence [53]. One solution that is very popular is called periodic poling, and is the most common method now used to fabricate nonlinear crystals for quasi-phasematching. Periodic poling was first demonstrated by [54] and works for ferroelectric materials. The idea is to apply electrodes to a

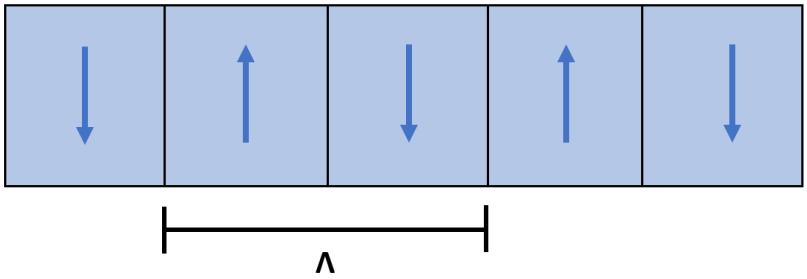


Figure 1.3: A periodically polled material with the poling period labeled.

crystal once every period, which thus reverses the polarity of the domain in the material. This also inverts the sign of the $\chi^{(2)}$, which causes the phasematching condition to become:

$$k_p = k_s + k_i + \frac{2\pi}{\Lambda} \tag{1.41}$$

where Λ has units of length is known as the poling period. More specifically Λ is the distance over which to make one period of polarity reversal, see Fig 1.3.

In general, this method does not suffice to get perfect phasematching. However, with slight temperature adjustments and tuning, the phasematching can be met and in fact, for SPDC, the signal and idler wavelengths may be tuned via the change in temperature.

1.2.1 Types of SPDC

It is now good to mention that there are different configurations of SPDC. The various types are based on pump, signal and idler polarizations. For this work I will use type-0 SPDC for the work described in Chap. 2, which is when all the photons involved are identically polarized i.e. $|H\rangle_p, |H\rangle_s, |H\rangle_i$. For the work done in Chap. 3, the source is a type-II SPDC source. This means that the signal and idler photons have perpendicular polarizations and there is not necessarily any polarization correlation between successive pairs [55], i.e. $|H\rangle_p, |V\rangle_s, |H\rangle_i$. The third type of SPDC, that is not used in this work, is type-I, this is when the signal and idler share the same polarization but can differ from that of the pump, i.e. $|H\rangle_p, |V\rangle_s, |V\rangle_i$.

1.2.2 Desired Specification for SPDC for Free-Space QKD

Amongst the many practical applications of SPDC, QKD is one in which it can be used to produce entangled photon pairs. However, not all nonlinear crystals can give the desired

performances for specific QKD applications. In the case of the QEYSSat mission [39], the requirements for a free-space up-link are far more stringent then for a laboratory setting [56].

The first requirement for QEYSSat system is that the signal photons be produced at around 780 nm [56]. This can be achieved by many different nonlinear crystals including periodically poled Lithium Niobate that is further discussed in Chap. 2. Now the requirement for the idler photon (the partner photon of the signal photon) is less strict and can be any detectable wavelength. However, the ideal case would be a typical telecommunications band such as 1550 nm. The convenience of having the idler photon in the telecommunications range allows for easy integration of the photon pair with fiber optic communication networks.

Another requirement is that the source be sufficiently narrow band in spectrum as to be distinguishable from the background noise [56]. This is ideally on the order of 1 nm but, the narrower the bandwidth, the better. This also includes a limited amount of background noise that can be produced by the nonlinear crystal, see Sec. 2.3.1 for a discussion on this topic.

Since the implementation of the SPDC is a specifically free space satellite up-link, the source must have a brightness, or emission rate, that is capable of producing enough signal in such a channel. The minimum requirement for the brightness of an SPDC source used in an up-link is about 100 MHz [56].

There are also the requirements of practicality, the source should not require optical setups that take up the entirety of a room. The source should also ideally be mobile to and easy to function and align so that it can be utilized in a widespread global network. However, the practicality can be sacrificed if all the other requirements are met, within in reason, of course.

1.3 Waveguide Physics

Waveguides are widely applicable in electromagnetic wave manipulation. They are used in many practical as well as experimental setting. In this work, Chap. 2 particularly, requires the knowledge of several waveguide concepts, the physics involved is thus important in understanding this work. This section will cover the basic physics of a waveguide needed for this thesis as well as some notes on the optical fibers used throughout this work.

1.3.1 Optical Waveguides

The main concept of optical waveguides is the supported solutions for the wave equation or Helmholtz equation. However, we will discuss this in more detail with the specific case of the optical fiber in Sec. 1.3.2. For now we will introduce the concept of optical waveguides with what is know as the metal guide as seen in Fig. 1.4.

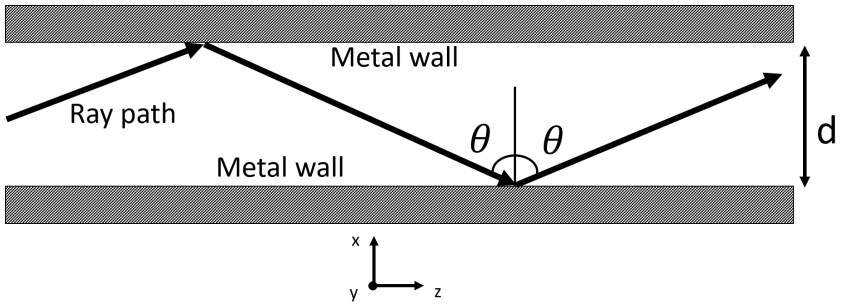


Figure 1.4: Metallic walled waveguide of width d

The walls of this waveguide are mirrors and every time a ray is incident on the mirror, we expect it to be reflected and then re-reflected. This propagation results in an effectively a net z-direction travel. To find out what field is allowed to exist inside the waveguide, we start with the time-independent field that is a y-polarized plane wave traveling along some angle, θ, with respect to the z-axis Eq. (1.42), as seen in the Fig. 1.4.

$$E_y(x,z) = E\exp\big(-ik_0\{z\sin\theta \pm x\cos\theta\}\big) \tag{1.42}$$

with the total field being a combination of both the upward and downward components.

$$E_y(x,z) = E_-\exp\big(-ik_0\{z\sin\theta - x\cos\theta\}\big) + E_+\exp\big(-ik_0\{z\sin\theta + x\cos\theta\}\big) \tag{1.43}$$

The $E_\pm$ is determined by the boundary conditions which are that the fields at $x = 0$ and $x = d$ vanish, i.e. $E_y(0,z) = 0$. Thus for $x = 0$, $E_- = -E_+$ and for $x = d$,$E_y(d,z) = 0$, which gives $\sin k_0 d\cos\theta = 0$. Which finally gives us the condition on which modes and angles are permitted within the waveguide.

$$\cos^{-1}\big(\frac{\pi\nu}{k_0 d}\big) = \theta_\nu \qquad \text{(where } \nu = 1,2,3,...\text{)} \tag{1.44}$$

Eq. (1.44) is referred to as the eigenvalue equation of the waveguide [17]. Each θ_ν corresponds to a particular mode that the guide can support. However, only a finite number of modes are supported, i.e. the case where $\frac{\pi\nu}{k_0 d} > 1$ has no supported modes since the guide is too small ($\frac{\pi\nu}{k_0} > d$). This implies a condition that for any mode to exist $\frac{\pi\nu}{k_0} < d$ and $\frac{\pi}{k_0} > d$ or half the optical wavelength [50]. Now these conditions dictate the number of modes that can be supported by the waveguide, i.e. if d is slightly larger than $\frac{\pi}{k_0}$, then it is a single mode guide, and if d is even larger, the guide becomes multimode.

1.3.2 Optical Fibers

Optical fibers are a circular dielectric waveguides and can be considered probably one of the most common application of optical waveguides. The same concepts from above provide a good basis for understanding the physics of optical fibers. Particularly, the optical fiber supports electromagnetic fields that satisfy the wave equation, or Helmholtz equation, given the boundary conditions and media of the fiber. The fibers can be single mode fibers (SMF), meaning they allow only one spatial mode of light to propagate, while other fibers can be multimode fibers (MMF) and can support many modes. It should be mentioned that we will discuss only step-index fibers where there is two distinct indices of refraction between the core and the cladding materials. However, the reader should be made aware of graded index fibers or GRIN fibers that have a slowly varying core index of refraction. The highest being in the center of the core and the lowest being where the core meets the cladding material. For further information on GRIN fibers the reader is encouraged to look in [17] and [57] as a good starting reference.

Before we discuss the physics of the fields within an optical fiber. I would like to mention an important quantity that dictates the acceptance angle of the fiber. This is known as the numerical aperture (NA) and is given in Eq. (1.45).

$$\mathrm{NA} = \sqrt{n_1^2 - n_2^2} \tag{1.45}$$

Where n_1 and n_2 are the indices of refraction of the core and cladding, respectively. Now given the NA, the acceptance angle of the fiber is given by Eq. (1.46)

$$\mathrm{NA} = \sin\theta_a \tag{1.46}$$

Any ray that is incident on the fiber core with an angle of incidence $\theta < \theta_a$, the ray will propagate through the fiber. However, any ray that is incident with an angle $\theta > \theta_a$, the ray will only propagate a short distance through the fiber before it refracts out of the core since it will not undergo total internal reflection [17]. Like in a waveguide, it is the bounce angles that support a mode that are of interest.

We now proceed to develop the theory of light in fibers. Before we begin, there are a few assumptions to be made. First we assume that this is a weakly guiding fiber, which means that the core and cladding have vary similar refractive indexes, $n_1 - n_2 \ll 1$. For most practical purposes, $n_1 - n_2 \ll 1$ is true. Second, we take the cladding radius to infinity, this very much simplifies the problem and can be done because the fields outside the core decay exponentially (evanescent fields) [58], see also Eq (1.53).

To start, we must find the electric and magnetic fields that propagate in the fiber via Maxwell's equations and the boundary conditions of the fiber. This effectively becomes a Helmholtz equation problem, which is the time-independent form of the wave equation after separation of variables is done. We solve the Helmholtz equation for a generic step index fiber of refractive index $n(r)$ Eq. (1.47) [12] to get the modes and fields that are supported by the optical fiber. Now we restrict the guided modes to waves traveling in the z-direction thus, we take the longitudinal components of E_z and H_z, these satisfy Eq. (1.47). We can use Maxwell's equations to find the transverse components.

$$\nabla^2 U + n(r)^2 k_0^2 U = 0 \tag{1.47}$$

where $k_0 = \frac{2\pi}{\lambda}$, U is the function describing the field, either (E or H components), and

$$n(r) = \begin{cases} n_1, r < a \\ n_2, r > a \end{cases}$$

where a is the core radius. Now writing Eq. (1.47) in cylindrical coordinates we get Eq. (1.48)

$$\frac{\partial^2 U}{\partial r^2} + \frac{1}{r}\frac{\partial U}{\partial r} + \frac{1}{r^2}\frac{\partial^2 U}{\partial \phi^2} + \frac{\partial^2 U}{\partial z^2} + n(r)^2 k_0^2 U = 0 \tag{1.48}$$

By separation of variables $U(r, \phi, z, t) = T(t)R(r)\Phi(\phi)Z(z)$. Now the z and time dependence of $U(r, \phi, z, t)$ can be solved for and make up the factor

$$T(t)Z(z) = \exp[i(\omega t - \beta z)] \tag{1.49}$$

with ω being the monochromatic frequency and β being the propagation constant. Eq. (1.49) should be a common factor for the reader if they are familiar with plane wave solutions to Maxwell's equations [50]. We are now left with the radial and angular dependence of $U(r, \phi, z, t)$. From which we try a solution that is 2π periodic in ϕ with $\nu = 0, 1, 2, ...$

$$R(r)\Phi(\phi) = u(r)e^{-i\nu\phi} \tag{1.50}$$

Substituting Eq.(1.50) into Eq. (1.48) gives us a resulting equation.

$$\frac{\partial^2 u(r)}{\partial r^2} + \frac{1}{r}\frac{\partial u(r)}{\partial r} + \left(n(r)^2 k_0^2 - \frac{\nu^2}{r^2} - \beta^2\right) u(r) = 0 \tag{1.51}$$

[12] Eq. (1.47) can also be derived from Maxwell's equations by eliminating the transverse field components and solving for either E_z or H_z [58].

We get what is the well know Bessel equation. The solutions and type of Bessel function that $u(r)$ gets is dependent on $n(r)$. Now β is within the limits $n_2k_0 < \beta < n_1k_0$. This means that within the fiber core we will get the ordinary Bessel function as the solution, while in the cladding we obtain the modified Bessel function, Bessel-K. Eq. (1.51) can then be written in terms of inside and outside of the core.

$$\begin{aligned} \frac{\partial^2 u(r)}{\partial r^2} + \frac{1}{r}\frac{\partial u(r)}{\partial r} + \left(\kappa^2 - \frac{\nu^2}{r^2}\right) u(r) = 0, \qquad r < a \\ \frac{\partial^2 u(r)}{\partial r^2} + \frac{1}{r}\frac{\partial u(r)}{\partial r} - \left(\gamma^2 + \frac{\nu^2}{r^2}\right) u(r) = 0, \qquad r > a \end{aligned} \tag{1.52}$$

where $\gamma^2 = \beta^2 - n_2^2k_0^2$ and $\kappa^2 = n_1^2k_0^2 - \beta^2$. Now it should be possible to write a solution for $U(r, \phi, z, t) = T(t)R(r)\Phi(\phi)Z(z)$.

$$U(r, \phi, z, t) \propto \begin{cases} J_\nu(\kappa r)\, e^{-i\nu\phi}\, e^{i(\omega t - \beta z)}, & r < a \\ K_\nu(\gamma r)\, e^{-i\nu\phi}\, e^{i(\omega t - \beta z)}, & r > a \end{cases} \tag{1.53}$$

The proportional sign is needed because there are constant out front that are ignored in our derivation. The reader is referred to the great derivation done in [58] for more details on finding the values for these constant and the exact values of all the field components. κ and γ determine the properties of the fields in the fiber. For instance, larger values of γ means faster decay in the cladding ($r > a$) while large values of κ means more radial oscillations in the core ($r < a$). From κ and γ we can define a dimensionless parameter that is very important for the number of modes supported by the fiber called the V parameter that is define in Eq. (1.54).

$$V^2 = (\kappa a)^2 + (\gamma a)^2$$

$$V^2 = \mathrm{NA}^2 k_0^2$$

$$V = 2\pi \frac{a}{\lambda} \mathrm{NA} \tag{1.54}$$

where NA is defined in Eq. (1.45). As eluded to above, this parameter helps determine the number of modes supported in the fiber since it is related parameters that dictate the zeros of the Bessel functions, i.e. κ and γ. For convenience we define $W = \kappa a$ and $\mathrm{T} = \gamma a$ such that $V^2 = W^2 + T^2$. Now the field supported inside the fiber must be continuous at the boundary. Therefore, the function $U(r, \phi, z, t)$ and $U'(r, \phi, z, t)$ must be continuous

at the boundary where $r = a$. Taking the derivative and equating the functions at $r = a$ gives rise to what is know as the characteristic equation, Eq. (1.55).

$$W\frac{J_{\nu\pm1}(W)}{J_\nu(W)} = \pm T\frac{K_{\nu\pm1}(T)}{K_\nu(T)} \tag{1.55}$$

Now given that $T = \sqrt{V^2 - W^2}$ and knowing the value of V and ν, the only parameter we need to solve for is W. The solutions to this equation can be done graphically by plotting the left-hand side and the right-hand side and the intercepts are where the solutions for W are found, see Fig. 1.5

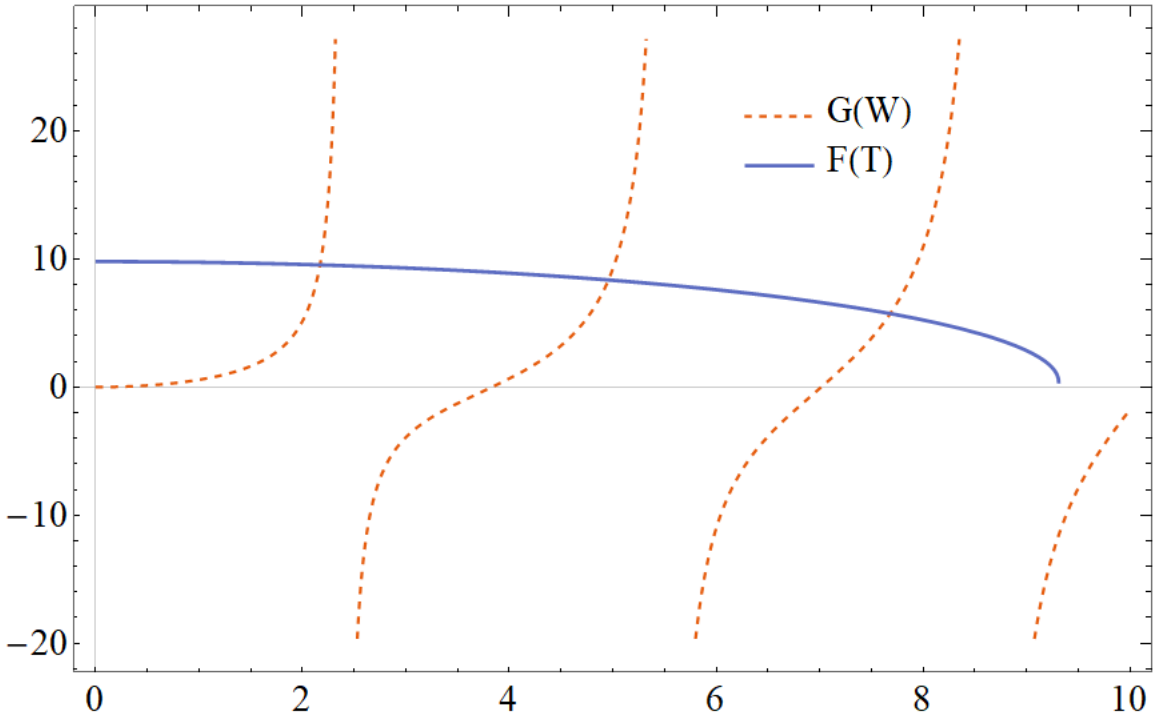


Figure 1.5: Solutions to the characteristic equation for a fiber with a V parameter of $V \approx 9$. In this graph $\nu = 0$. Each intersection corresponds to a W_m with $m = 1, 2, 3, ...$, but $W_m \leq V$. Here $G(W)$ corresponds to the left-hand side of Eq. (1.55), while $F(T)$ corresponds to the right-hand side. Both axes are unitless.

To determine the number of modes in a fiber, one must estimate the number of roots of Eq. 1.55. For large values of V, the number of modes N can be approximated by the formula

$$N \approx \frac{V^2}{2}. \tag{1.56}$$

A derivation of this formula can be found in [58] and similar concepts are used in applied mathematics for various partial differential equation problems that are eigenvalue problems similar to the case of the optical fiber.

1.3.3 Polarization Maintaining Fibers

Polarization maintaining fibers (PMF) are designed specifically to maintain the polarization of any light that is coupled into either one of its polarization mode axes. The typical single mode fiber (SMF) should in theory not effect the polarization state of the light transmitting through it. However, any break in the rotational symmetry of the fiber's refractive index will cause the polarization modes of a fiber to mix or rotate.

Polarization maintaining fibers have two axes that will preserve any polarization that is aligned to these axes [59]. They are know as the slow and fast axis. The concept behind this is to alter the index of refraction of the core such that there are two distinct indexes of refraction. Unfortunately, these two axes, due to differences in their respective refractive indexes, create a phase difference between the two polarizations.

The reader might be wondering why would one make a polarization maintaining fiber such that the axes of the fiber have differing indexes of refraction. In theory, there should be no need to do this to normal single mode fibers if the incident light is purely in one polarization since there should be no mixing into the other polarization mode. However, in practice, due to fiber imperfections and strain, having the group and phase velocities matched allows for the different polarization modes to mix, thus regular single mode fibers cause polarization rotations and drift [17]. This would not be an issue if the fibers were simply used for transferring power. However, due to this polarization mixing in single mode fibers, the resulting output polarization is elliptical and thus impractical for polarization sensitive applications such as QKD. In order to reduce the polarization mode mixing, manufacturers introduce a phase difference through a group velocity delay of one polarization mode relative to another that is orthogonal. This makes it very difficult for the two polarizations to mix as they are not phase matched when traversing the fiber. The slow axis literally means that the light couped with a polarization mode along that axis will travel slower than that along the fast axis.

Any polarization not aligned to one of these two axes, such that both polarization modes are excited, the light will be subject to the polarization mode dispersion caused by the induced fiber asymmetry. One will slip out of phase relative to the other. The difference birefringence will cause a rotation to the polarization and at most points throughout the fiber, the polarization will be elliptical. However, if the phase difference becomes 2Π, the

original polarization is returned. Thus the effect of a (uniform) birefringence is to cause a general polarization state to evolve through a periodic sequence of states as it propagates. The length over which this occurs is the fiber beat length $L_b = 2\pi/\beta$. An integer number of these beat lengths will result in the original polarization being returned. However, in many applications, the number of beat lengths experienced by the light will not be integer and the unaligned polarizations will most likely be returned in an elliptical state.

The phase difference, or asymmetry in the index of refraction, of the PMF's, can be produced in several difference ways [59]. The most common way is to induce a stress along one axis of the fiber core that will cause a relative difference between two orthogonal axes of the fiber. This can be done via several techniques such as; physically pressing the fiber core [60], using stress inducing rods such as the Bow-tie [31] and Panda fibers [61]. The polarization maintaining fibers used in this work are all Panda fibers.

Chapter 2

Waveguide Entangled Photon Source

In this chapter, I will discuss the work done on a bright entangled photon source. The project was an attempt to make a source that is capable of meeting the requirements of Sec. 1.2.2. We start with the characterization of the waveguide crystal and show the promising brightness, then move to the issues and discuss the difficulties encountered, present the attempted solutions and their results. Then conclude with the future ideas and outlook.

2.1 Design

The selection of the periodically poled lithium niobate magnesium oxide doped (PPLN-MgO) waveguide crystal was done with a satellite QKD link in mind, Sec. 1.2.2. The idea was to select a crystal that has a high brightness, 100 MHz pair rate, and is capable of being mobile thus requiring easy alignment. In considering the mobility and easy alignment, the choice was made to pigtail two 780 nm PM fibers of 1 m in length, to the waveguide. The fibers were to create a source that is mobile and simple to align as per the requirements in Sec. 1.2.2. I was not involved in any of the design choices and selection of the crystal as this was done before my arrival to the Quantum Photonics Lab.

The choice of a waveguide over a bulk crystal was made since the waveguide allows for the pump light to have a longer interaction length with the nonlinear material in comparison to bulk crystals [62]. The idea is that the waveguide prevents the need for the pump light to be focused down tightly, which would cause damage to the crystal and reduce the interaction length with the nonlinear material.

2.1.1 Sagnac Loop

The design of the source is based off the well established Sagnac loop design. See [53] for a description of these sources. We plan to implement this system using a rotated PM fibers in one arm similar to the source in [63]. In order to generate polarization entangled photons, we use a 405 nm pump laser that pumps a nonlinear optical crystal from two sides at the same time to produce photon pairs with spontaneous emission. These photon pair emissions are combined on a polarizing beam splitter (PBS) which closes the interferometer. This is known as a Sagnac interferometer. Because the paths of the interferometer are indistinguishable, the photon pairs cannot be connected to a specific path, and therefore become entangled in their polarization. This correlation can be used for quantum communications and other applications requiring entangled photons.

The overall design of this Sagnac loop can be seen in Fig. 2.1. The Thorlabs NanoMax™ stages were selected in order to have fine adjustment capabilities since coupling into single mode fibers can be difficult. The PPLN waveguide that was selected, is a type-0 crystal. All the down conversion propagates back towards the pump and needs to be separated from the pump by a dichroic mirror, as seen in Fig. 2.1. All the optics that are in Fig. 2.1 prior to the SMF 405 nm are used to get a monochromatic pump, Fig. 2.2. As will be discussed in Sec. 2.3.1, there is a large amount of noise present in the waveguide and reducing the pump to a clean monochromatic beam is a means of troubleshooting the source of the noise. See Appendix A for details on how a non-monochromatic pump can reduce source quality.

2.1.2 Detection Analyzer

The detection of the photon pairs was done using the setup found in Fig. 2.3 know as the frequency analyzer in Fig. 2.1. The wavelengths of the signal and idler photons were not at ideal peaks for the central wavelengths of the filters. This required rotating the filter in order to shift the central wavelength [64].

The photons are separated from each other in the setup shown in Fig. 2.4. The separation of the photons allowed for coincidence detection between the signal and the idler. This was done using single photon avalanche diodes (SPAD's) and timetaggers of 158ps resolution.

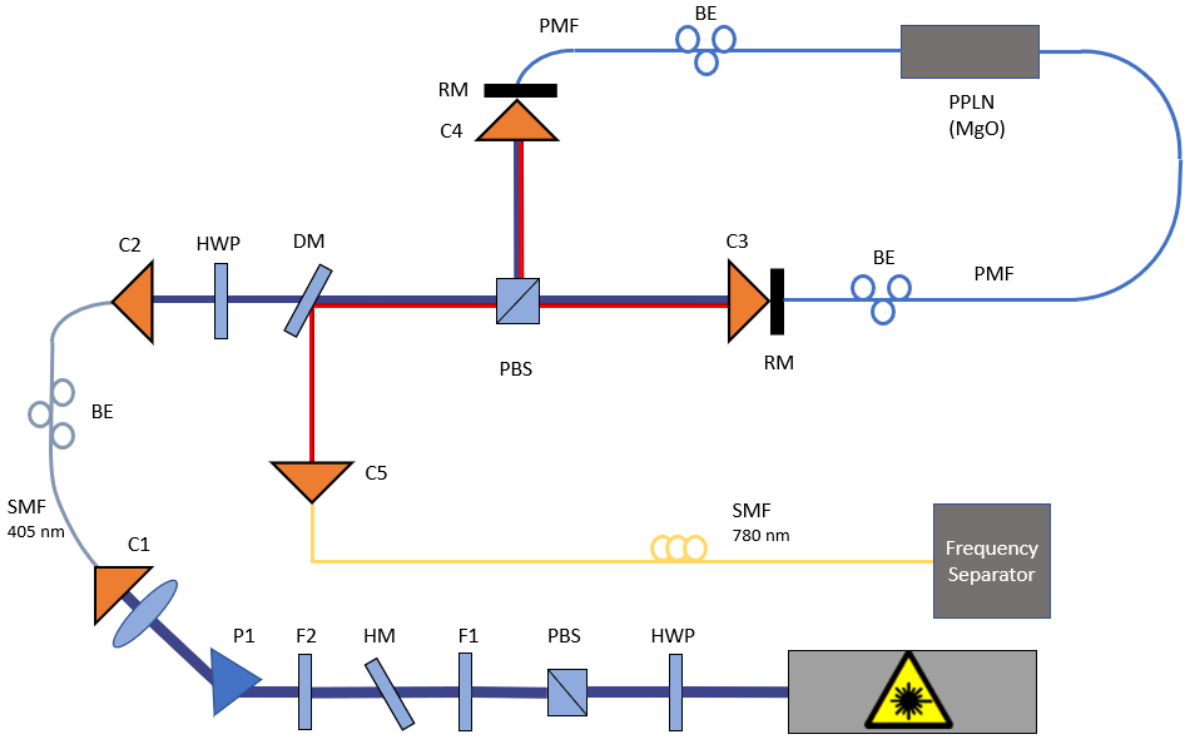


Figure 2.1: Schematic optical setup of the pigtailed waveguide Sagnac loop. The pump wavelength is 405 nm and the signal and idler wavelengths are centered around 785 nm and 834 nm respectively. HWP- 405 nm half wave plate, PBS- polarizing beam splitter, F1- Thorlabs FES0800 shortpass filter, HM- Thorlabs M253H45 hot mirror, F2- Thorlabs FGB37 color filter, P1- prism, C1-C5 Thorlabs Nanomax 6-axis Fiber coupling stages, DM- dichroic mirror reflect red and transmit blue, SMF- Single mode fiber, PMF- polarization maintaining fiber, RM- Fiber rotating mount, BE- Bat ears.

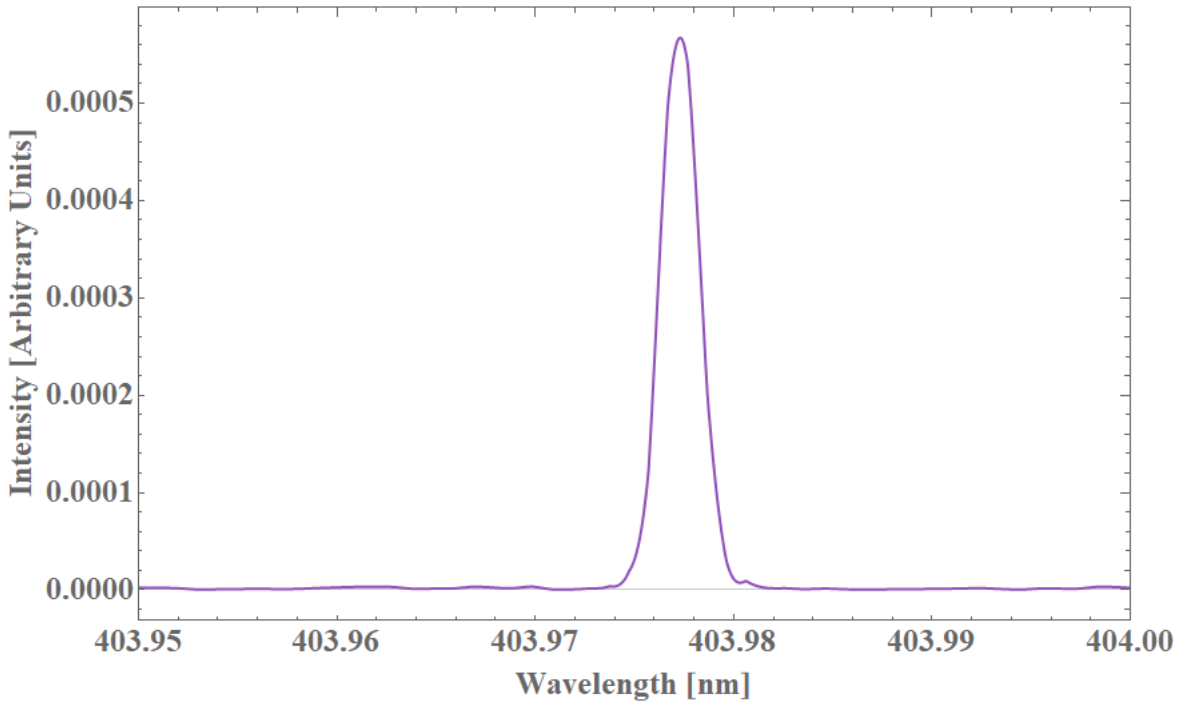


Figure 2.2: Pump spectra, the various optical elements that are in the pump path prior to the SMF 405 nm are to ensure a monochromatic pump as seen in the spectra.

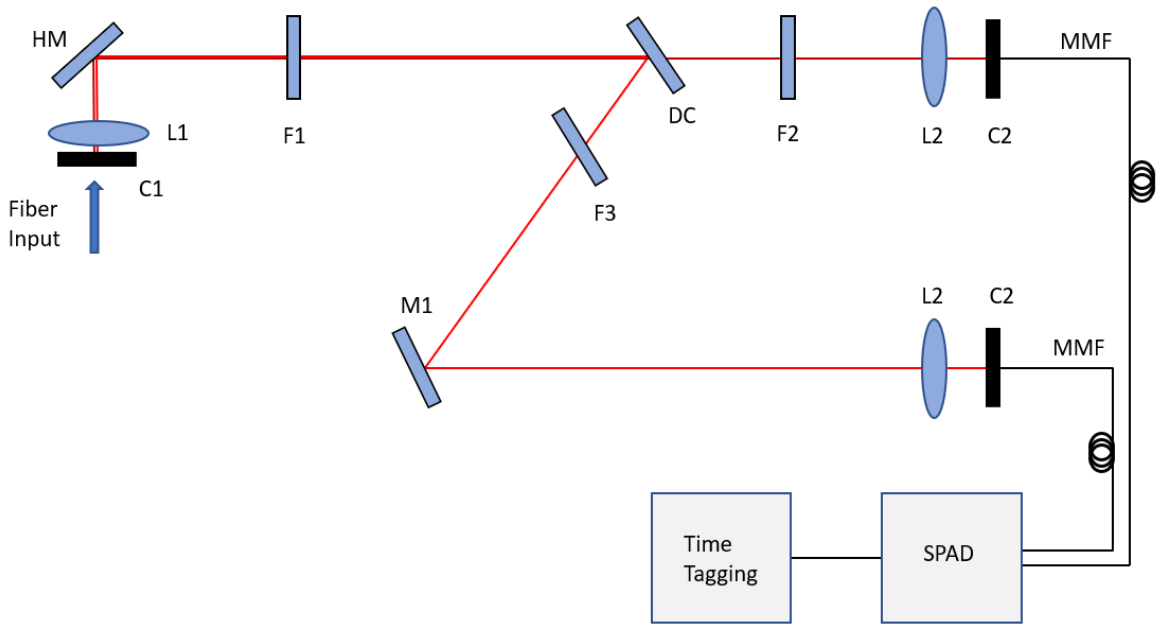


Figure 2.3: Schematic optical setup of the frequency separator for the coincidence analysis of the photons. C1-C2-Fiber coupling stages, L1-Thorlabs F220FC-780 fiber collimator, F1-Thorlabs FEL0750 longpass filter, DC-Thorlabs DMSP805 dichroic mirror, F2-Semrock LL01-785-12.5 bandpass filter, F3-Thorlabs FL850-10 laser line filter, M1-Thorlabs P01 silver mirror, L2-Thorlabs RMS10X achromat objective, MMF-Thorlabs multimode fiber, SPAD-Excelitas Single Photon Avalanche Diode detectors.

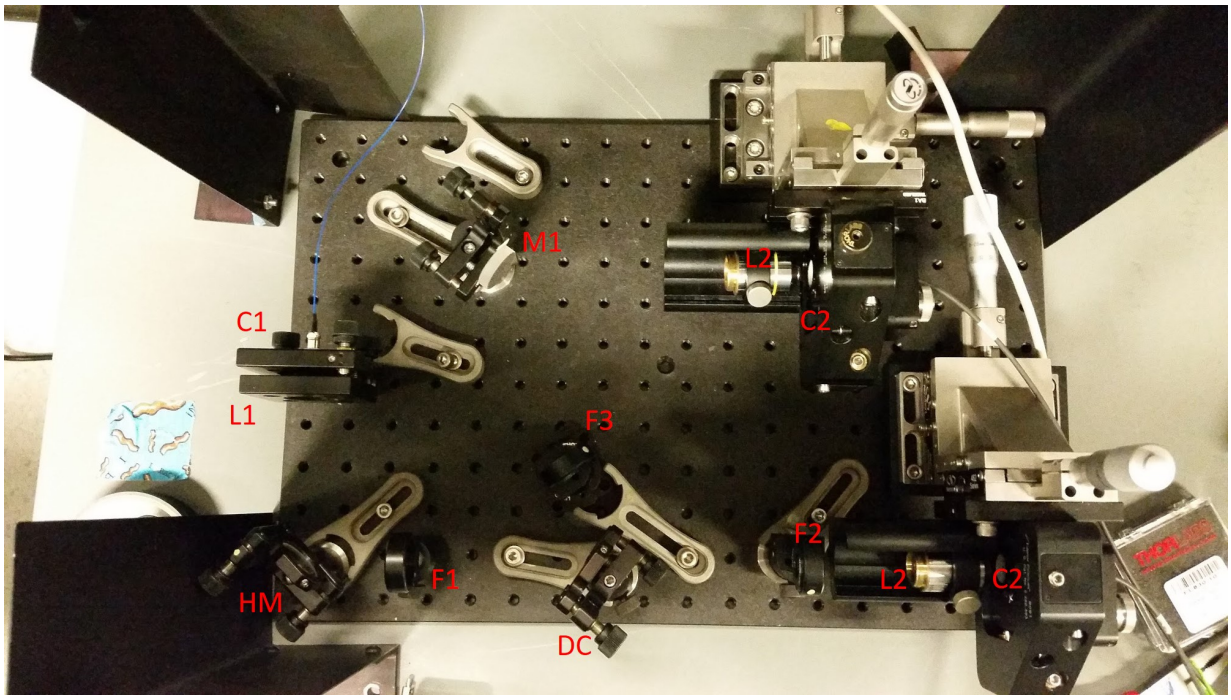


Figure 2.4: Optical setup as seen in the experiment of the frequency separator for the coincidence analysis of the photons, the individual components and description of labels are found in Fig. 2.3

2.2 Characterization of the Crystal

2.2.1 Phase Matching and SPDC Spectra

In order to produce the appropriate wavelength, the crystal temperature must be tuned appropriately as the down converted photons' energies are a function of the crystal temperature. The phase matching curve is shown in Fig. 2.5.

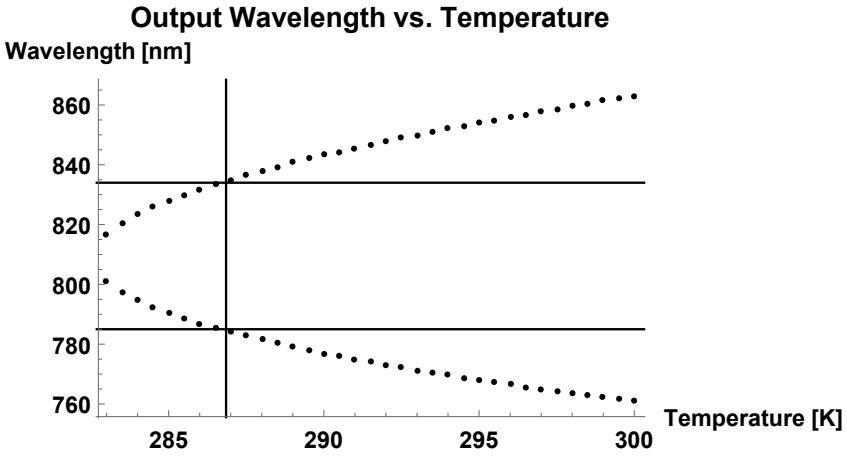


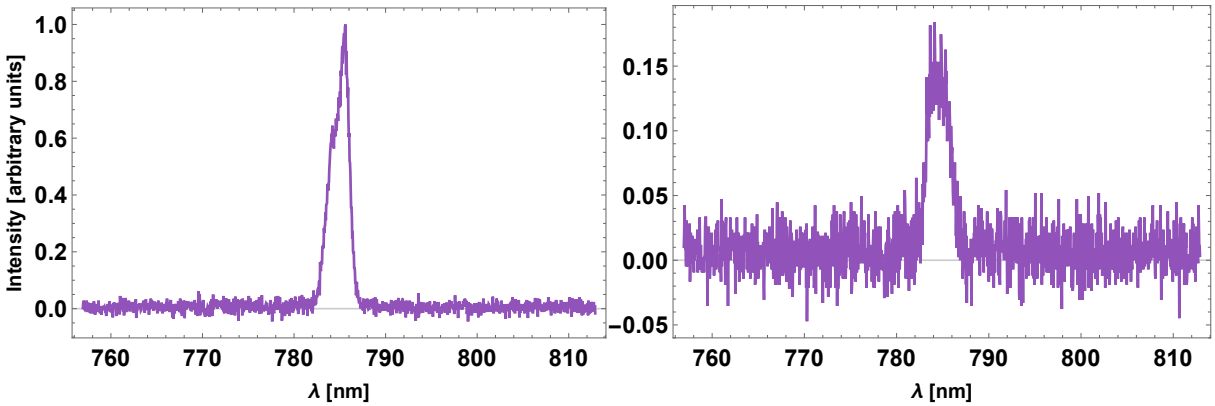
Figure 2.5: Calculated wavelength of the down-converted photons as a function of the crystal temperature. With the input pump wavelength of 404.39 nm, a polling period of $\approx$2.741 μm, and one photon emitted at 785.0(5) nm the other photon will be 834(2) nm and a temperature of 13.7(1) °C.

For quantum communication applications, the source of photons must be narrow band in order to ensure proper transmission and detection [56]. Our source has a narrow bandwidth of sub 1 nm. This is shown in Fig. 2.6 and Fig. 2.7 which meets the criteria outline in Sec. 1.2.2.

Overall, the waveguide crystal's output bandwidth can be reduced with more precise filtering. However, custom filters would be required and prove to be quite costly.

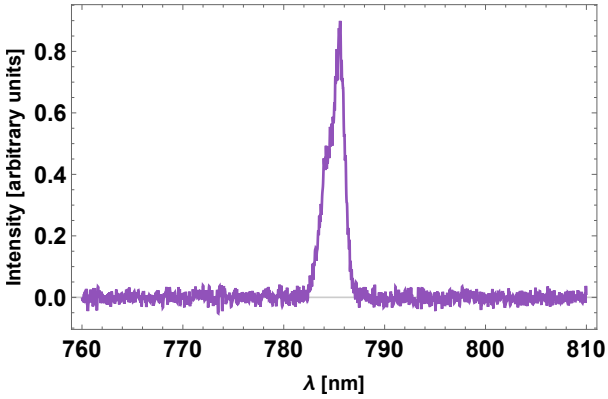
2.2.2 Brightness

Quantum communication applications require a high source brightness and efficiency due to transmission losses that can occur over the communication channel, whether it be free-space or fiber. We calculated the brightness of the source as follows.



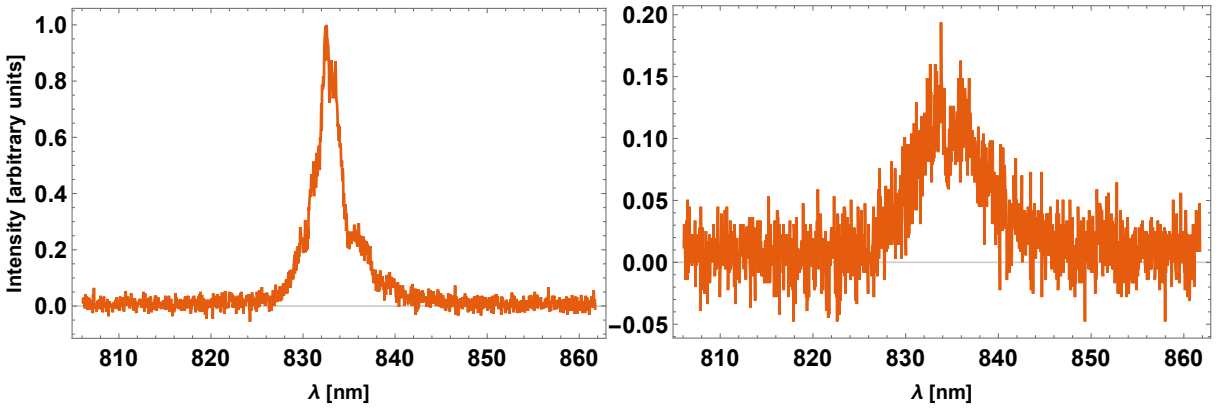
(a) T= 13.7°C

(b) T= 19.3°C



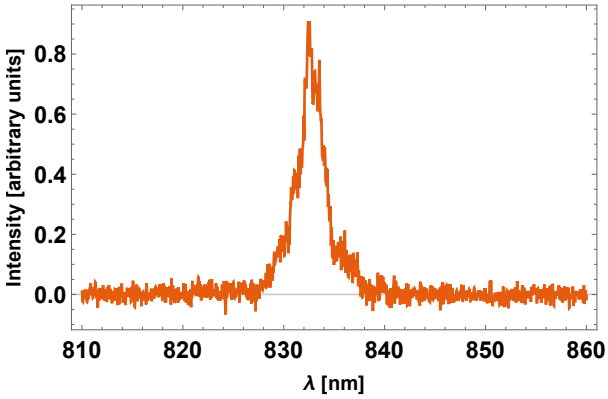
(c)

Figure 2.6: Measured spectrum of the 785 nm photon. This arm of the down-conversion passes through a 785 nm 3 nm bandpass filter. (a) The measured spectrum including the background IR light from the waveguide crystal. (b) The background light created by the crystal when pumped by the laser at an offset temperature. (c) The spectrum with background noise subtracted from spectra (a). The total area under the curve was calculated to be 1.72 for the signal in (c), while the background area from (b) was calculated to be 0.44, giving a signal to noise ratio of 3.90.



(a) T= 13.7°C

(b) T= 19.3°C



(c)

Figure 2.7: Measured spectrum of the 834 nm photon. This arm of the down-conversion passes through a 834 nm 3 nm bandpass filter. (a) The measured spectrum including the background IR light from the crystal. (b) The residual near-IR light generated by the the crystal when pumped by the laser at an offset temperature. (c) The spectrum with background noise subtracted from spectra (a). The total area under the curve was calculated to be 2.82 for the signal in (c), while the background area from (b) was calculated to be 0.84, giving a signal to noise ratio of 3.37.

Table 2.1: Values for singles in both channels as well as coincidences in counts per second (cps). The coincidences detuned field shows the amount of coincidences when the delay between the two channels is set far from the correct value to show the background coincidences. This data is taken at the proper crystal temperature of 13.7 °C. The error values are derived using error propagation of the statistical counting error.

Pump power in fiber [μW]	785 nm singles [cps]	834 nm singles [cps]	Coincidences [cps]	Coincidences detuned [cps]
6.75	175000 ± 418	112000 ± 334	4700 ± 68	61 ± 8
7.75	258000 ± 508	167000 ± 334	6800 ± 82	175 ± 13
9.00	370000 ± 508	240000 ± 408	9400 ± 96	370 ± 19
10.25	408000 ± 639	261000 ± 489	11000 ± 104	450 ± 21
11.50	506000 ± 711	319000 ± 510	13500 ± 116	650 ± 25
12.75	605000 ± 779	384000 ± 564	16400 ± 128	1020 ± 31
14.50	708000 ± 841	456000 ± 619	19000 ± 137	1330 ± 36
16.50	823000 ± 907	527000 ± 675	22500 ± 150	1800 ± 42
18.50	935000 ± 967	609000 ± 725	25800 ± 160	2200 ± 47
19.25	1070000 ± 1034	700000 ± 780	29700 ± 172	3190 ± 56

Table 2.2: Values for singles in both channels as well as coincidences in counts per second (cps). The coincidences detuned field shows the amount of coincidences when the delay between the two channels is set far from the correct value (100 ns detuned) to show the background coincidences. This data is taken at a distant crystal temperature of 19.3(10) °C which will generate photons outside the bounds of our collection optics. Statistical counting error is used to compute the errors.

Pump power in fiber [μW]	785 nm singles [cps]	834 nm singles [cps]	Coincidences [cps]	Coincidences detuned [cps]
6.75	36000 ± 189	34000 ± 184	40 ± 6	10 ± 3
7.75	56000 ± 237	51000 ± 225	60 ± 8	13 ± 4
9.00	80000 ± 282	72000 ± 268	85 ± 9	27 ± 5
10.25	83000 ± 288	75000 ± 273	105 ± 10	39 ± 6
11.50	104000 ± 322	88000 ± 296	127 ± 11	43 ± 7
12.75	129000 ± 359	110000 ± 331	170 ± 13	68 ± 8
14.50	154000 ± 392	130000 ± 360	200 ± 14	80 ± 9
16.50	171000 ± 413	148000 ± 385	245 ± 16	110 ± 10
18.50	189000 ± 433	160000 ± 400	290 ± 17	140 ± 12
19.25	221000 ± 470	190000 ± 436	400 ±20	196 ± 14

The coincidences measured in the system are:

$$C_{\text{SPDC}} = R_s \times \eta_1 \times \eta_2, \tag{2.1}$$

where R_s is the singles rate, η_1 is the efficiency of the 785 nm photon collection and η_2 is the efficiency of the 834 nm photon collection. The singles rate can be calculated as:

$$S_{1,\text{SPDC}} = R_s \times \eta_1, \tag{2.2}$$

and similarly for S_2:

$$S_{2,\text{SPDC}} = R_s \times \eta_2. \tag{2.3}$$

Since singles and coincidences are measured, we can now find the efficiencies as:

$$\eta_1 = \frac{C_{\text{SPDC}}}{S_{2,\text{SPDC}}}, \tag{2.4}$$

and

$$\eta_2 = \frac{C_{\text{SPDC}}}{S_{1,\text{SPDC}}}. \tag{2.5}$$

These efficiencies, however, also include the background light from other sources. The efficiency from just the crystal for the proper SPDC photons can be found by subtracting the background from the temperature detuned trials of Fig. 2.6 and 2.7. Subtracting the background in Eq.(2.4) and Eq. (2.5) we get:

$$\eta_{1,\text{corr}} = \frac{C_{\text{SPDC}}}{S_{2,\text{SPDC}} - S_{2,\text{back}}}, \tag{2.6}$$

and

$$\eta_{2,\text{corr}} = \frac{C_{\text{SPDC}}}{S_{1,\text{SPDC}} - S_{1,\text{back}}}, \tag{2.7}$$

The associated pair production rate can be found by rearranging Eq. (2.2) or (2.3) for R_s:

$$R_s = \frac{S_{1,\text{SPDC}}}{\eta_1}, \tag{2.8}$$

with the similar corrected value of:

$$R_{s,\text{corr}} = \frac{S_{1,\text{SPDC}} - S_{1,\text{back}}}{\eta_{1,\text{corr}}}. \tag{2.9}$$

An equivalent equation can be done with Eq. (2.3). The brightness of the source is calculated by:

$$B_s = \frac{R_{s,\text{corr}}}{P}, \tag{2.10}$$

where P is the input pump power into the waveguide. These values for varying powers can all be seen in Table 2.3.

Table 2.3: Measured efficiencies of the system with η_1 corresponding to the 785 nm photon and η_2 corresponding to the 834 nm photon. The pair production rate is based off the arm with the higher efficiency and the corrected pair rate takes into account the background noise. The η are unitless. The single and coincidence counts corresponding to these calculated values are measurements are found in Tab. 2.1 and Tab. 2.2.The error values are derived using error propagation of the statistical counting error.

Pump Power in fiber [μW]	η_1	η_2	$\eta_{1,\text{corr}}$	$\eta_{2,\text{corr}}$	Pair Production [cps](10^6)	Corrected Pair Production [cps](10^6)	Brightness [counts/s/μW](10^5)
6.75	0.0420 ± 0.0006	0.0269 ± 0.0004	0.0603 ± 0.0009	0.0333 ± 0.0005	4.17 ± 0.10	2.31 ± 0.36	3.42 ± 0.05
7.75	0.0407 ± 0.0005	0.0264 ± 0.0003	0.0586 ± 0.0007	0.0329 ± 0.0004	6.34 ± 0.13	3.45 ± 0.43	4.45 ± 0.06
9.00	0.0392 ± 0.0004	0.0254 ± 0.0003	0.0560 ± 0.0006	0.0315 ± 0.0003	9.45 ± 0.16	5.18 ± 0.56	5.76 ± 0.06
10.25	0.0421 ± 0.0004	0.0270 ± 0.0002	0.0591 ± 0.0005	0.0330 ± 0.0003	9.68 ± 0.16	5.50 ± 0.55	5.36 ± 0.05
11.50	0.0423 ± 0.0004	0.0267 ± 0.0002	0.0584 ± 0.0005	0.0323 ± 0.0003	11.96 ± 0.17	6.88 ± 0.62	5.98 ± 0.05
12.75	0.0427 ± 0.0003	0.0271 ± 0.0002	0.0599 ± 0.0005	0.0331 ± 0.0003	14.17 ± 0.19	7.95 ± 0.64	6.24 ± 0.05
14.50	0.0417 ± 0.0003	0.0268 ± 0.0002	0.0583 ± 0.0004	0.0329 ± 0.0002	16.99 ± 0.21	9.51 ± 0.72	6.56 ± 0.05
16.50	0.0427 ± 0.0003	0.0273 ± 0.0002	0.0594 ± 0.0004	0.0333 ± 0.0002	19.28 ± 0.22	11.0 ± 0.76	6.66 ± 0.05
18.50	0.0424 ± 0.0002	0.0276 ± 0.0002	0.0575 ± 0.0003	0.0333 ± 0.0002	22.07 ± 0.24	13.0 ± 0.84	7.02 ± 0.04
19.25	0.0424 ± 0.0002	0.0278 ± 0.0002	0.0582 ± 0.0003	0.0338 ± 0.0002	25.22 ± 0.25	14.6 ± 0.86	7.57 ± 0.04

From the data in Table 2.3 we have calculated average efficiencies of $\eta_1 = 0.059$ and $\eta_2 = 0.033$ which correspond to 5.9% and 3.3% respectively. With the measured pair production rates, the crystal brightness is measured to be approximately 5.9×10^5 Pairs/s/μW which is an extremely bright value as only microwatts are required produce millions of pairs of photons. Fig. 2.8 and Fig. 2.9 show the efficiencies and pair production rates of the source over varying powers. By comparison, the Sagnac source used for the work done in Chap. 3 required milliwatt power levels to produce a photon pairs on the order of $\approx 10^5$ Hz.

Given the pair production rates and the source brightness for such low pump powers, the PPLN-MgO waveguide source looks very promising for free-space QKD applications. Typical bulk nonlinear crystals require that the pump have an incident power of around 1 mW and do not come close to similar brightness levels for these down conversion wavelengths [62]. Thus the concept of using a waveguide PPLN-MgO doped crystal could meet the brightness requirements of Sec. 1.2.2. However, as will be discussed in the following section, there are some limitations to the quality of the source.

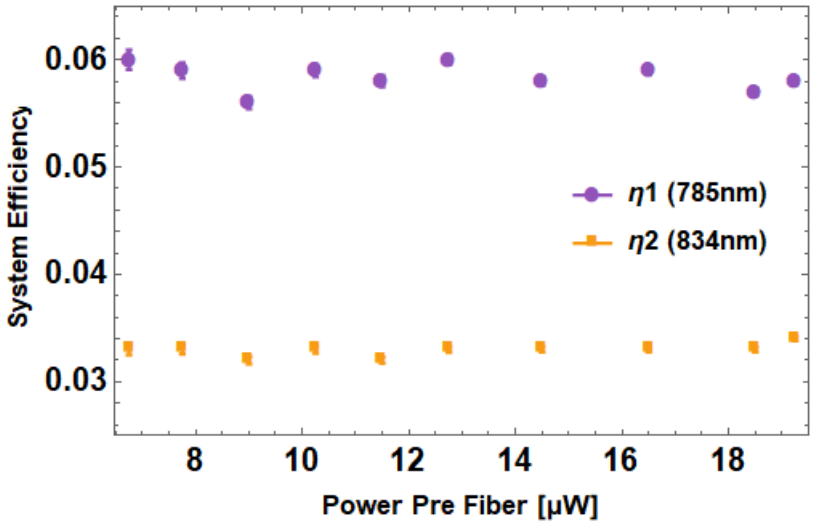
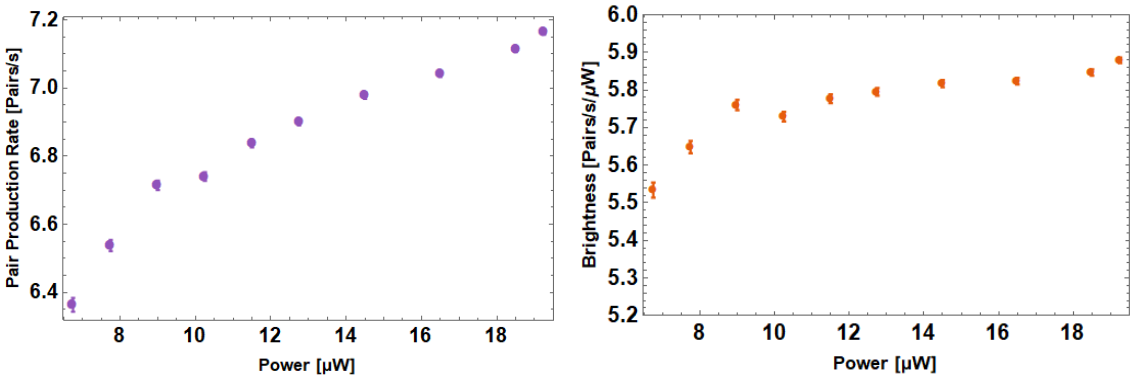


Figure 2.8: Calculated efficiencies, η_m, for varying powers of the source. $m = 1$ corresponds to the 780 nm photons while $m = 2$ corresponds to 834 nm photons. The efficiencies are a unit less quantity. The error bar values are derived using error propagation of the statistical counting error.



(a) (b)

Figure 2.9: (a) Pair production rate for varying powers of pump. As expected, the pair production rate increase with pump power. (b) Source brightness as a function of pump power. The brightness should remain relatively constant over time which is observed here. Both curves are plotted in $\log_{10}$ scale on the y-axis. The error bar values are derived using error propagation of the statistical counting error.

2.3 Difficulties

The following section will outline and discuss the relevant issues that were encountered when attempting to realize the goal of a fiber based Sagnac entangled photon source. It is due to the issues below that this source will not be used for any free space QKD applications. However, the brightness and the information gained from such a project are still valuable and the source could potentially be used in other applications. Though the source appears to have a very high brightness, the quality of the output state is ultimately determined by the signal to noise ratio. In our context, this ratio will be quantified by the ratio of coincidence counts to single counts. For a typical good entangled photon source, one wants this ratio to be above 10% [65], ideally 25% for the uplink QKD case. However, due to various source issues that are intrinsic to waveguide sources and those introduced by the design choice, limited the ability to achieve a good quality source.

2.3.1 Noise in Waveguide

The benefits of using a waveguide for SPDC are presented above in Sec. 2.1. However, one of the drawbacks is the production of noise [66]. The noise produced by waveguide nonlinear crystals are an observed phenomena and seem to be plaguing many users. For further discussion and information on this topic, [66] and [67] have a much more detailed and in depth explanation of the noise observed. However, here I will give a simple explanation. The issue is that the waveguides used for SPDC can be multimode for both the pump wavelength and the down conversion wavelengths. In such a multimode waveguide, the phase matching conditions and energy conversion can be satisfied by several spatial mode bands that can produce signal and idler photons that are not within the frequency or mode structure desired [66]. In addition, these alternate SPDC bands can thus significantly degrade source performance [66].

For examples, lets consider a pump that comes in a $(00)_p$ spatial mode, i.e. the fundamental mode, there are several down conversion modes including:

$$\begin{aligned} &A \quad (00)_p \rightarrow (00)_s + (00)_i, \\ &B \quad (00)_p \rightarrow (01)_s + (01)_i, \text{ and} \\ &C \quad (00)_p \rightarrow (10)_s + (10)_i \ \& \ (02)_s + (02)_i. \end{aligned} \tag{2.11}$$

Here the individual modes are labeled with a pair of integers (kl). We can see in the case of B and C,that higher order modes are produced [67]. These created triplets are still

parity conserving modes and are thus physically allowable. The thing to note is that the wavelengths of the signal and idler in A-C may differ significantly depending on the phase matching conditions of the nonlinear material. Thus without proper filtering, these higher order mode triplets contribute to background noise and can thus reduce the quality of the performance of the source.

In our case, the waveguide is pigtailed with single mode PM780 fibers so any higher order modes will be filtered out. However, the case in which the pump is in a higher order mode within the waveguide such as the $(01)_p$ spatial mode. For parity conservation, there is the possibility to produce a signal or idler photon in the fundamental or (00) spatial mode. For example,

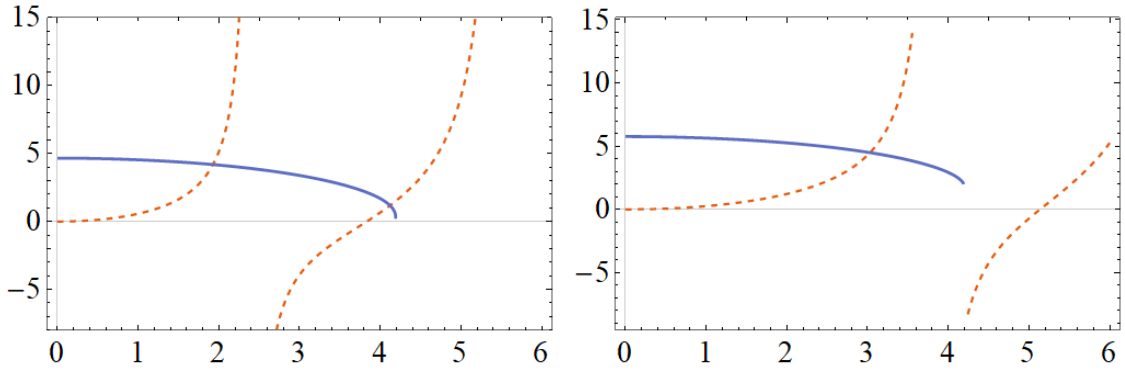
$$\begin{aligned} D \quad & (01)_p \rightarrow (01)_s + (00)_i \;\&\; (00)_s + (01)_i \\ E \quad & (01)_p \rightarrow (01)_s + (02)_i \;\&\; (02)_s + (01)_i \end{aligned} \tag{2.12}$$

which can theoretically produce signal and idler photons of similar wavelength to the fundamental triplet in Eq. (2.11), depending on the phase matching conditions [67]. Therefore, narrow filtering of the signal and idler may not remove these photons and can thus are regarded as noise. This problem is further discussed in Sec. 2.3.2.

2.3.2 Multimode Fibers

Another added issue to the source design is the selection of the fibers used. The pump light of 405 nm is multimode in the PM780 fibers that were selected. If one calculates the V-parameter presented in Eq. (1.54) for the pump wavelength propagating through the PM780 fibers, the result is a V-parameter of 4.190 which is above the single mode limit of 2.405 [17]. Fig. 2.10 shows the results of the solutions to the characteristic equation, Eq. (1.55) This brings forth many issues because any small defect in the fiber will cause mode mixing and thus it is very difficult to maintain fundamental mode propagation of the pump in the fibers as seen in Fig. 2.11. Now if the pump light is multimode when traversing through the fibers and reaches the waveguide in higher order modes other than the fundamental mode, the SPDC photons will be created in these higher order modes as eluded to in Sec. 2.3.1, which do not couple to the single mode output fiber. When only one photon is lost while the other is successful at coupling into the single mode output fiber, such as case of Eq. (2.12), this creates a lot of noise and thus decreases the coincidence to single count ratio. One gets a larger than expected single count rate due to the photons that emerge from the waveguide without their partner. For a typical good

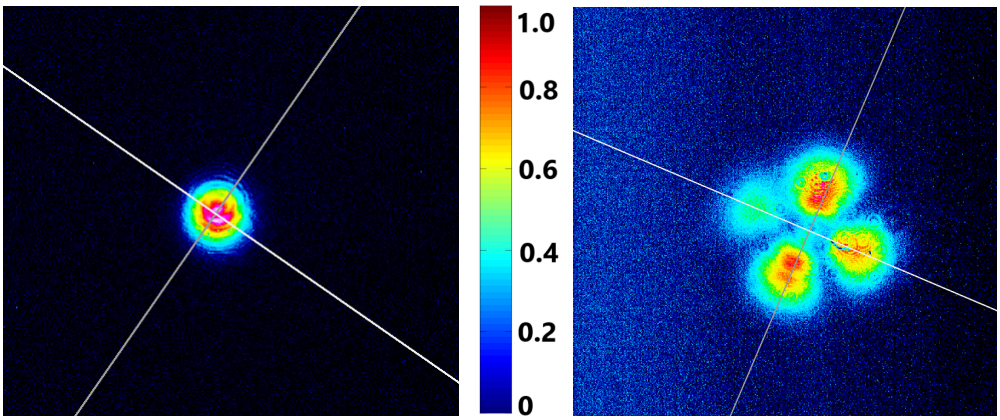
entangled photon source, one wants the coincidence to single count ratio to be above 10% [65], and specifically for this source, we would like about 25% [25]. However, I was only able to achieve consistently 3% coincidence to singles ratio with a maximum attained value of $\approx 6\%$.



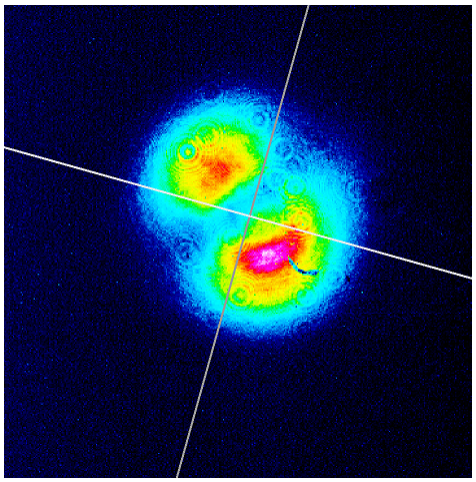
(a) $l = 0$ (b) $l = 1$

Figure 2.10: Solutions to the characteristic equation for the PM780 fiber at the pump wavelength of 405 nm that is pigtailed to the waveguide source. The blue line is the right-hand-side of Eq. (1.55), while the dashed red line is the left-hand-side, with their intercepts being the solutions to Eq. (1.55) . The results clearly show that the fibers are multimode for the pump wavelength. The axes are unitless since, for the y-axis, Bessel functions return unitless quantities and the values of the x-axis is the unitless quantity W presented in Sec. 1.3.2. (a) Shows the case for l=0, we can see that there are solutions for m=1 and m=2. (b) Shows the case for l=1, we can see that there is only the solution for m=1.

The combination of the multimode fibers and the intrinsic noise of a waveguide nonlinear crystal, make for a very difficult task of achieving high $g^{(2)}$ entangled source. Thus, in the following section (Sec. 2.4, I will discuss the attempted solutions that try to optimize the fundamental mode propagation of the 405 nm pump through the PM780 fibers, which should reduce the noise and thus increase the coincidence to singles ratio.



(a) LP_{01} (b) LP_{21}



(c) LP_{11}

Figure 2.11: Intensity plot of the modal structure for the pump wavelength of 405 nm (a) pump output Gaussian structure, (b) and (c) output mode structure from the PM780 fiber that is pigtailed to the waveguide source. The results clearly show that the fibers are multimode for the pump wavelength.

2.4 Attempted Solutions to Issues

Several attempts at resolving the issues of the waveguide source stemmed from prior experimental experience and advice of others, as well as a literature search conducted by the author. The obvious issue was to some induce only the fundamental mode to propagate through the fibers. This was investigated by several means and a beam pickoff was made such that I could investigate the various techniques against another PM780 fiber, see Fig. 2.12

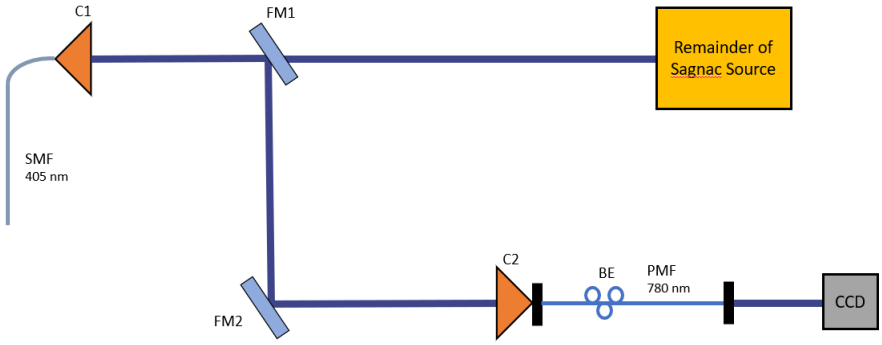


Figure 2.12: Pick off of the pump beam that enabled the analysis of various solutions. SMF- Single mode fiber, PMF- polarization maintaining fiber, C1-C2- Thorlabs Nanomax 6-axis coupling stages, BE- Bat ears, FM1-FM2- flip mirrors, CCD- charge coupled device (camera).

2.4.1 Lens System

The first and most obvious solution would be to attempt to excite only the fundamental propagation mode of the multimode fiber. This can be done by selecting the correct lens system to achieve the appropriate magnification such that the spot size of the incident beam is equal to that of the NA of the fundamental mode. One can calculate the appropriate size that the incident spot size should be given the core diameter and numerical aperture of the fiber [68]. The equation used to calculate the power coupling coefficient (η_{lm}) of the various modes is given by,

$$\eta_{lm} = \frac{\left| \int_0^{\infty} dr \int_0^{2\pi} d\phi \, \mathcal{L}_{m-1}^{l}(Vr^2)\, e^{-\left(\frac{r^2}{2\left(\frac{1}{\Omega^2}+V\right)}\right)} r^{l+1} \right|^2}{\int_0^{\infty} r dr \int_0^{2\pi} d\phi \left| e^{-\left(\frac{r^2}{2\Omega^2}\right)} \right|^2 \int_0^{\infty} dr \int_0^{2\pi} d\phi \, r^{2l+1} \left| \cos\left(\frac{l}{\phi}\right) \mathcal{L}_{m-1}^{l}(Vr^2)\, e^{-0.5r^2V} \right|^2} \tag{2.13}$$

where V is the V-parameter of the fiber, Ω is the ratio of the spot size to the core diameter, $l = 0, 1, 2, ...$ is the azimuth mode number, $m = 1, 2, 3, ...$ is the radial mode number and $\mathcal{L}_n^a(x)$ is the generalized Laguerre polynomial. The results obtained for the PM780 fiber is in Fig. 2.13. The results indicate that a spot size that is roughly half the core diameter should excite only the fundamental mode, assuming normal incidence. For the setup in Fig. 2.1, this meant an overall magnification of ≈ 0.7. A telescope system was set up to achieve such a magnification and this was investigated using the pick off mentioned above in Fig. 2.12, however no positive results were found as the output mode of the fiber can be seen in Fig. 2.14.

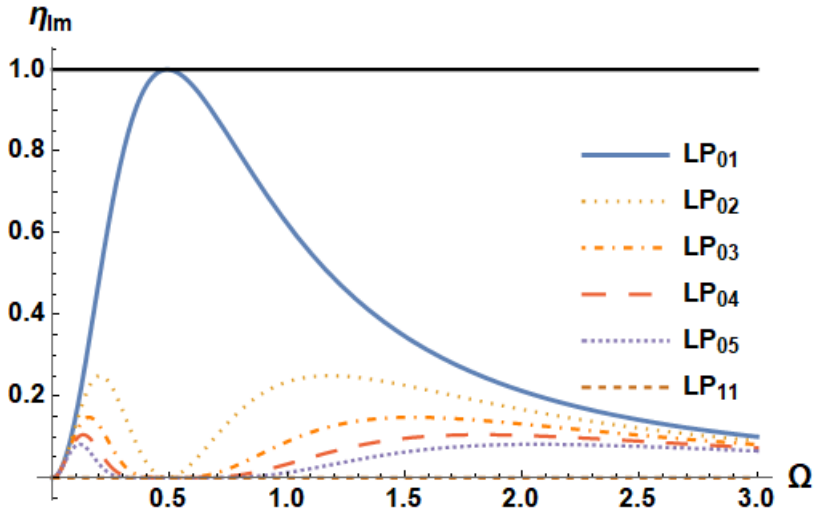


Figure 2.13: Power Coupling Coefficients of LP_{lm} modes versus normalized incident spot size, η_{lm} is the uniteless power coupling coefficient, Ω is the normalized spot size (uniteless), normalized to the core diameter. Calculated using Eq. (2.13).

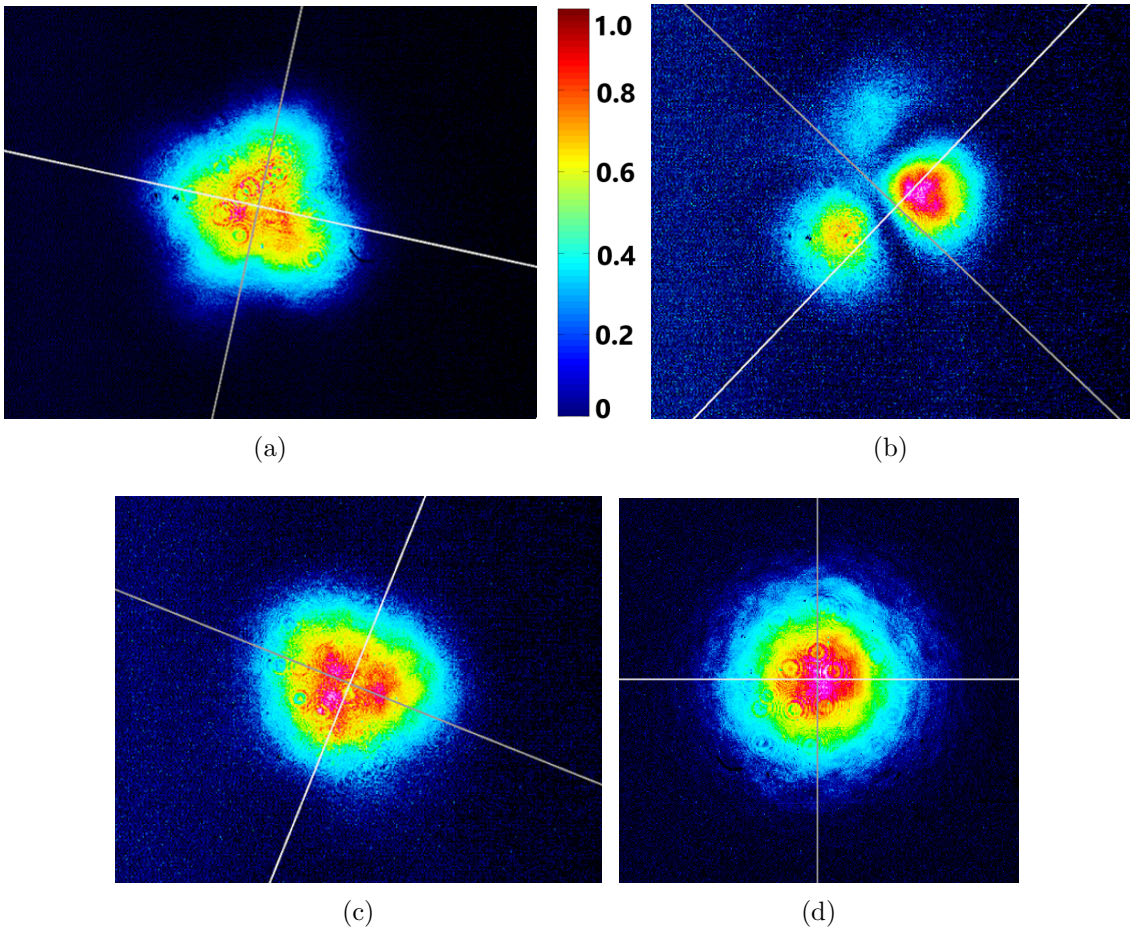


Figure 2.14: Output mode for 0.7 magnification telescope system, (a)-(c) show the output of the 405 nm pump light after passing through the PM780 fiber. The various modes were obtained by adjusting the coupling. (d) A Gaussian mode as reference for the reader

Given that the calculations done following [68] did not lead to any sufficiently positive result. A characterization effort was undertaken with to try and find the best combination of lenses that would give the best coincidence to singles ratio with the results shown in Fig. 2.15.

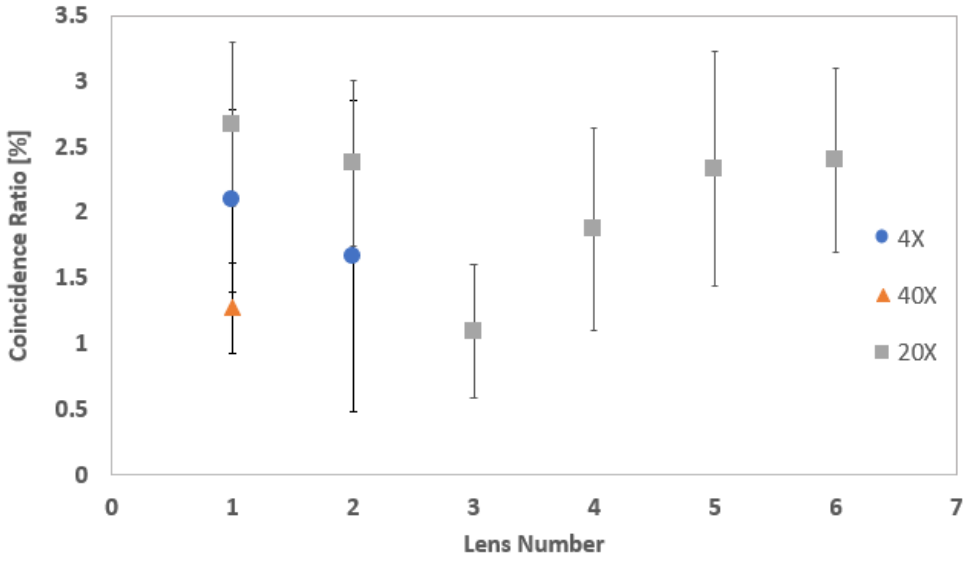


Figure 2.15: Coincidence counts versus focusing lens focal length, see Tab. 2.4. The collimating lens focal length is specified in the plot legend. The fibers were attached to bat ears whose positions were optimized as explained in Sec. 2.4.2. The error bar values are derived using error propagation of the statistical counting error.

Table 2.4: Information about lenses used for the measurements in Fig. 2.15.

Magnification	Effective Focal Length [mm]	NA	Manufacturer
4	45.00	0.10	Olympus
10	17.09	0.25	Edmund
10	18.00	0.25	Olympus
16	11.00	0.30	Newport
20	9.00	0.40	Olympus
40	4.50	0.65	Olympus

In Fig. 2.15 we see that none of the lens combinations performed well, i.e. coincidence to single ratio $\approx 3\%$. However, this can be due to a number of factors such as fiber alignment and orientation. Nonetheless, the lens that did perform the best was investigated further with other collimating lens but to no positive result. Many hours were dedicated to increasing the coincidence counts to single counts ratio, however, there was no increase

in the ratio beyond 3%, thus further methods to induce fundamental mode propagation were investigated.

2.4.2 Bat Ears

Another method that was sought to combat the multimode nature of the fibers is to use what are known as bat ears. Bat ears are a laboratory tool that is typically used to apply a controlled stress to an optical fiber. They are normally used to cause the unitary birefringent induced polarization rotation of single mode fibers to be identity. A picture of commonly used bat ears can be found in Fig. 2.16. The idea is that the bat ears will be able to adjust the fiber shapes and stress such that the mode mixing is optimized for SPDC generation. The position of the bat ears is essentially unpredictable as it is difficult to define how the bat ears will effect the individual count rates. However, there is a considerable effect and the bat ears position can alter the coincidence to singles ratio. Fig. 2.17 shows the results of the various positions that the bat ears were placed and counts were recorded for. It is apparent that there is an increase in the coincidence to singles ratio. However, there is not a significant increase that will make this solution viable.

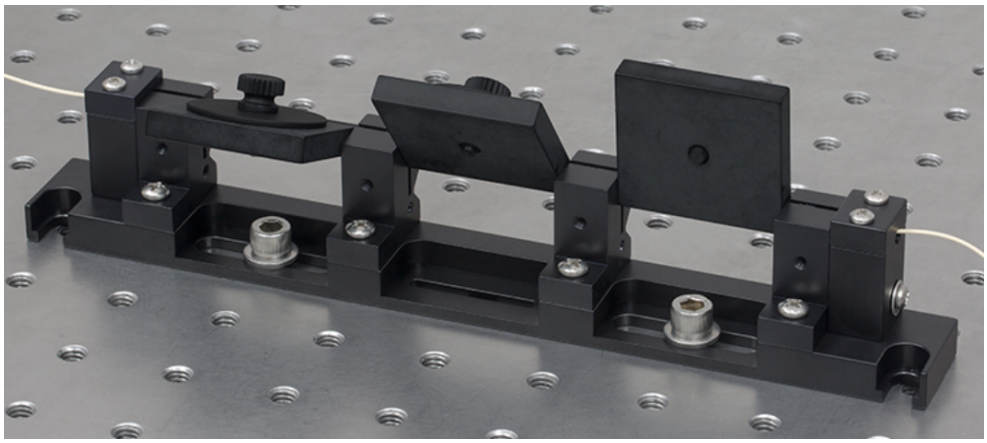


Figure 2.16: A laboratory tool commonly known as bat ears used to apply a controlled stress to a fiber, usually to manipulate the birefringence induced polarization rotations caused by single mode fibers. Picture taken from [69]

2.4.3 Curve Fiber

Another technique that was used and is based on inducing power loss by bending the fiber [70]. This is similar in theory to what the bat ears do, however, rather than trying

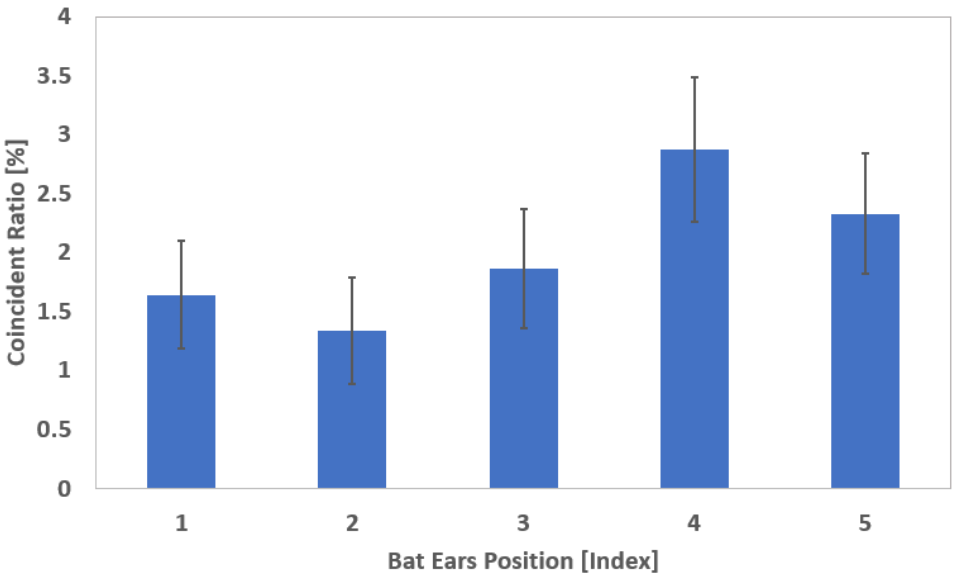


Figure 2.17: Coincidence counts as a function of various Bat Ear positions. The numbering of positions are simply numbered in the order that they were taken. The error bar values are derived using error propagation of the statistical counting error.

to change the input pump mode, we are inducing power loss to the higher order modes. The basic premise is that the curving of the fiber induces loss for the various modes of a multimode fiber. The theoretical loss induced to the power of the higher order modes is larger in magnitude than that of the fundamental mode as seen in Fig. 2.18 with the experimental result in Fig. 2.20. The modal used to calculate the curves in Fig. 2.20 is done using a large bend radius $R \gg a$ where a is the core radius. The power loss of a mode ν is given by the following equation:

$$2\alpha = \frac{\sqrt{\pi}\kappa^2 \exp[-\frac{2}{3}(\gamma^3/\beta_g^2)R]}{e_\nu \gamma^{3/2} V^2 \sqrt{R} K_{\nu-1}(\gamma a) K_{\nu+1}(\gamma a)}$$
$$e_\nu = \begin{cases} 2, \nu = 0 \\ 1, \nu \neq 0 \end{cases} \tag{2.14}$$

where κ is the first zero of the special Bessel function $K_n(x)$, γ and β_g are constants derived from the dispersion relation of the light propagating through the fiber and V is the V-parameter of the fiber [70]. The results of using this formula for the given fibers and pump wavelength are shown in Fig. 2.18. The experimental values are obtained by removing the fiber from the bat ears in Fig. 2.1 and wrapping the fiber around posts of

decreasing diameter as seem in Fig. 2.19. The results from this are shown in Fig. 2.20. Again, there is no significant increase in the coincidence to singles ratio from what was a achieved with only manipulating the Nanomax™ that would confirm that this method is effective for the length of fibers we have chosen. The trend in Fig. 2.20 also does not seem to follow what should be expected from simulation as it should be noted that the derivation of Eq. (2.14) is done with some assumptions such as a large bend radius, amongst other [70].

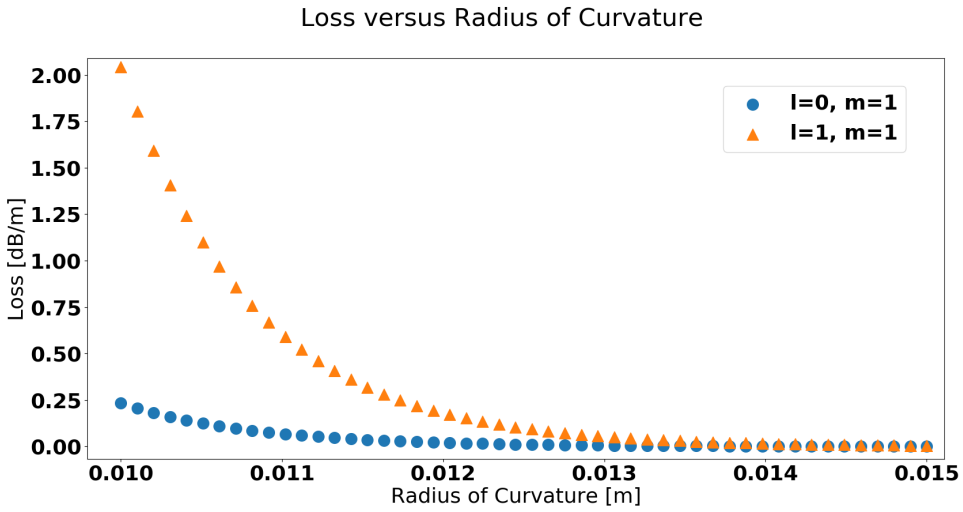
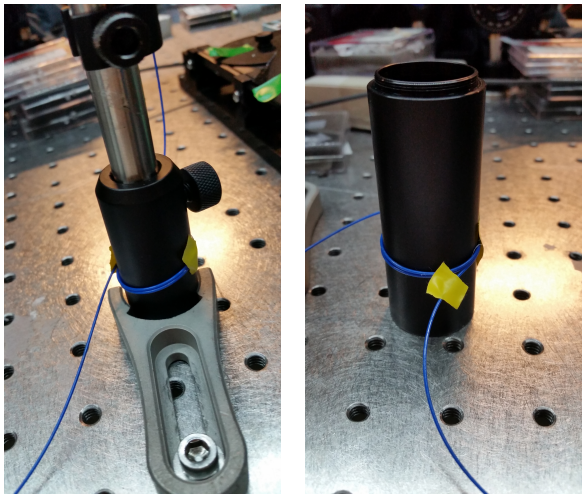


Figure 2.18: Simulation of the loss induced to the fundamental LP_{01} mode or $\nu = 0$ and the LP_{11} or $\nu = 1$ via a curved fiber. It is clear that the higher order modes experience much higher power loss at shorter bend radii.



(a) (b)

Figure 2.19: Coiled fibers wrapped around differing tube sizes to allow for accurate diameter of curvature measurements. (a)3 cm (b)3.2 cm

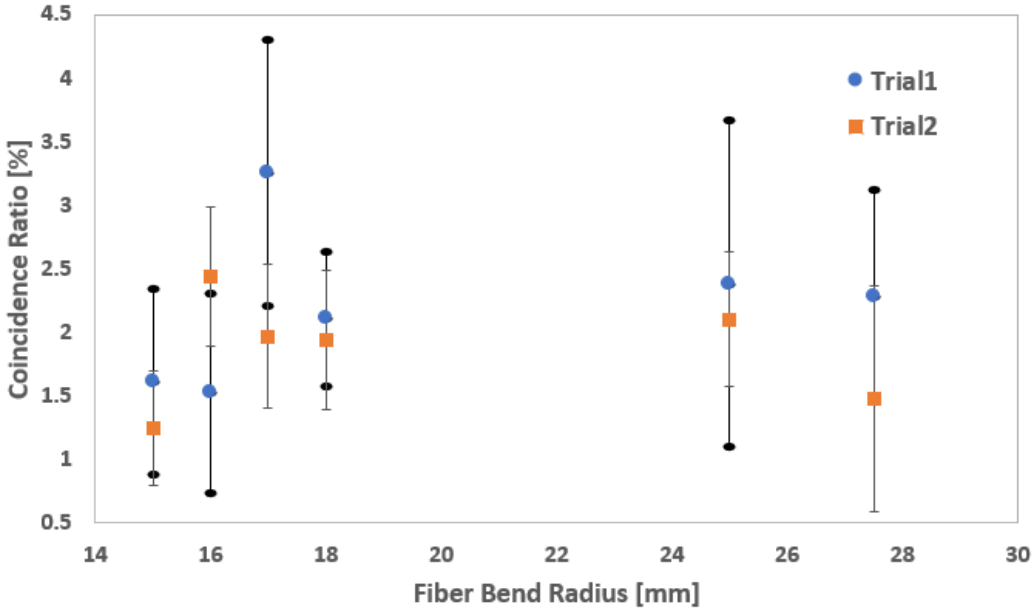


Figure 2.20: Coincidence counts as a function of various fiber curvature radii. The smallest fiber bend radius was chosen to be sufficiently large above the stress limit of the fiber (12 mm). This measurement was repeated twice to show that there is no reproducibility in the results. This is to be expected as we are well above the threshold where curvature loss begins to take effect, as per Fig. 2.18. The error bar values are derived using error propagation of the statistical counting error.

2.5 Conclusions and Future Suggestions

After the rigorous characterization and testing, it is apparent that this pigtailed configuration of PPLN waveguide crystals will not meet the requirements of Sec. 1.2.2, due to the low signal to noise ratio, with no clear solution to resolve this issue. However, since there is still the need for a high rate entangled photon source, the author has compiled some suggestions for future investigations of PPLN waveguide sources that could meet the requirements of Sec. 1.2.2.

The first suggestion would be to use the exact configuration of [63], where they did not pigtail the fibers but rather have the fiber alignment to the waveguide be a degree of freedom. This allows for the selection of the proper pump mode that enters the waveguide and thus can ignore the multimode nature of the fibers for the pump wavelengths.

Another suggestion would be to use a free space coupled waveguide and not use the fiber based technique. The advantages of this is that one can guarantee the mode structure of the pump light. The disadvantages are that the alignment is tedious and thus making the source not easily mobile. There is also the added issue that though the waveguide has a very high brightness that can be utilized, there is still the inherent scattering background of PPLN waveguides. Given the above, a bare waveguide might not be the best solution that mets the criteria of Sec. 1.2.2.

One of the most probable solutions for resolving the multimode pump, is to cut or shorten the fibers that are pig-tailing the waveguide. The reason for this suggestion is that there is a substantial amount of literature on fundamental mode propagation in short multi-mode fibers of fiber cores on the order of 100 μm and lengths on the order of a few centimeters [71]. The advantage of using the short fibers is that it allows the user to have the ability to keep the fiber as straight as possible, which is a common theme in [71]. Using the simple setup of Fig. 2.21, I was able to manipulate the output mode of the pump wavelength through a short PM780 fiber. The output mode of the pump was easily adjusted by small detuning of the input or output coupler, the mode are seen in Fig. 2.22. There is some promise that the use of short fibers is effective, however it requires some future investigation.

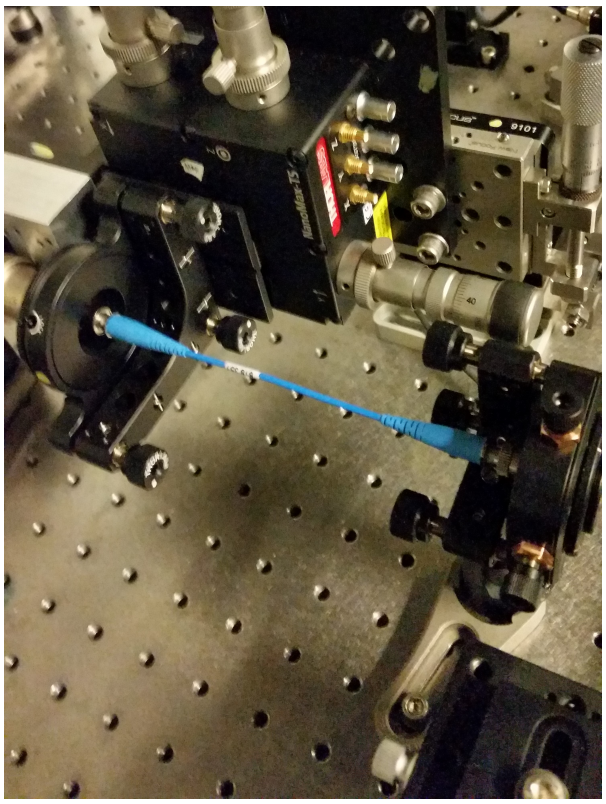
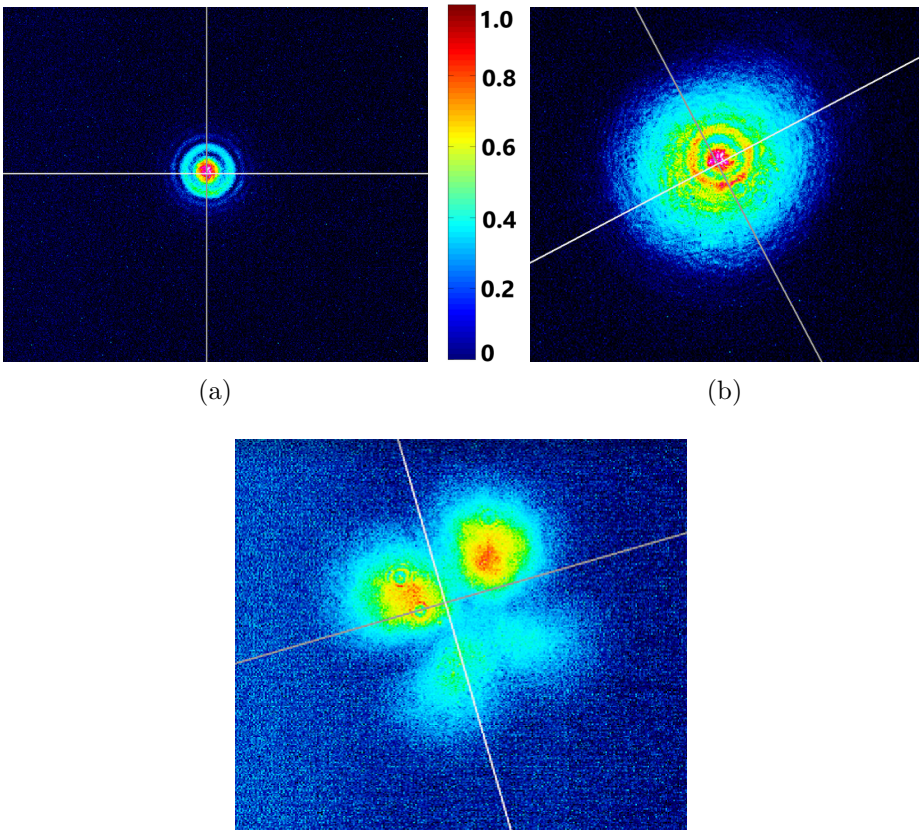


Figure 2.21: A 17 cm 780PM fiber is investigated for the mode selection of 405 nm laser light. The mode is easily selected via changing the coupling at the input. The mode can also be adjusted by bending the fiber by adjusting the tilt of the output coupler.



(a) (b)

(c)

Figure 2.22: Spots that are produced with the 17 cm 780PM fiber that was mounted to be as straight as possible. (a) The input and output couplers are adjusted such that the fiber is as straight as possible. (b) The focus and tilt of the input and output couplers are adjusted such as to create a Gaussian output mode with the highest output power. (c) Higher order output mode induced by adjusting the output and input coupler

Chapter 3

Reference Frame Independent Protocol with PM fibers

In most QKD protocols, both Alice and Bob need to agree on fixed measurement bases as this is essential for key generation. However, in reference frame independent protocols (RFI), only the computational bases, the bases from which a key will be extracted, is fixed, while the other two are free to rotate by some rotational phase ϕ. RFI protocols are useful in many settings such as free-space satellite links and time-bin encoded QKD. As further explain in Sec. 1.1.2.

3.1 Concept

RFI protocols are of great interest to the QEYSSat mission as it will enable the transmitter to reduce the number of moving parts and adaptive optics that have been historically used to compensate the birefringent polarization changes caused by the single mode fibers (SMF) that link the quantum source to the transmitting telescope.

The birefringence results from manufacturing defects and small amounts of stress in the core of the fiber that can alter the relative index of refraction of the different polarization modes. Even the smallest defect in the fiber can cause a large amount of power mixing of the polarizations [40]. Therefore, there is a need for compensation systems that can correct for any shift in polarization. In the laboratory setting, most systems can be fixed by the simple addition of a half-wave plate or bat ears to recover the initial polarization state. This however, requires that the fiber be fixed and at a stable temperature. For other practical applications, such as the transmitting telescope for an up-link QKD system,

simple bat ears and wave plates will not suffice and adaptive compensation systems are needed. Historically for the QEYSSat specific system, this involved moving parts and a complex active feedback system [38].

One solution requires only polarization maintaining fibers (PMF) to combat the birefringence induced changes by the SMF. The PMF has two axes that will preserve any polarization that is aligned to these axes (Sec. 1.3.3) [59]. They are know as the slow and fast axis. Unfortunately, these two axes, due to differences in their respective refractive indexes, create a phase difference between the two polarizations:

$$\phi = \frac{2\pi(n_s - n_f)L}{\lambda} \tag{3.1}$$

where n_s and n_f are the indexes of refraction for the slow and fast axes respective. It is this phase difference that causes the rotation of any polarization that is not aligned to the axes of the PMF. ϕ is also subject to bends in the fiber, temperature of the fiber, basically any stress on the PMF will cause this phase to change and thus is difficult to accurately measure for Alice and Bob. Now if we send both qubits of a Bell State each through a PMF. The resulting state will be, for example:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + e^{-i\phi}|1\rangle_A|0\rangle_B) \tag{3.2}$$

where ϕ is from (3.1), the subscripts A and B refer to the qubits of Alice and Bob respectively. It is this entangled state that is used in the demonstration of the 3-2 basis RFI protocol. However, it should be noted that I did not do a complete QKD since we were disclosing the measurement results between Alice and Bob. Complete QKD would only share the measurement basis and the timetags of the photons detected. From the shared measurement basis and timetags, Alice and Bob can use the entanglement to solidify the expected bit results that they have between them and transfer a secure key.

3.1.1 Transmission of Entangled Photons in PM fibers

In addition to a relative phase difference between the slow and fast axis, polarization maintaining fibers also introduce a walk-off between the modes of the two axes, shown in Fig. 3.1. Now the walk-off induced by a polarization maintaining fiber is given by:

$$\tau_p = \frac{\mathrm{B}}{c} \tag{3.3}$$

Figure 3.1: Walk-off induced by the polarization maintaining fiber. In this figure the two PM fibers are 90° relative to each other such that the polarizations traveling along each axis is different in each fiber. τ_c is the coherence time and τ_p is the fiber induced walk-off. The length and walk-off induced by each fiber needs to be similar to preserve the indistinguishably of the photons.

where c is the speed of light in vacuum and B is the fiber birefringence [59]. τ_p is in units of s/m. Now if this walk-off is greater than the coherence time of the photons traveling through the fiber, the photons will lose interference visibility. More importantly for this work, the entanglement will no longer be capable of being observed until the walk-off is undone [72].

Now the coherence time of a photon is calculated by dividing the coherence length by the phase velocity of the photon:

$$\tau_c \approx \frac{\lambda^2}{c\,\lambda} \tag{3.4}$$

where c is the speed of light in vacuum, $\Delta\lambda$ is the bandwidth and λ is the wavelength of the light [17]. Now calculating this value for a single photon source that has a emission spectrum centered at 800 nm with a 3 nm bandwidth, which is similar to the characteristics of the SPDC photons that are used in this experiment, the coherence time is $\tau_c \approx 0.71$ ps. Calculating the walk-off due to a induced by the 2 m polarization maintaining fibers used (Thorlabs PMF780) which have a birefringence of 3.5×10^{-4}, via Eq. (3.3) gives $\tau_p L = 2.34$ ps. Now comparing this to the coherence time of a 800 nm $\pm$ 3 nm photon, we see that the walk-off is greater than the coherence time which causes a drop in interference visibility and should cause the entanglement to no longer be observable if measured [72]. In fact, if one were to send single photons that have a large bandwidth across a single PM fiber, the walk-off would destroy the coherence of the photons. This particularly effects the polarizations that are not aligned to either the slow or fast axis. The component along the slow axis will end up temporally displaced from that along the fast axis which, if displaced greater than the coherence time of the photon, will destroy the polarization state.

However, contrary to a simple single photon source, entanglement is much more resistant to the displacement since the coherence time of entangled photons is dictated by the coherence time of the pump [73–75]. For this experiment the pump is centered at 404 nm with a bandwidth of 0.005 nm. The pumps coherence time is $\tau_c \approx 1.08$ ns which is much greater than the walk-off induced by the fibers. Given these calculated values, the entangled photons should be capable of withstanding the walk-off, provided that the walk-off is equal and symmetric in both arms of the entangled source to allow the photons to remain indistinguishable [72]. The results in Sec. 3.4 indicate that not only is the entanglement still observed, but a very high purity is maintained, something that is not typically known for high birefringent fibers such as PM fibers.

In addition to the work presented in the chapter, which is done using one PM fiber for each arm of the entangled photon source, see Fig. 3.2, we also tested the feasibility of using two PM fibers in each arm. The idea behind this is that the second fiber is to be rotated such the photons that propagated along slow axis in the first fiber, then propagate along the fast axis of the second fiber and vice-versa. If the fiber lengths are selected correctly, then the walk-off induced by the first fiber can effectively be canceled by the second fiber, which would reduce the need for a long photon coherence. This two fiber concept works because the walk-off is effectively a local unitary effect that can be undone. The two fiber concept was investigated using one arm of an entangled photon source as a single photon source with a large bandwidth. The results were quite promising since we achieved a visibility of 93% compared to 50% with only on PM fiber.

3.1.2 3-2 Basis Protocol

One key element to understand in this particular experiment is the protocol. I will start by identifying that the measurements made in the 3-2 basis protocol are not tomographically complete. However, they are capable of executing the protocol and are in fact the minimum amount of bases needed to compensate for the rotations induced by the PM fiber.

The basics of the protocol are very similar to the RFI protocol described in Sec. 1.1.2. The only differences are that Bob only has two measurement bases rather than three. The advantages of having two bases at Bob instead of three is that it reduces the complexity of Bob, which in this case would be a satellite. The reduced complexity is an added benefit to any project that requires substantial amount of resources to implement. Thus, reducing the complexity of the receiver reduces the amount of optics and detectors that would be rendered unnecessary in the end. The loss of the third basis in Bob does not have any real changes to the protocol presented in Sec. 1.1.2. However, the computational basis is

changed to the basis that is aligned to the axes of the PM fiber, in this case the H/V or Z basis. Due to the lack of basis in Bob's state analyzer, the C-parameter is reduced from Eq. (1.13) to only have two terms instead of four.

$$C = \sqrt{\langle X_A X_B \rangle^2 + \langle Y_A X_B \rangle^2} \tag{3.5}$$

It can be seen in Eq. (3.5), that any decrement in the expectation value of the correlation between X_A and X_B will be compensated exactly by an increment in the Y_A and X_B correlation. The compensation is further presented in Appendix B. It is also shown in Appendix B that Eq. (3.5) is still bounded by 1 and anything other than the perfect value of 1 indicates a loss in entanglement or purity of the state.

3.2 Experiment

Prior to discussing any results, I will discuss the experimental setup. Fig. 3.2 shows the general schematic of the experimental setup. Each component is explained in more details below. Most of the setup was made be Dr. Jeongwan Jin, however, the alignment techniques, fine tuning of the source and minor adjustments to the setup were done by the author after Dr. Jin's departure.

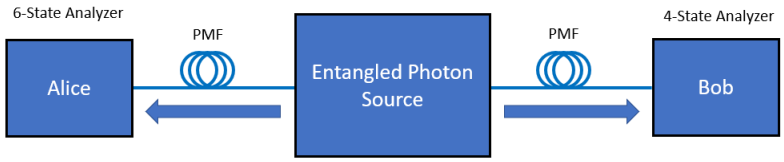


Figure 3.2: The RFI setup that includes a Sagnac interferometer as the entangled photon source and Alice has a 6-state analyzer while Bob has a 4-state analyzer. The photons are transmitted to the state analyzers via a polarization maintaining fiber (PMF).

3.2.1 Entangled Photon source

The experimental setup is shown in the Fig. 3.3. The entangled photon source used is well know Sagnac interferometer [76]. A periodically poled potassium titanyl phosphate ($KTiOPO_4$) nonlinear bulk crystal is bi-directionally pumped with a blue mode 405nm and each direction of the pump photons produces SPDC photon pairs as described in Sec. 1.2.

This particular crystal is a type-II crystal which means that the photon pairs produce are anti-correlated. Thus overall producing the bell state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \tag{3.6}$$

where the $\pm$ depends on the pump's phase. For this particular protocol the pumps phase is not important and can be ignored. The temperature of the crystal is tuned such that the down-conversion photons are at wavelengths of 776nm and 842nm. The alignment of the source is done by using the *Hiking Boot* and *Stiletto* methods that are outline in [65].

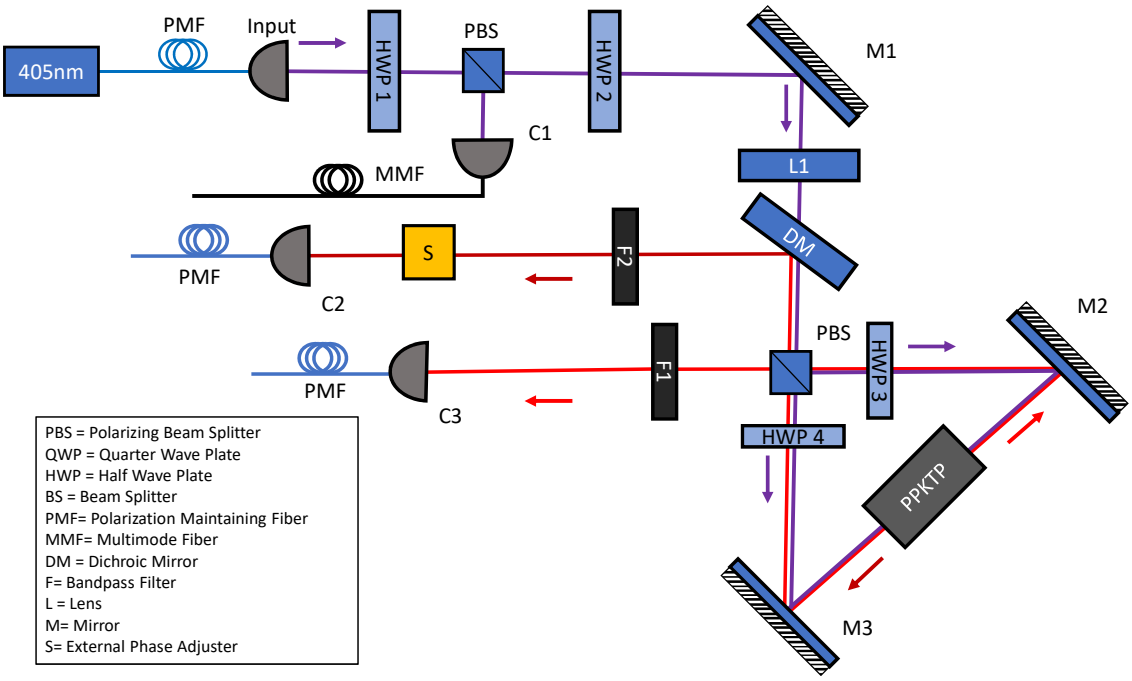


Figure 3.3: Optical components of the Sagnac Interferometer, HWP3, and HWP4 are to align the pump polarization to the appropriate crystal polarization that will maximize the nonlinear SPDC interaction. S is the external source that will enable the phase to be adjusted at a faster rate than produced by the fibers alone.

The down conversion photons are sent to both polarization state analyzers through

polarization maintaining fibers (PM780) of 2 m in length. It is these fibers that induce a relative phase between the slow and fast axis as explained in Sec. 1.3.3. The fibers need to be of the same length in order to preserve the entanglement. In fact, if the length difference causes a phase difference that is longer than the pump's coherence time, then the entanglement is lost [72]. Thus, ultimately, it is sufficient to have fibers that are similar in length such that the difference in the walk-off is smaller then that of the pump's coherence time.

3.2.2 Measurements

The measurements were done using two separate state analyzers that correspond each to either Alice or Bob. Alice's state analyzer is shown in the Fig. 3.4 and is capable of measuring six polarization states in three separate bases (H/V, D/A, R/L). In contrast, Bob has a 4-state analyzer as seen in Fig. 3.5 which can measure only 4 separate polarizations (H/V, D/A). Each analyzer needed to be adjusted such that the birefringent phase induced by the optics is nulled within the analyzer. This allows for higher visibility/contrast in the D/A and R/L basis.

To null the phase induced by the optical elements of the analyzer, one must use a birefringent element (such as a HWP or QWP) and rotate it about its vertical axis, (i.e. about the post that normally holds optics to an optical table). One rotates the birefringent element until the phase is nulled or when it is minimized, further explained below:

1. Select a birefringent element (HWP or QWP) with a known slow and fast axis angle setting.
2. Place a polarizer at the input of the analyzer such that the polarization that propagates through the analyzer is known.
3. Set the polarizer to a known polarization, such as horizontal or diagonal.
4. Observe the count rate or power output at the various detector ports.
5. If the contrast value does not make sense for the given polarization, place the birefringent element in the signal path (aligned to either the slow or fast axis) and rotate the birefringent element until it does.
6. Do this for every detection basis, for every input polarization, and for both the slow and fast axis of the birefringent element until the contrast is optimized.

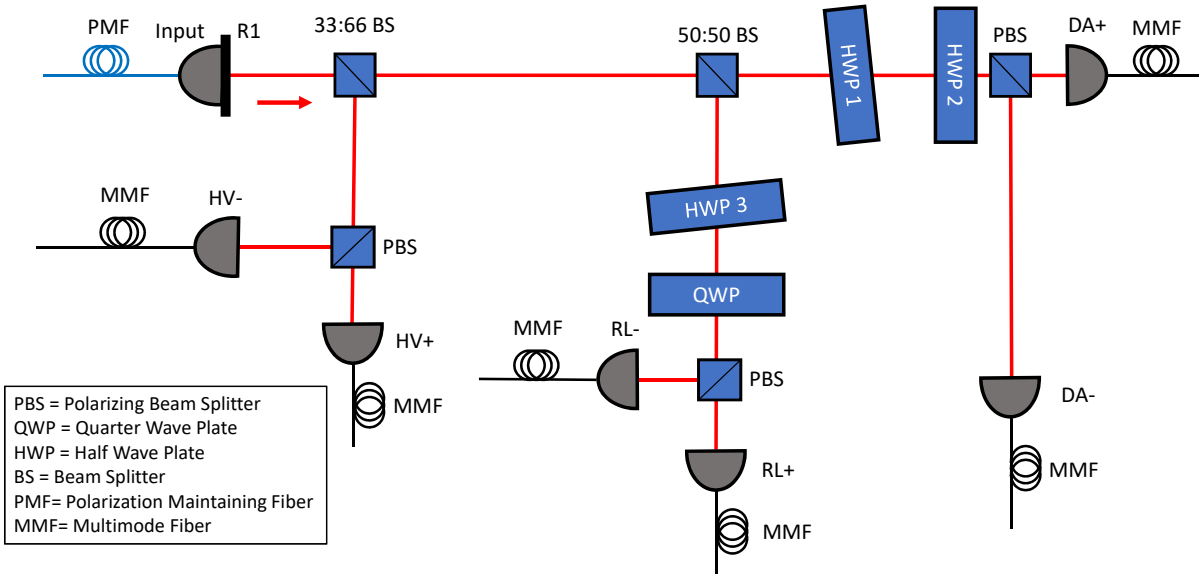


Figure 3.4: Optical components of the 6-state analyzer (Alice)

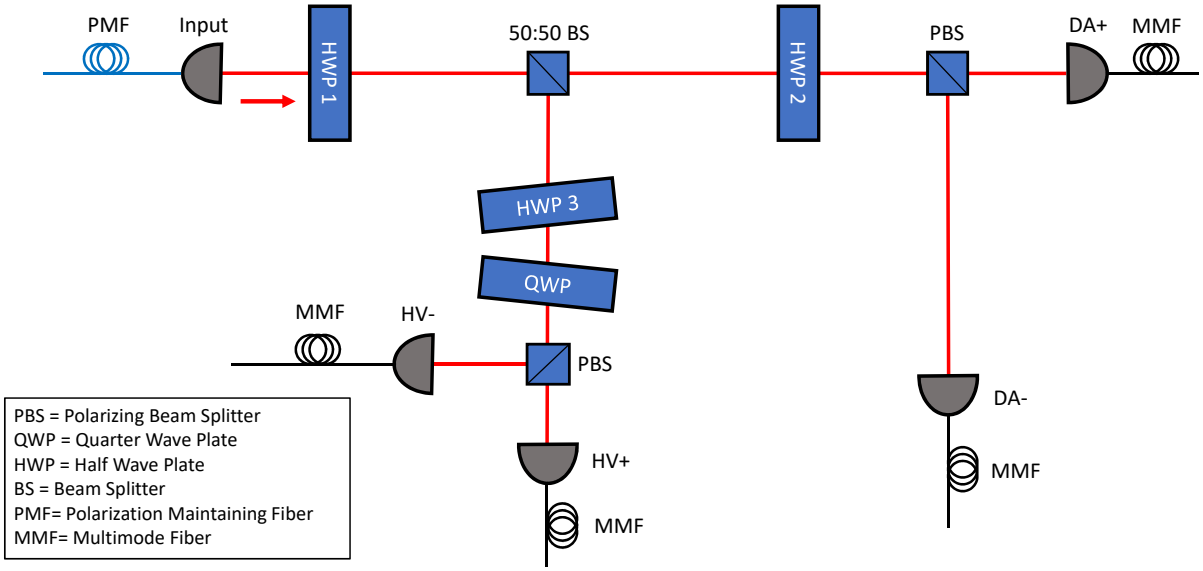


Figure 3.5: Optical components of the 4-state analyzer (Bob)

7. Once optimized, secure the birefringent element in place.

8. If no optimal rotational position can be achieved for a measurement path, a halfway point is chosen.

As an example, the 6-state analyzer D/A basis measurement, if there is no relative phase introduced by the analyzer, there should be a large contrast when the polarizer is set to the diagonal polarization. Basically the anti-diagonal detector should effectively be reporting background counts. If not, following the steps above, a HWP or QWP would be placed in the D/A path, similar to the location in Fig. 3.4 and rotated until the diagonal counts are optimized and the anti-diagonal counts are minimized. Then one would do the same procedure but setting the polarizer to send anti-diagonal, maximizing the anti-diagonal counts and minimizing the diagonal counts. If the two polarizations cause differing rotation positions of the birefringent element, a halfway point is chosen.

To detect the photons, ten avalanche photo diodes with time tagging units record the time of arrivals of the photons in both state analyzers. These time tags are then compared for correlations between Alice and Bob's detections. There are twenty four total correlations that can be measured for coincidence counts. From these measurements, I can perform state tomography of the entangled source, calculate the expectation values in each measurement bases, measure the phase ϕ in (3.2) and extract a key rate.

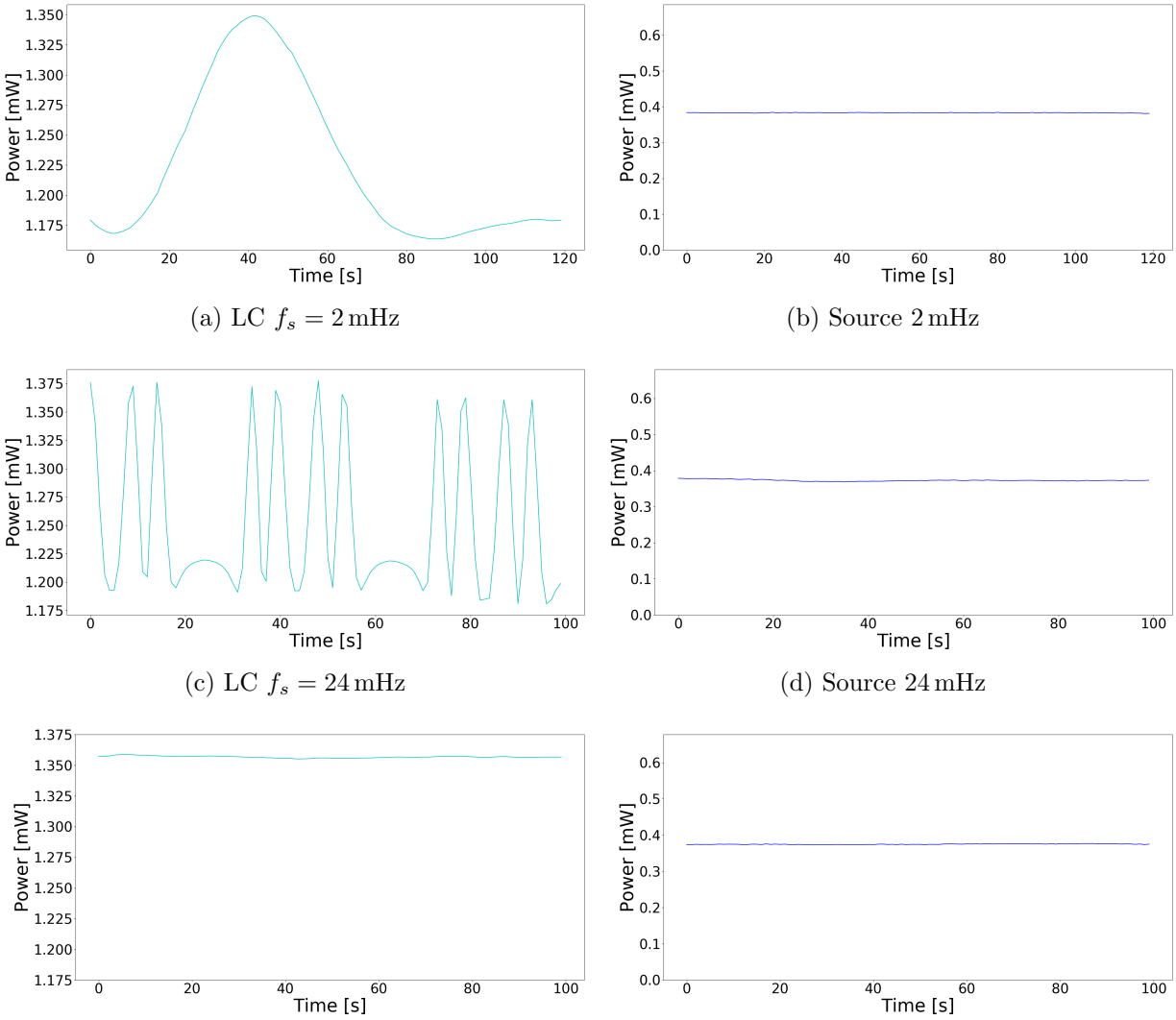
3.2.3 Phase Sweep

Normally the phase ϕ, in (3.2), is slow and visible state rotations are on the order of hours in time, if the fibers and system are left undisturbed in a laboratory setting. This renders it very unpractical to reasonably observe any phase drift unless very long data sets are taken. To shorten the data collection, I induced a faster phase drift with external sources denoted by S in Fig. 3.2.

One technique to inducing an increased phase drift is to take advantage of the fact that bending the fiber causes a phase drift, I used a micrometer translation stage to induce controlled bends in the fiber. By attaching the fiber on Alice's side to the translation stage and slowly moving it such that the fiber bends. The phase induced by the fiber changes as a function of bend angle. If bent slowly enough, this phase change can be smooth a continuous. Unfortunately, this technique is not accurate and is difficult to reproduce the same phase drift speed for different data collections.

To induce a phase shift that is more accurately controlled and faster, I used a liquid crystal (LC) retarder (Thorlabs LCC1411-A) to induce a phase on again Alice's side of

the entangled state in (3.2). The LC retarder can change the index of refraction for along one of its crystal axes, typically the slow axis, which similarly to the PMF, can induce a phase difference between any polarization aligned to this axis and its orthogonal pair. One can change the amount of phase difference by changing the voltage applied to the LC. The voltage applied to the LC can change very quickly and can have a variety of modulation shapes and depths. The problem with the LC is that their was an absorption along the slow axis as a function of the voltage. This causes a drop in entanglement quality and visibility in the superposition bases (D/A, R/L). This absorption can be clearly seen in Fig. 3.6 (a)&(c). The power transmission was measured by send a know polarization of light towards the LC, in this case horizontal polarization was used. The polarization was aligned to the slow axis of the LC since this is the axis which can alter its index of refraction. The power of the transmitted light is recorded by a power meter. The power meter was not polarization sensitive and was recording the optical power of the beam after the LC. To ensure that the laser source was not a source of the power fluctuations, the source power was monitored via a second power meter. To further demonstrate that this effect is polarization dependent, vertically polarized was also sent to the LC and the output optical power was recorded. Fig. 3.8 shows that the vertically polarized light is not effect by the voltage modulation, thus only the polarization that is aligned to the slow axis of the LC will experience a loss in transmission. This absorption would cause an imbalance in the state and thus a loss in entanglement quality. Data runs were collected with using the LC retarder, however, I wanted a technique that does not induce loss of entanglement quality.



(a) LC $f_s = 2\,\text{mHz}$ (b) Source 2 mHz

(c) LC $f_s = 24\,\text{mHz}$ (d) Source 24 mHz

(e) LC $f_s = 0\ 2\,\text{V}$ (f) Source 2 V

Figure 3.6: LC Retarder transmission data to demonstrate the absorption loss as a function of applied voltage. The incident polarization was set to be horizontal with the slow axis of the LC aligned to it. (a) 2 mHz voltage modulation frequency from $1V-2$V. There is a clear peak transmission. (c) 24 mHz voltage modulation frequency from $1V-2$V. The voltage dependence of the LC is evident in the peaks that are present throughout the figure. (e) A constant 2 V is applied to horizontally polarized light. No loss in transmission is observed indicating the loss in transmission is voltage dependent. (b)&(d)&(f) Laser source power during the same data acquisition as the corresponding data set to indicate that the source of the loss in transmission is not laser instability. The f_s are described as in Fig. 3.7.

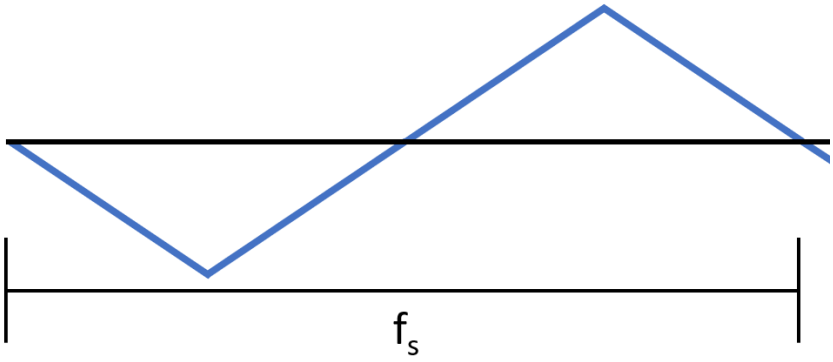


Figure 3.7: Waveform pattern for the voltage applied to the LC. The f_s is defined in this figure for reference in Fig. 3.6.

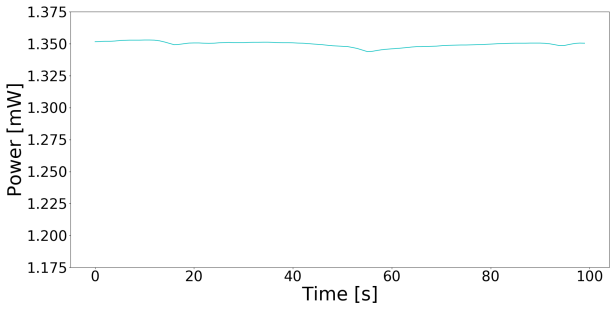


Figure 3.8: Vertically polarized light subject to 24 mHz voltage modulation frequency from $1V - 2$V. There is no absorption as the effect is only seen for polarizations aligned to the slow axis.

The other technique that is used to induce the phase is a well known technique amongst experimental optics groups. The rotation of a birefringent element such as a Half-wave plate (HWP) or a Quarter-wave plate (QWP) with its slow axis aligned to one of the polarization of the computation basis it will induce a phase difference as a function of angle. This technique is somewhat in-between the first two whereas it does not induce loss as a function of phase difference while it is still controllable. One issue was that large rotation angles of, in my experiments case, the HWP will cause an alignment shift in the analyzer and thus cause a loss in visibility in all bases and thus entanglement quality. Ideally automation of this system would have been great but one only has so much time when completing a Master's of Science.

3.3 Models

In every good experiment, one needs models to predict and demonstrate what to expect from experiments. To simulate the 3-2 basis protocol, I have made some models to attempt to describe and model the system that we are dealing with. To start we take (3.2) but instead add the ability to imbalance the entanglement, i.e. pump one direction through the crystal more than the other.

$$\begin{aligned} |\Psi'\rangle &= (a|0\rangle_A|1\rangle_B + e^{-i\phi}\sqrt{1-a^2}|1\rangle_A|0\rangle_B) \\ \rho' &= |\Psi'\rangle\langle\Psi'| \end{aligned} \tag{3.7}$$

Where $\|a\| \leq 1$ and ϕ is from Eq.(3.1). Now we apply a depolarizing channel to it via the well know Kraus operators for depolarizing channels to simulate overall losses in the system, which includes dark counts, background counts and other depolarizing effects [77].

$$\begin{aligned} \hat{p}_0 = \sqrt{1 - \frac{2\,p + dep_{DA}}{4}}I, \quad \hat{p}_z = \sqrt{\frac{dep_{DA}}{4}}\sigma_z \\ \hat{p}_y = \sqrt{\frac{p}{4}}\sigma_y, \quad \hat{p}_x = \sqrt{\frac{p}{4}}\sigma_x \end{aligned} \tag{3.8}$$

where σ_i are the Pauli matrices and$p \leq 1$ is the probability of a σ_x and σ_y spin flip error which can be regarded as the degree of depolarization in the computational basis (H/V), which causes depolarization of the entire state (stronger in the HV basis then others), while $dep_{DA} \leq 1$ is the probability of a σ_z flip error which can regarded as the degree of depolarization in the "diagonal" visibility. We claim here that the diagonal bases, because of the PM fibers, may have a reduced visibility (Eq. (1.9)) compared to the computational basis (H/V). Applying the Kraus operators to the density matrix ρ'

$$\rho_{mod} = \sum_i (\hat{p}_i \otimes \hat{p}_i)\rho'(\hat{p}_i^\dagger \otimes \hat{p}_i^\dagger) \tag{3.9}$$

Eq. (3.9) is the final density matrix model is used to simulate the expected experimental results. The results of this model are shown in Fig. 3.9 and Fig. 3.10 where a set of random data similar to what one would expect in an experiment is generated in order to simulate fluctuations in the count rates, relative detector efficiency mismatches and other losses. The parameter ranges are found in Tab. 3.1 The data was generated by selecting a range for each of the parameters $a, p, \mathrm{dep_{DA}}$ and have a randomly generate values for the parameters within that range. The phase was a continuous sweep from $0 \leq \phi \leq \pi$.

Table 3.1: Simulation parameter range that was selected in order to simulate the fluctuations in count rates and variations in detector efficiencies. The dep_{DA} range was selected to be quite large since this was observed during experiments

Parameter	Range
a	$\left[\frac{1}{\sqrt{2}} - 0.02, \frac{1}{\sqrt{2}} + 0.02\right]$
p	$[0.010, 0.028]$
dep_{DA}	$[0.03, 0.12]$

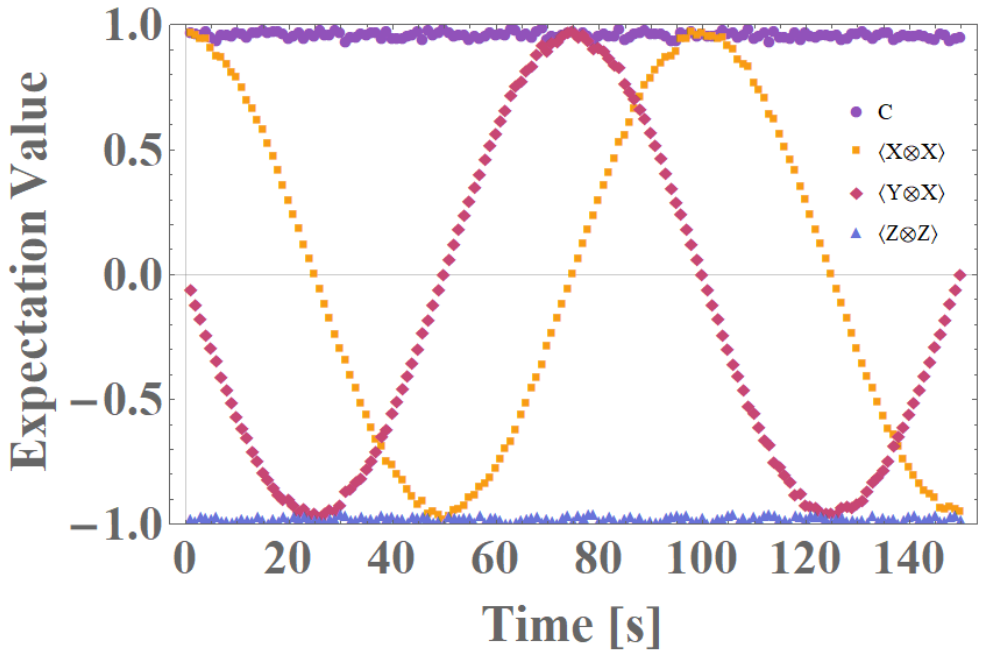
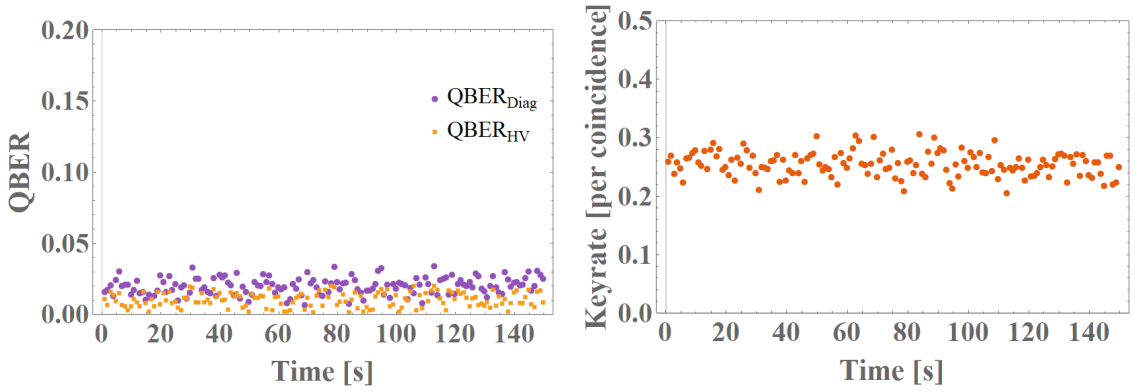


Figure 3.9: Expectation values of the simulated data for a modeled density matrix. As we can see that C is constant.

Figure 3.9 shows that though the relative phase in the computational basis is changing as is evident in the $\langle X_A \otimes X_B \rangle$ and $\langle Y_A \otimes X_B \rangle$ values. However, we can still infer the visibility in the diagonal basis and thus extract a QBER and Keyrate as seen in Fig. 3.10



(a) QBER (b) Keyrate

Figure 3.10: (a) QBER calculated for both the computational basis and the "diagonal" basis. (b) A keyrate is estimated form these QBER's using Eq. (3.12).

The QBERs in Fig. 3.10 are calculated via,

$$\text{QBER}_{HV} = \frac{1 - \langle Z \otimes Z \rangle}{2}, \qquad \text{QBER`}_{Diag} = \frac{1 - \langle C \rangle}{2} \tag{3.10}$$

where,

$$C = \sqrt{\langle X_A \otimes X_B \rangle^2 + \langle Y_A \otimes X_B \rangle^2} \tag{3.11}$$

which allows us to infer the maximum visibility for the diagonal basis this is further discussed in Appendix B. The QBER in this work is unitless and is reported as a ratio and not as a percentage. The keyrate is calculated via:

$$R \geq Q_\lambda (1 - f H_2(\text{QBER}_{HV}) - H_2(\text{QBER}_{Diag})) \tag{3.12}$$

[78] where Q_λ is the basis reconciliation factor, ($\frac{1}{6}$ in our case), and f is the bidirection error correction efficiency, ($f \approx 1.22$ in our case). It should be noted that the keyrate here is is in the units of fraction of secure key per detection event (in our case coincidence count). It is also the asymptotic case which means that the sample has effectively and infinite number of events. QBER_{HV} can be estimated from a subset of the data, by using every nth bit, or from error correction algorithms [26–29]. QBER_{Diag} is directly determined from

the measured coincidences, as per Eq. (3.10). In addition, the basis reconciliation factor changes based on the implementation, as seen in Fig. 3.4 and Fig. 3.5 we selected evenly distributed basis selections, however, one can have different weighting selections for the measurement basis selections. For example, in Fig. 3.5, rather than having a 50:50 even distribution between the measurement bases, one could select say 90:10 [79]. The only requirement is that there are statistically sufficient counts for all the bases.

We also show the results for QBER and keyrate as a function of each parameter in ρ_{mod} that may be varied as shown in the Fig. 3.11. Each parameter in Fig. 3.11 is varied over a full range, while the other parameters are left constant at some initial value. As is prevalent in Fig. 3.11 it is apparent that the keyrate is gravely affected by the quality of the entanglement. The most important thing to note from the results in Fig. 3.11 is that the keyrate is not affected by the changing phase. This is should not come as a surprise, though it is quite important for our protocol which allows for the use of the PM fibers. The phase independence should be stressed further that it also does not have an effect on the QBER of the "diagonal" basis as seen in Fig. 3.11 (d). Given that the QBER is not effected by the phase, we can further justify the use of the C-parameter as a means of verifying the presence of an eavesdropper thus validating our protocol.

Though this model does demonstrate the various aspects of how the protocol will behave, it is not accurate. This is because, most entangled sources are not varying in purity or visibility as rapidly as this model depicts. Most of the parameters we varied in this model, other than the phase, are actually fairly stable and constant with time. Thus, we needed another model in order to accurately simulate what is observed in the experiments.

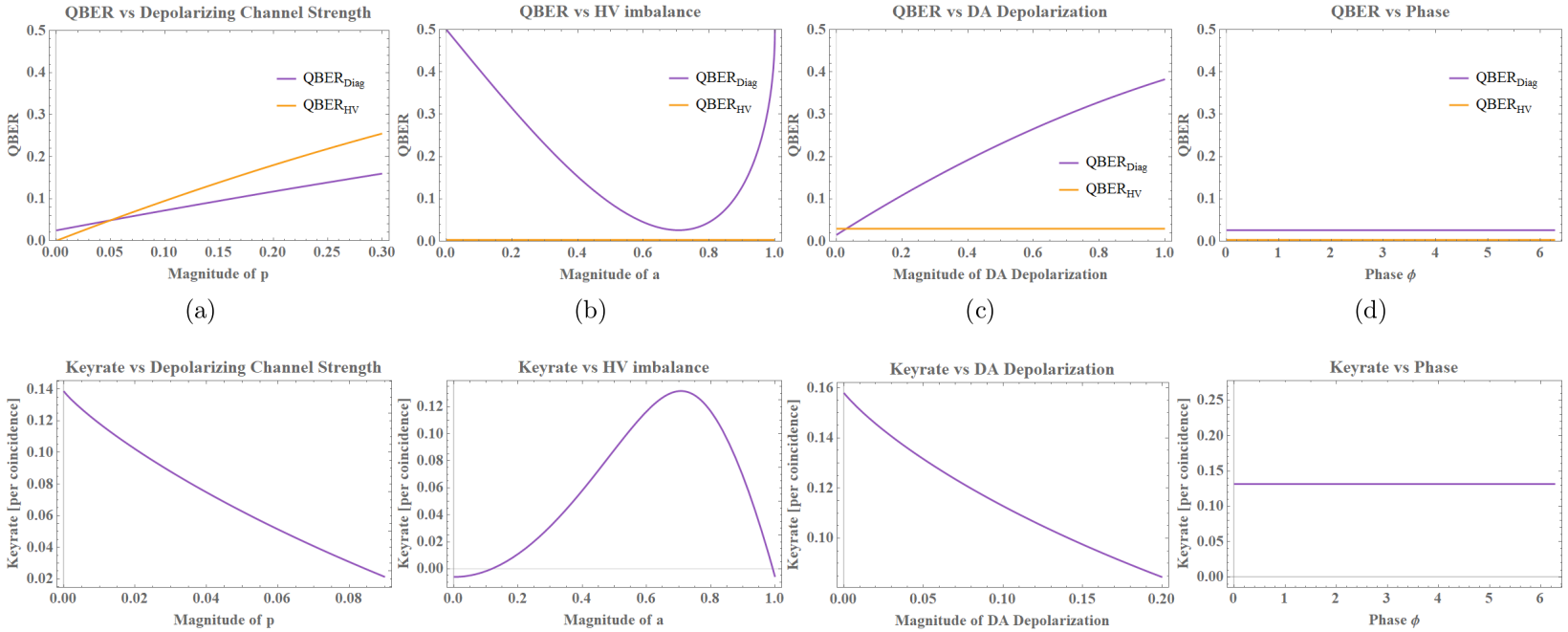
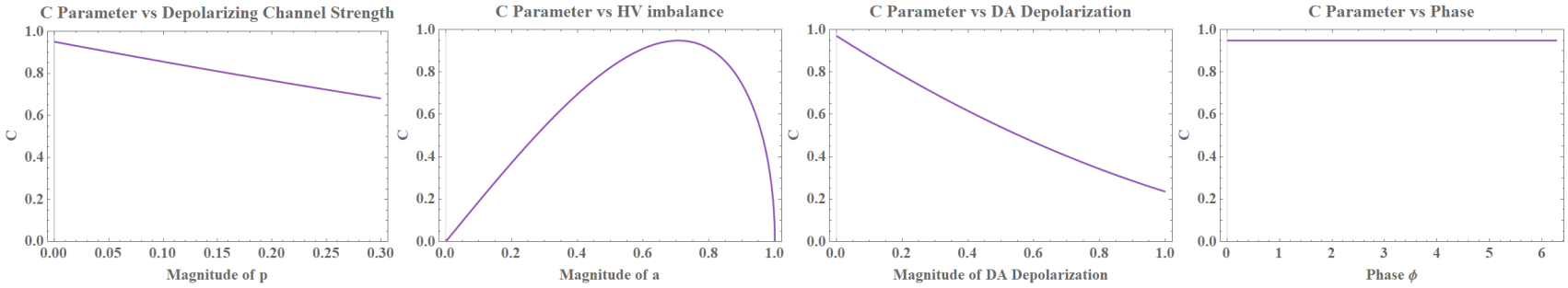


Figure 3.11: Various plots demonstrating the effect of the various parameters of our model on the QBER and Keyrate. Other than the parameter that is being adjusted, the other values are set to a predetermined, fixed initial value with no random variation. When not varied, $a = \sqrt{\frac{1}{2}}$, $p = 0.003$, $dep_{DA} = 0.05$ and $\phi = 0$. (a) The QBER of the system as a function of the strength of the depolarizing channel, p in Eq. (3.8). (b) QBER as a function of HV imbalance (magnitude of a parameter in Eq. (3.7)), note that a value of $\frac{1}{\sqrt{2}}$ is the perfectly balanced case dues to normalization. (c) QBER as a function of diagonal depolarization. (d) QBER as a function of relative phase in radians induced by the PMF, note that the phase has no effect on QBER. (e) The lower bound for the keyrate as a function of the depolarizing strength. (f) Keyrate as a function of HV imbalance (magnitude of a parameter in Eq. (3.7)), note that a value of $\frac{1}{\sqrt{2}} = 0.707$ is the perfectly balanced case dues to normalization. (g) Keyrate as a function of diagonal depolarization. (h) Keyrate as a function of relative phase in radians, phase also has no effect on keyrate.



(a) (b) (c) (d)

Figure 3.12: Plots of the C parameter as a function of the model parameters. These figures should be compared with those in Fig. 3.11 to observe the relations between QBER, keyrate and the C parameter. When not varied, $a = \sqrt{\frac{1}{2}}$, $p = 0.003$, $dep_{DA} = 0.05$ and $\phi = 0$. (a) The C parameter of the system as a function of the strength of the depolarizing channel, p in Eq. (3.8). A decrease is observed as expected. (b) C parameter as a function of the as a function of HV imbalance (magnitude of a parameter in Eq. (3.7)), note that a value of $\frac{1}{\sqrt{2}}$ is the perfectly balanced case dues to normalization and thus a maximum value for C at $a = \frac{1}{\sqrt{2}}$. (c) C parameter as a function of diagonal depolarization. An increase is observed as expected. (d) C parameter as a function of phase. There is no change as is expected via the derivation in Appendix B.

Poissonian Count Parameter Variation

Another more precise count model that allows us to better simulate the noise that is observed during experiments is to generate simulated coincident count rates with a Poisson distribution. The goal was to generate pseudo data with a random number generator such that the data matched a Poisson distribution as shown in Fig. 3.13

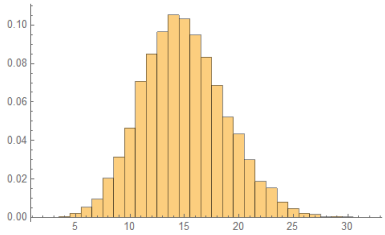


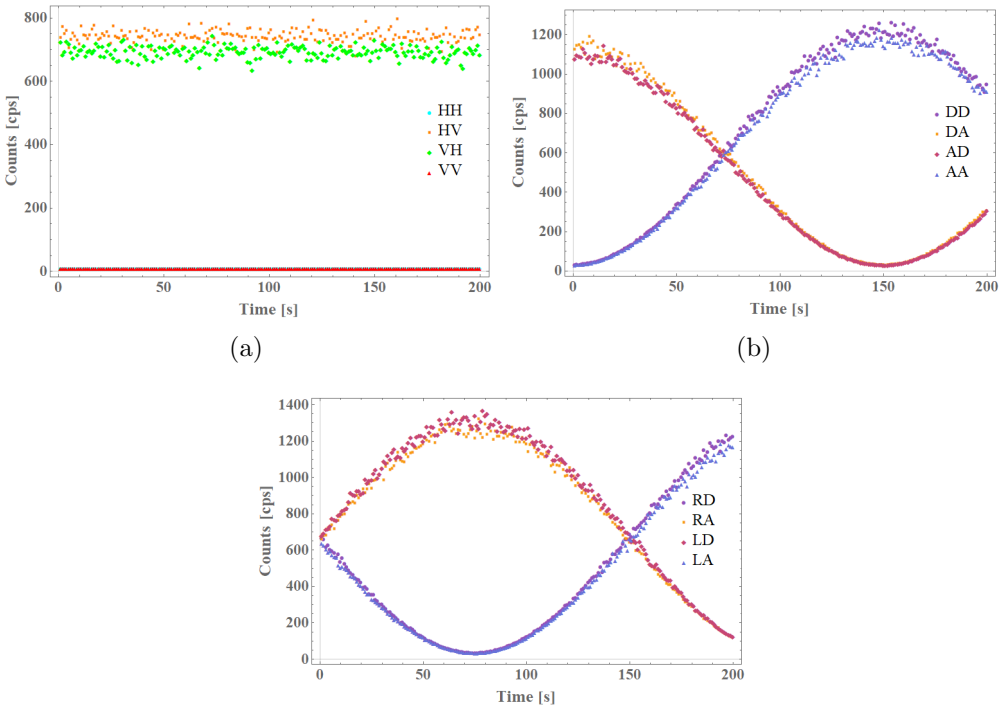
Figure 3.13: Poisson distribution probability density function with a mean of 15.

this distribution is typical for counting experiments, detectors, and is suitable for our simulations. The simulation is as follows:

1. Select the parameters for the density matrix model Eq.(3.9)
2. Use the positive-operator valued measures (POVM) of the various measurements done in the 3-2 protocol to compute the probabilities of detection ($\text{Prob}_{ji} = \text{Tr}(\rho_{mod} M_{ji})$), where M_{ji} is the POVM, where $i = \{H, V, D, A, R, L\}$ and $j = \{H, V, D, A\}$
3. Compute the count rates of each detection $\eta_{ji} = \text{Prob}_{ji} N_{ji}$ where N_{ij} is the randomly generated Poisson distribution for each of the coincidence measurement pair. This is further explained below.
4. Calculate all the various quantities using the equations presented above ((3.10),(3.12),(3.13)), tomography as discussed in Sec.3.4.2 was also performed on the simulated counts

The results of this simulation are in Fig. 3.14

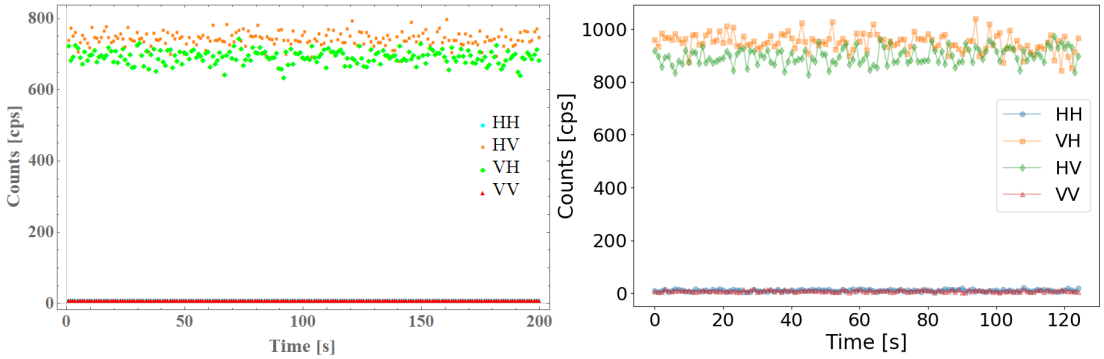
To further explain the need for differing count rates for each measured coincidence pair, each detector and optical path will have differing efficiencies that will effect the overall count rates. To simulate this, one cannot capture this in the model of Eq.(3.9) alone and thus is not prevalent in the Prob_j. However, by giving each individual coincident measurement pair an unique count rate, we can capture the discrepancies observed in experiment as seen in Fig. 3.15.



(a) (b)

(c)

Figure 3.14: Various plots demonstrating the simulated coincidence count data (a) HV basis coincidence counts (b) DA basis coincidence counts (c) $\langle Y_A \otimes X_B \rangle$ measurement coincidence counts. The expectation values in (b) and (c) varying with the varying phase, as expected



(a) Simulation (b) Experiment

Figure 3.15: Comparison of coincidence counts between the simulation (a) and the experiment (b). It is evident that the simulation matches the experimental results that are obtained for the system.

Seeing that this model is sufficient to describe the experimental situation given the coincidence counts, we plot the results of the expectation values, Fig. 3.16 and the QBER and keyrate, Fig. 3.17. We will later use these simulation results to compare to the experimental values presented in Sec. 3.4.

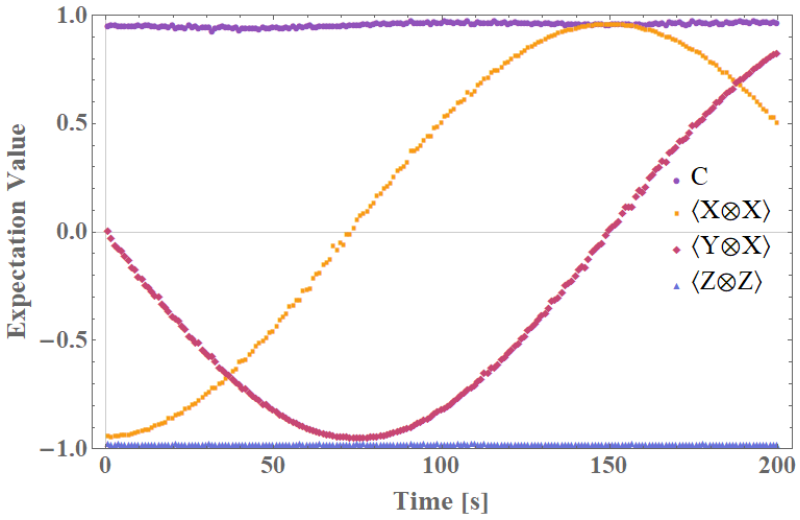
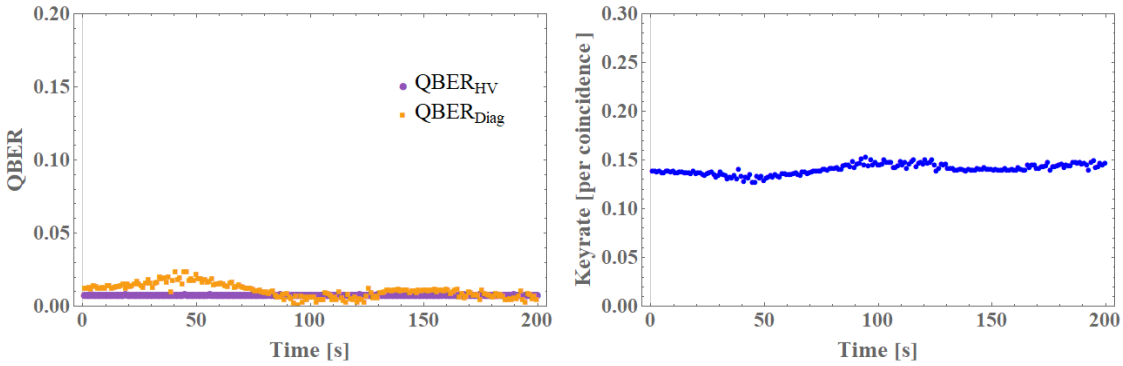


Figure 3.16: Expectation value results for the Poissonian count variation. The expectation values behave as expected with the diagonal bases varying with the phase and C remaining constant with the change in phase.



(a) QBER (b) Keyrate

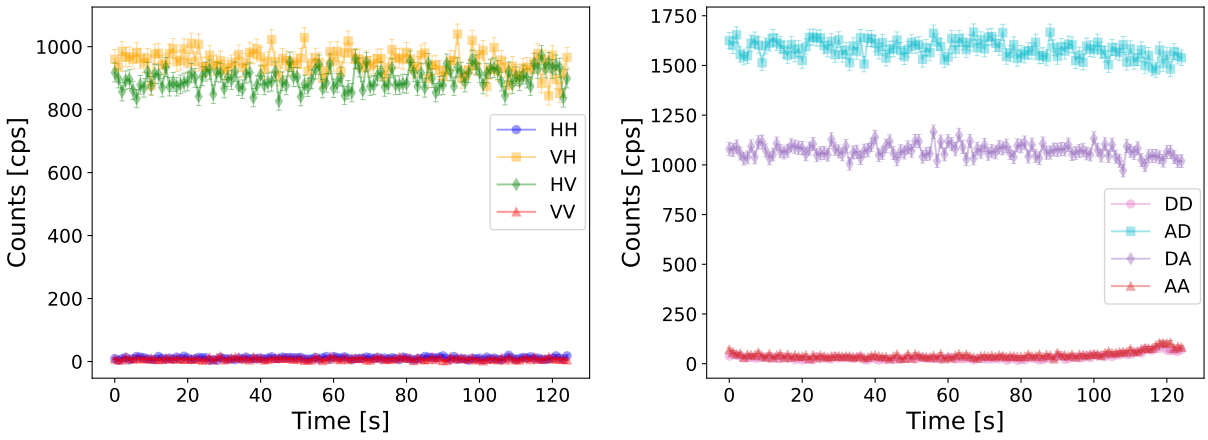
Figure 3.17: The QBER (a) and keyrate (b) results for the Poissonian count variation. The QBER is much more stable than that in Fig. 3.10 which can be attributed to the much more accurate model since source stability plays a major role in the QBER and keyrate.

3.4 Experimental Results

The following section will describe the results in various test situations. As mentioned in Sec. 3.2, the data collection was done allowing for an induced phase drift to be applied to the system and also collected for when the system is allowed to drift on its own. Both cases are analyzed for various results. I collected coincidence detections and single photon detections on both Alice and Bob's analyzers.

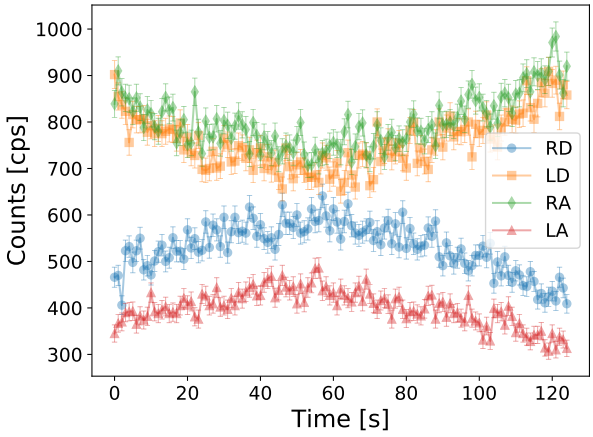
3.4.1 Counts and Expectation Values

Below are some figures that show the collection of the single photon and coincidence counts. The experimental source should output equal counts amongst all the detection ports. However, it should be noted that the differences can be correlated to detection efficiencies of the individual detectors and channel loses through each port as seen in Fig. 3.18, 3.19 and 3.20.



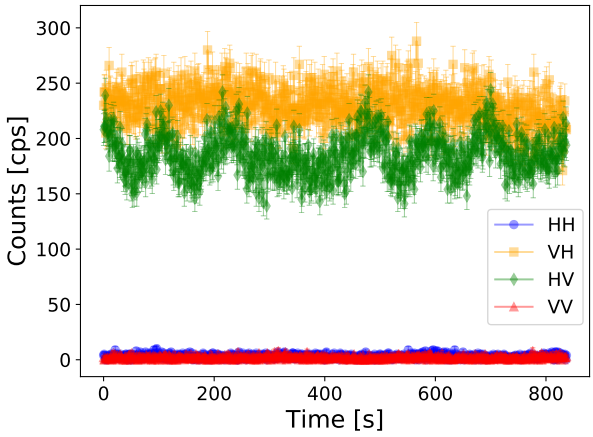
(a)

(b)

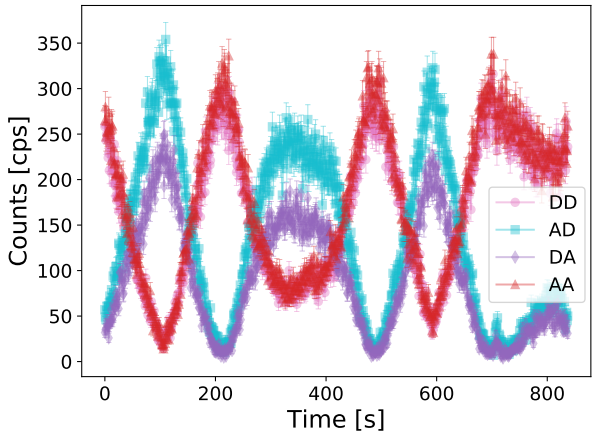


(c)

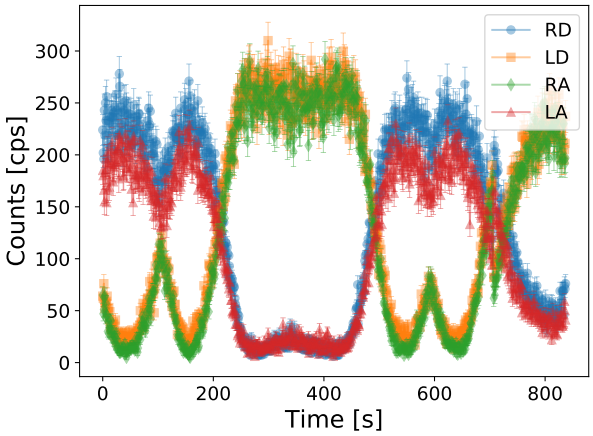
Figure 3.18: Plots demonstrating the experimental coincidence count data when the system is left to drift on its own (a) HV basis coincidence counts (b) DA basis coincidence counts (c) $\langle Y_A \otimes X_B \rangle$ measurement coincidence counts. Error bars are present in all figures, however, some might be too small to be visible. The error bar values are derived using error propagation of the statistical counting error.



(a)

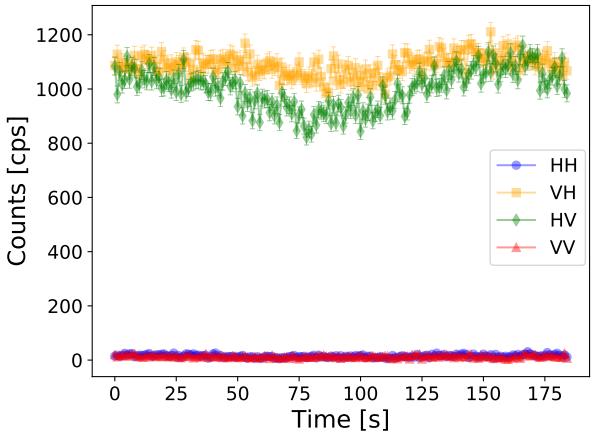


(b)

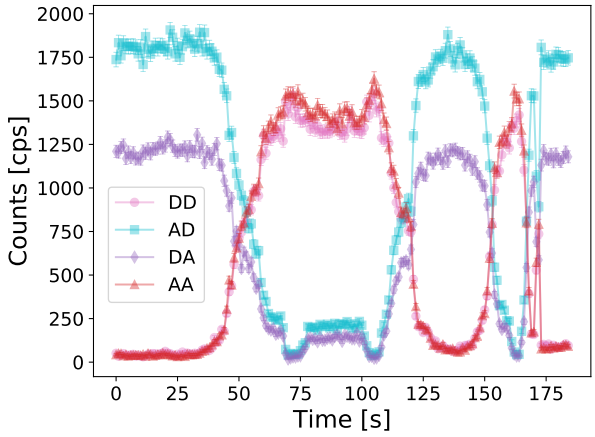


(c)

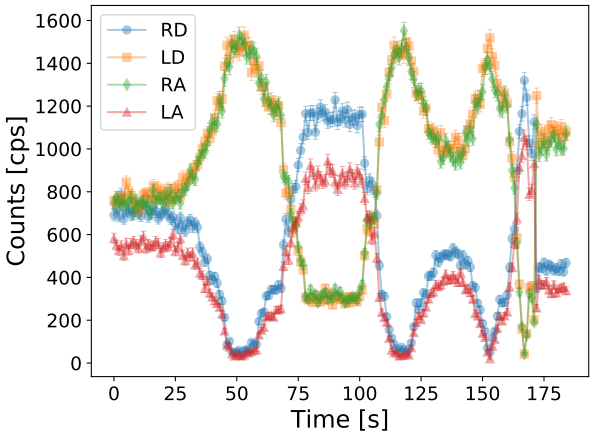
Figure 3.19: Plots demonstrating the experimental coincidence count data with an induced phase by a liquid crystal retarder (a) HV basis coincidence counts (b) DA basis coincidence counts (c) $\langle Y_A \otimes X_B \rangle$ measurement coincidence counts. Error bars are present in all figures, however, some might be too small to be visible. The error bar values are derived using error propagation of the statistical counting error.



(a)

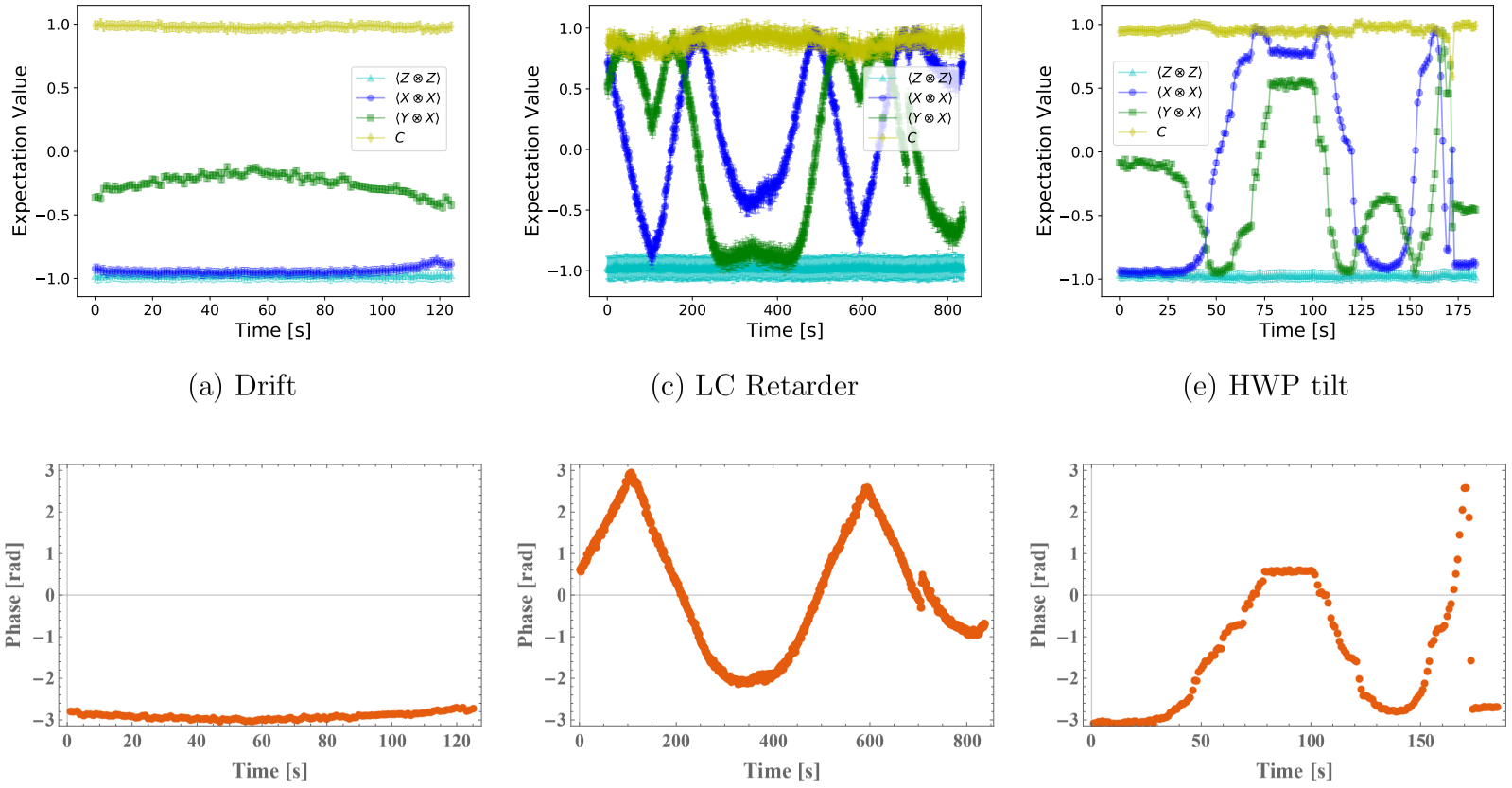


(b)



(c)

Figure 3.20: Plots demonstrating the experimental coincidence count data with an induced phase by rotating a birefringent material such as a HWP (a) HV basis coincidence counts (b) DA basis coincidence counts (c) $\langle Y_A \otimes X_B \rangle$ measurement coincidence counts. Error bars are present in all figures, however, some might be too small to be visible. The error bar values are derived using error propagation of the statistical counting error.



(a) Drift (c) LC Retarder (e) HWP tilt

(b) Drift Phase (d) LC Retarder Phase (f) HWP tilt Phase

Figure 3.21: Plots demonstrating the experimental expectation values (Eq. (3.13)) in the different experimental situations (a) System left to drift, average C value of $C = 0.9777 \pm 0.0104$ (b) LC induced phase drift, average C value of $C = 0.8877 \pm 0.0459$ (e) HWP induced phase drift, average C value of $C = 0.9571 \pm 0.0394$. (b),(d) and (f) shows the relative phase between H and V that the system is subject to, Alice and Bob do not know this value. Error bars are present in all figures, however, some might be too small to be visible. The error bar values are derived using error propagation of the statistical counting error.

The expectation values of each basis was calculated via:

$$\langle M \rangle = \frac{m_{++} - m_{+-} - m_{-+} + m_{--}}{\sum_{i,j} m_{ij}} \tag{3.13}$$

where $i, j \in \{+, -\}$, m_{ij} are the coincidence counts between Alice and Bob's measurements, and M is the overall two qubit measurement of choice. The thing to note from Fig. 3.21 is that the expectation value of the H/V basis is a constant $\langle Z \otimes Z \rangle = -1$ for all tests while the values for both the diagonal and rotational bases are drifting with the phase induced by the fibers and the external phase source. Both non-computational bases follow a sine curve that are π shifted from one another. It should also be noted that these plots are very similar to the randomly generated data from our simulation models. In addition, we also observe that the constant C is indeed constant if the phase is rotation slow enough. If the phase is too fast we see a drop in the visibility (Fig. 3.20 (c)) due to the counting statistics of the measurements.

When the phase moves to quickly, the finite time interval in which the time tagger is collecting counts will experience a large fluctuation. This large fluctuation of counts will result in a drop in visibility because the number of coincidences will be "smeared" over the interval. If the time tagger were sufficiently fast and our integration time for recording the coincidence counts was also very small,(1s for our experiments), one could observe very fast phase fluctuation with little effect on the overall visibility. This should not occur in theory because there is no phase dependence in C. However experimentally, due to the statistical nature of C the tolerance of the phase drift is dependent on the instrumentation used.

Comparing the experimental values for C to the simulated average value of $C = 0.9716 \pm 0.0094$[1] taken from the data used to generate Fig.3.16. Two of the experimental trials are in agreement with the simulated values, the system without an external phase inducer i.e. the drift case ($C = 0.9777 \pm 0.0104$) and the HWP tilt case ($C = 0.9571 \pm 0.0394$). The value for the LC retarder case of $C = 0.8877 \pm 0.0459$ is indicative that the LC caused absorption that reduces the quality of the entanglement as discussed in Sec. 3.2.3.

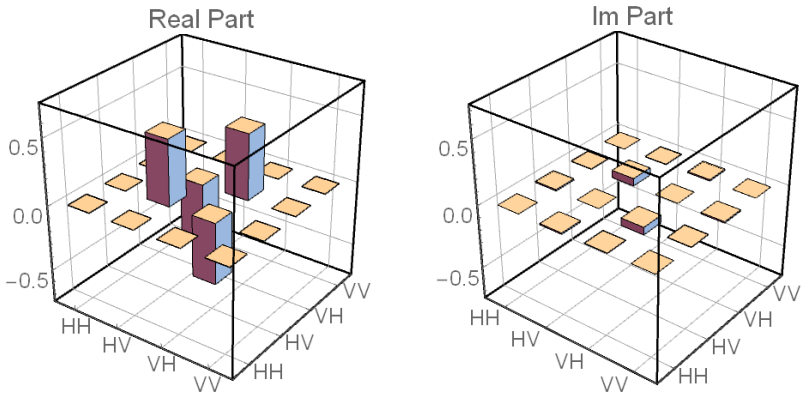
3.4.2 Tomography

With the measurements made, I was able to perform a tomographic reconstruction of the two qubit entangled photon state via the maximum likelihood method. This method's only assumptions are that the density matrix is physical i.e. trace being unity and being a

[1] This can be adjusted based by tuning the parameters in Eq. (3.9)

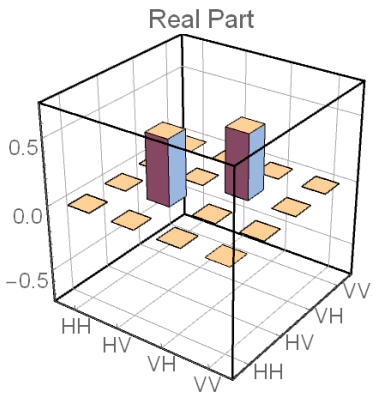
positive semi definite matrix, as seen in Sec. 1.1.4. The reason for the use of this method is that the combined measurements that Alice and Bob make are not a tomographically complete set of measurements. Thus typical linear inversion methods cannot be used Sec. 1.1.4. However, as discussed in Sec. 1.1.4, with these measurements we are limiting the subspace of the Hilbert space in which our density matrix may exist. Nonetheless, the maximum likelihood method fins the best density matrix to fit the data, thus some areas of the density matrix may be filled in by the optimization algorithm in order to find a solution. Thus, even without a tomographically complete set of POVM's, we are still able to get a fairly good approximation of the state of the system.

As we can see in Fig. 3.22 the phase has an expected effect on the density matrix. The effect is also prevalent in the experimental data as seen in Fig. 3.23.

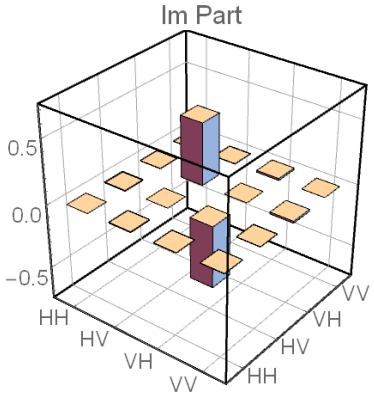


(a) $\phi = 2.961$

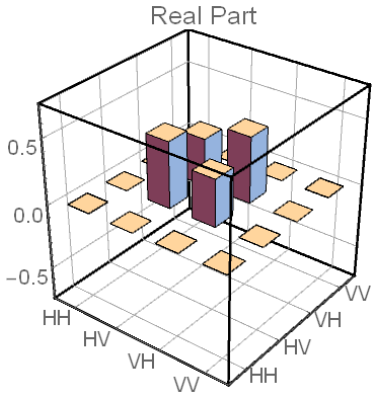
(b) $\phi = 2.961$



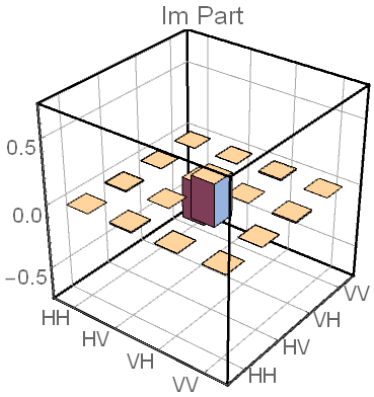
(c) $\phi = -1.499$



(d) $\phi = -1.499$

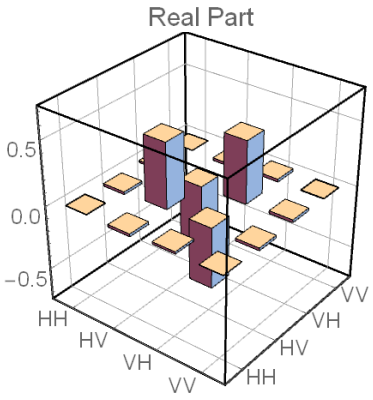


(e) $\phi = 0.616$

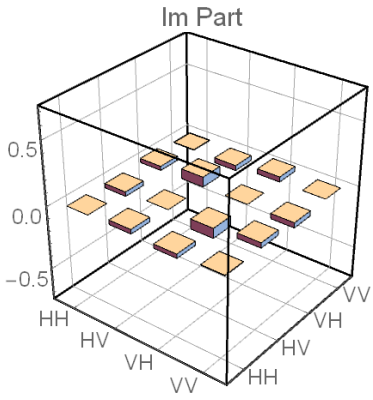


(f) $\phi = 0.616$

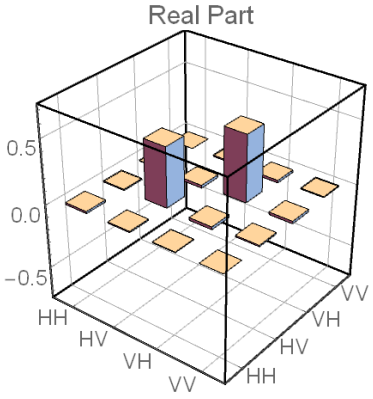
Figure 3.22: Various plots demonstrating the resulting density matrix from the simulated data at various phase values. Each row corresponds to a complete density matrix with the corresponding real and imaginary parts. All plots share the same parameters of $a = \frac{1}{\sqrt{2}}$, $p = 0.080$ and $dep_{DA} = 0.02$, with the phase value indicated in subcaptions.



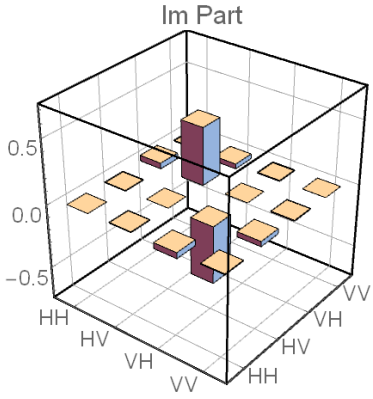
(a) Drift: $\phi_E = 2.957$, $t = 80\,\mathrm{s}$



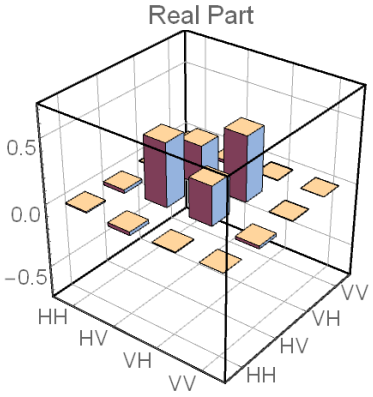
(b) Drift: $\phi_E = 2.957$, $t = 80\,\mathrm{s}$



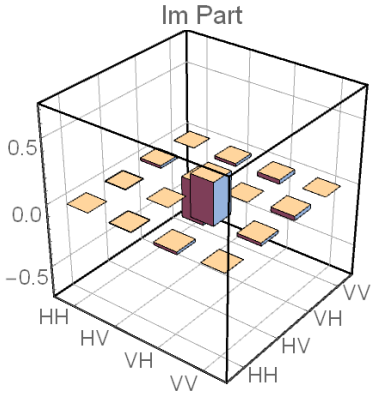
(c) LC Retarder: $\phi_E = -1.483$, $t = 42\,\mathrm{s}$



(d) LC Retarder: $\phi_E = -1.483$, $t = 42\,\mathrm{s}$



(e) HW tilt: $\phi_E = 0.622$, $t = 100\,\mathrm{s}$



(f) HW tilt: $\phi_E = 0.622$, $t = 100\,\mathrm{s}$

Figure 3.23: Various plots demonstrating the resulting density matrix from the experimental data at various phase values. Each row corresponds to a complete density matrix with the corresponding real and imaginary parts. These data points were chosen to be similar to that of the simulated data. Phase values are normally not know to Alice or Bob during the key transfer.

From these density matrices, we are also able to calculate the quality of the entangled state as a function of time and the phase. We calculated the purity, concurrence, fidelity, and tangle. Some results are found in the plots below. The interesting but not surprising results from this calculations is that the quality of the measured entangled state is dropped during times of large phase drift as well as periods in which there is losses of photons due to the various optical elements such as the liquid crystal retarder.

The fidelity was calculated by using a search algorithm that finds a value for a phase ϕ_F, when applied to a pure state, maximizes the fidelity with the experimental state. This phase is compared to the experimental phase that is applied by the fiber or the external source, Fig. 3.25. Interestingly, ϕ_F matches fairly well the trend of ϕ_E, as seen in Fig. 3.25.

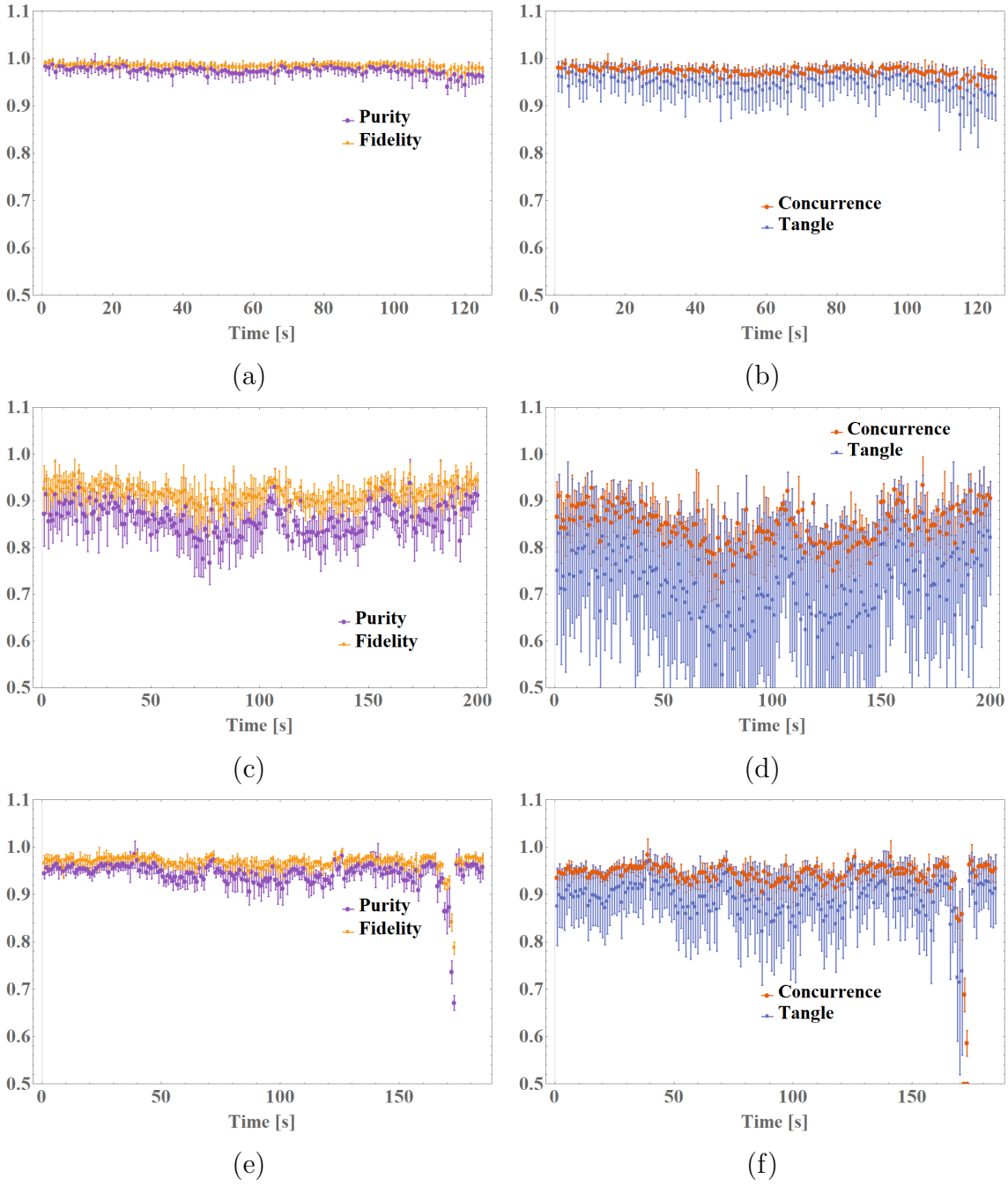
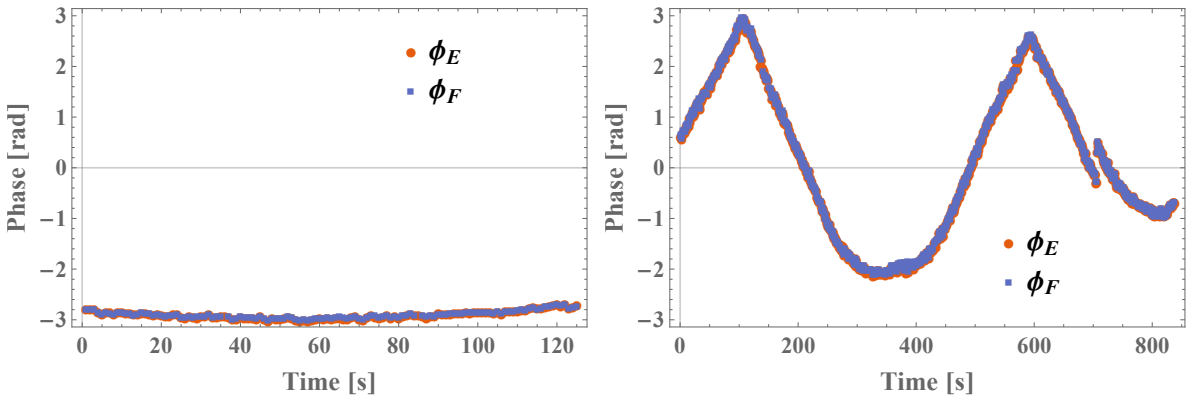
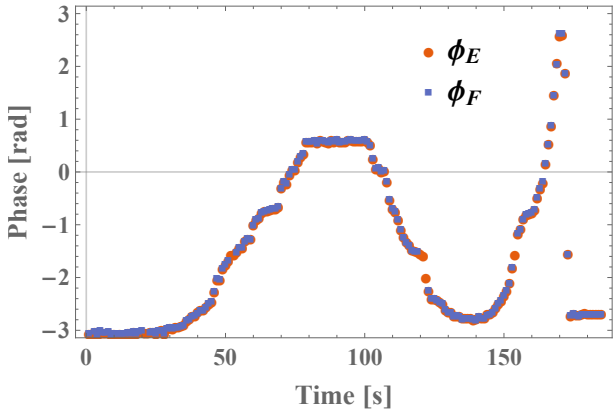


Figure 3.24: Various plots demonstrating the purity, fidelity, concurrence and tangle of the experimental data sets presented above. The fidelity was found by comparing the experimental state to the closest pure state. (a) & (b) correspond to the undisturbed system. (c) & (d) correspond to the liquid crystal induced phase. There is a clear drop in state purity, fidelity, concurrence and tangle. The count range was cut down to only show 200 s for clarity. (e) & (f) correspond to the half-wave plate. There is a sudden drop in the purity and fidelity at the end of (e) & (f) which is due to a period of rapid phase change. The error bars are derived using the Monte Carlo method presented in Sec. 1.1.4.



(a) Drift

(b) LC Retarder



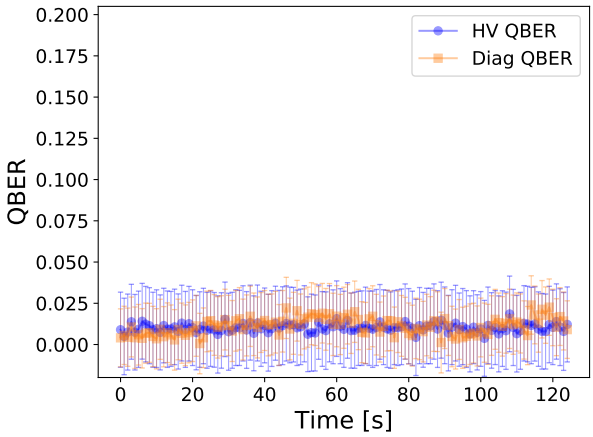
(c) HWP tilt

Figure 3.25: Experimental phase ϕ_E that is applied to the three data sets. ϕ_F is a calculated phase from the fidelity calculations done to produce the plots in Fig. 3.24. Interestingly, the two phases are equal in value for all three experimental cases.

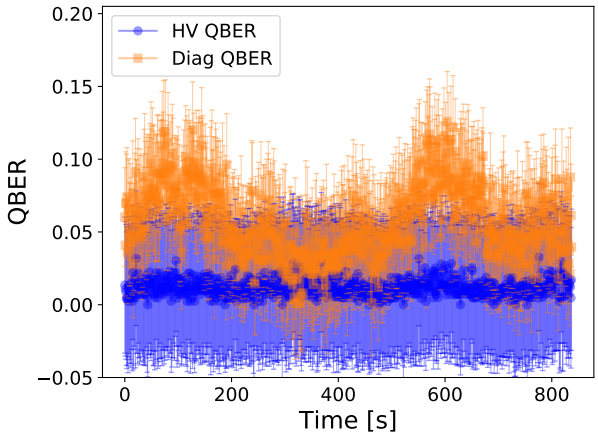
3.4.3 Key Rate/QBER

Following equation (3.10) I calculated the QBER of the experimental data. Select QBER's can be seen in the Fig. 3.26. As can be seen in Fig. 3.26 (b), the LC absorption has a very large effect on the QBER causing it to spike to 0.125 or 12.5% in the "diagonal" basis. It should also be noted that the total QBER is less than 0.06 or 6% in most of Fig. 3.26 (a) and some of Fig. 3.26 (c). There is also the spike in the QBER in Fig. 3.26 (c) that is caused by a rapid change in the phase. From Fig. 3.26 (c), I was able to determine a threshold for the robustness of the protocol. By finding the change in phase for points near the sudden spike in QBER that are below our threshold of 0.06, the protocol is determined to be resistant to phase changes up to 0.7 rad/s. This is great to quantify, but

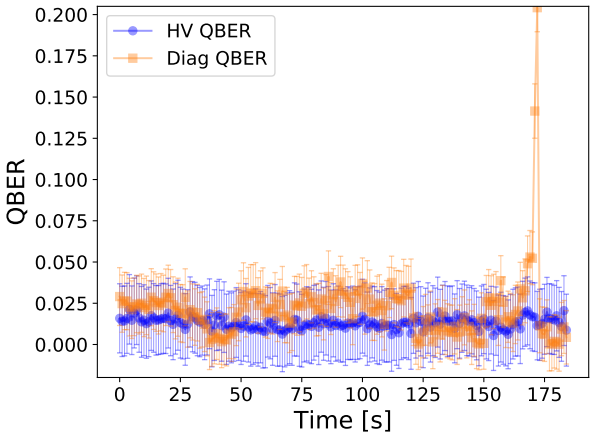
is difficult to translate to what would be expected when the system is implemented on the quantum optical ground station (Fig. 1.2). It is very difficult to predict how the angular speed of a moving transmitter translate to the phase induced by the fibers' motional stress. Nonetheless, this puts an upper bound to the phase resistance of the system in reference to our QBER threshold limit.



(a) Drift



(b) LC Retarder

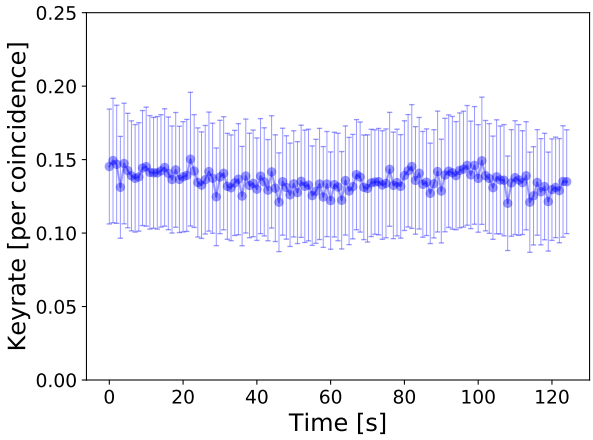


(c) HWP tilt

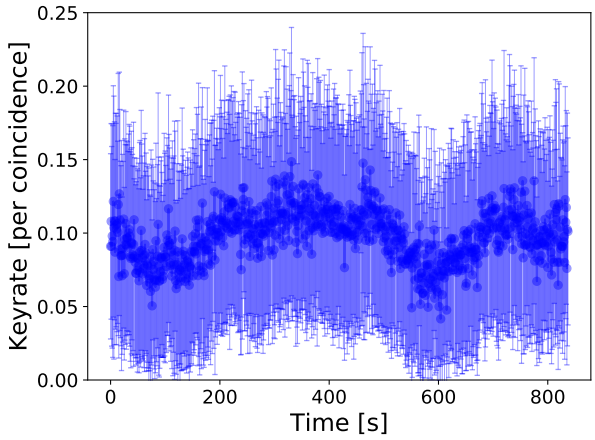
Figure 3.26: Plots demonstrating the experimental QBER that is obtained from Eq.(3.10) in the different experimental situations (a) System left to drift (b) LC induced phase drift (c) HWP induced phase drift. The sudden spike is due to a large shift in the phase value as varying the phase value too quickly causes smearing of the counts and increases the QBER. The error bar values are derived using error propagation of the statistical counting error.

I also calculated an estimated key rate based on the calculated QBERs as seen in the

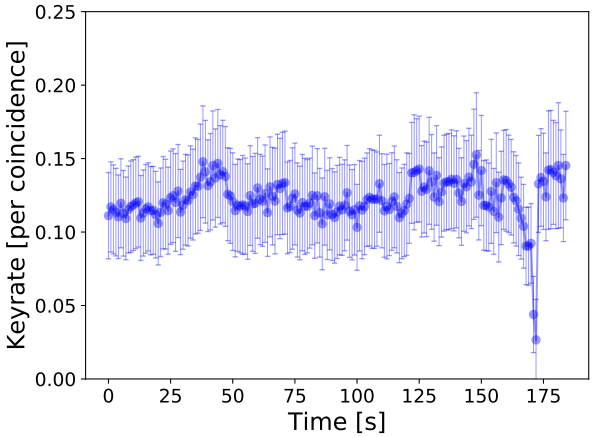
Fig. 3.27. Again, the effects of the LC absorption has an effect on the keyrate reducing it below 0.10 per coincidence. However, the case in Fig. 3.27 (a), where the system is let to drift, the keyrate is almost at an ideal value of ≈ 0.15 per coincidence. The ideal value comes from the basis reconciliation factor in Eq. (3.12).



(a) Drift



(b) LC Retarder



(c) HWP tilt

Figure 3.27: Plots demonstrating the experimental key rate that is obtained from Eq.(3.12) in the different experimental situations (a) System left to drift (b) LC induced phase drift (c) HWP induced phase drift. The drop in keyrate is due to the smeared resulting from a rapid change in the phase value. The error bar values are derived using error propagation of the statistical counting error.

Averaging Counting Blocks

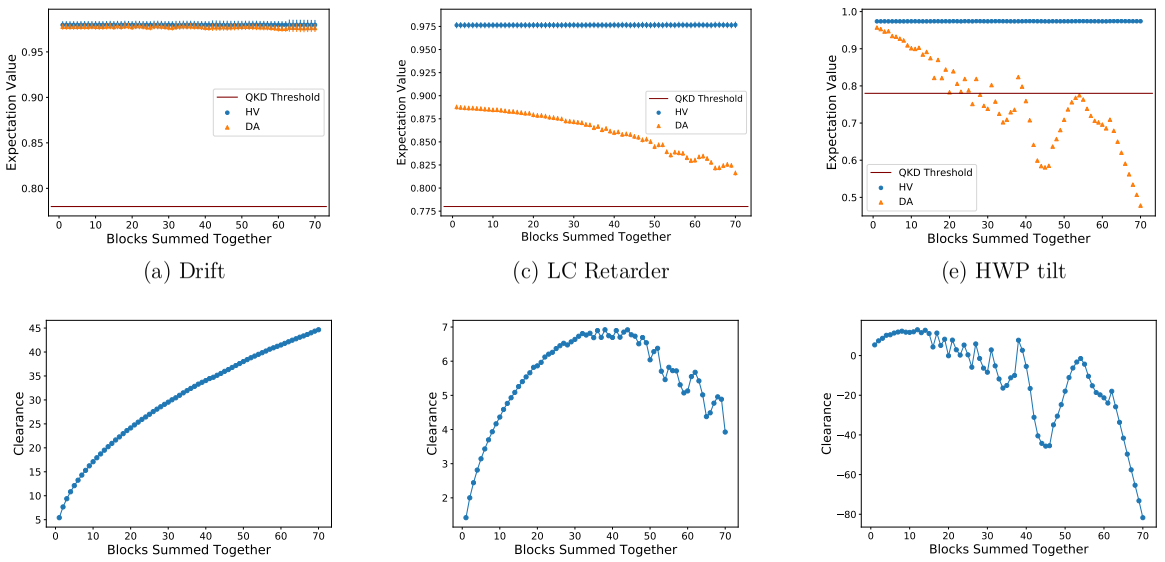
One means to overcome some of the finite size effects that are inherent to our system, due to the lower count rates, is to add the results of several counting blocks together. This can only be done if the relative phase of the system is drifting slowly. The adding of blocks can increase the clearance value from the minimum value for QKD. The basic idea is that the more blocks that are added together will reduce the relative error in the measurements. For example, having the counts collected over one second will produce a certain number of Poissonian counts, N_1. Now adding k number of these blocks will make it appear the system has collected counts over k seconds, i.e. $N_k > N_1$, for $k > 1$. Now the relative error in the counts is $\frac{\sqrt{N_k}}{N_k} < \frac{\sqrt{N_1}}{N_1}$. This reduction in error increases the clearance of the experimental value with a theoretical value. The clearance is given by the following equation.

$$Cl = \frac{M}{\sigma} \tag{3.14}$$

where M is the difference between the calculated expectation value and a theoretically estimated threshold value of ≈ 0.78 and σ is the error of the expectation value. The value of ≈ 0.78 can be found by taking the practical QBER limit for QKD of QBER≈ 0.06 and plugging this value into Eq. (1.8) where vis is the average visibility of both the diagonal and computational basis:

$$\text{vis} = \frac{\text{vis}_{HV}}{2} + \frac{\text{vis}_{diag}}{2}. \tag{3.15}$$

We get vis $= 0.88$. Now assuming a good visibility in the computational basis, say $\text{vis}_{HV} = 0.98$, plugging this into Eq. (3.15) and solving for the vis_{diag} we get $\text{vis}_{diag} = 0.78$. Now any value of the $\text{vis}_{diag} \geq 0.78$ is sufficient for QKD Fig. 3.28 shows this adding of blocks of counts and they show the effects of this on the various data sets I present. We can see that summing several time blocks together will decrease the value of the vis_{diag} if the phase is varying at an observable rate. However, the clearance increases since the summing the blocks increases the number of counts and thus reduces the relative error in the measurements as seem in Fig. 3.28 (b) and (d).



(a) Drift (c) LC Retarder (e) HWP tilt

(b) Drift (d) LC Retarder (f) HWP tilt

Figure 3.28: Plots demonstrating the expectation values and clearance in the different experimental situations (a) System left to drift, expectation value/visibility as a function of blocks summed together. There is no visible drop in the expectation value because the phase is varying very slowly. (b) Clearance value of the system left to drift, the clearance is constantly increasing due to no decrease in the expectation value as consequence of a low varying phase but the error is constantly decreasing with larger sums of blocks (c) LC Retarder, a drop in expectation value is present due to the observable varying phase, as more blocks are added together the expectation value should eventually average to 0 (d) Clearance of the LC Retarder case, there is a peak which corresponds to the situation where the error is sufficiently small while the value of the expectation value is still reasonably above the QKD threshold. (e) HWP induced phase drift, the expectation value drops below the threshold due to the quickly varying phase. (f) Clearance of the HWP tilt case, the clearance drops very rapidly due to the fast moving phase.

3.5 Conclusions an Outlook

The results in Sec. 3.4 indicate that the technique of using entangled photons to combat the birefringence induced by PM fibers is feasible for quantum information applications. Particularly in Sec. 3.4.3, it is shown that this technique is theoretically feasible for reference frame independent quantum key distribution and is able to obtain a potential keyrate of approximately 0.15 per coincidence. We also showed the feasibility of using entangled photons with polarization maintaining fibers.

Further investigation of this project would be to implement a higher rate entangled photon source to the system and perform proper QKD to an outdoor free-space link. This would only further solidify the argument that the protocol is feasible for satellite QKD. Future work could also be done to investigate whether the two PM fiber configuration discussed in Sec. 3.1.1 improves the robustness of the system. There is also still some room for more theoretical and experimental work, particularly on investigating the types of eavesdropping attacks that could potentially render this protocol insecure. The obvious methods would be to take advantage of the flawed implementation of the protocol. Nonetheless, the outlook for this particular implementation of polarization compensation using PM fibers and RFI QKD is particularly promising and is ready to be tested further towards being used in the larger QEYSsat system.

Chapter 4

Conclusion

In this thesis, I focused on developing polarization entangled photon sources for the use in free-space QKD. In Chap. 2, I characterized and attempted to implement a high brightness, narrow-band entangled photon source. The source used periodically poled materials in a waveguide configuration and had fibers pigtailed to either end of the waveguide for easy alignment. However, due to the intrinsic noise and multimode nature of the pump light in the pigtailed fibers caused a low signal to noise ratio, and the source is not usable for free-space QKD applications. Nonetheless, the source has the potential to be applied to other experiments and there is the invaluable information obtained through the thorough investigation of the fiber pigtailed waveguide-based entangled photon source.

The next experiment, presented in Chap. 3 demonstrated the feasibility of using polarization maintaining fibers with entangled photons. In addition, a reference frame independent QKD protocol concept using the PM fibers was also investigated and shown to be feasible. In doing this, we were able to provide a simple solution for the QEYSsat ground station to combat the birefringence rotational caused by the currently implemented single mode fibers. This has been shown to be feasible, particularly as a passive polarization compensation system that uses entanglement.

The next steps are to conduct further investigation of possibilities for bright entangled photon sources. One avenue that is promising is the use of shorter fibers. Another is to use birefringent fibers as the nonlinear material for pair generation. Nonetheless, once a suitable high brightness entangled photon source is produced, it can be implemented to conduct outdoor free-space quantum experiments. Further investigation of the PM fiber reference frame independent QKD system would include performing complete QKD to an outdoor free-space link. This would only further solidify the argument that the protocol is feasible for satellite QKD. In addition, the use of two PM fibers in each arm of the entangled

photon sources needs to be investigated further as this will have a clear path forward to implementation considering it can also be used with non-entangled single photons. The final steps would be full implementation of the PM fiber compensation method to the optical quantum ground station and testing of this system with a long distance free-space link.

References

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. OBrien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, 2010.

[2] S. P. Jordan, K. S. M. Lee, and J. Preskill, "Quantum algorithms for quantum field theories," *Science*, vol. 336, no. 6085, pp. 1130–1133, 2012.

[3] S. Jordan, K. S. M. Lee, and J. Preskill, "Quantum algorithms for fermionic quantum field theories," 04 2014.

[4] Warren, C, "Towards analog quantum simulations of dynamical gauge theories," Master's thesis, University of Waterloo, 2017.

[5] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, "Stable solid-state source of single photons," *Phys. Rev. Lett.*, vol. 85, no. 2, p. 290, 2000.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, (Bangalore, India), pp. 175–179, December 1984.

[8] W. Heisenberg, "Uber den anschaulichen inhalt der quanten theoretischen kinematik und mechanik," *Zeitschrift für Physik*, vol. 43, no. 3, pp. 172–198, 1927.

[9] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[10] D. Dieks, "Communication by epr devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, 1982.

[11] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information (cambridge series on information and the natural sciences)," 2010.

[12] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed energy-time entangled twin-photon source for quantum communication," *Phys. Rev. Lett.*, vol. 82, pp. 2594–2597, Mar 1999.

[13] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, "Distribution of time-bin entangled qubits over 50 km of optical fiber," *Phys. Rev. Lett.*, vol. 93, p. 180502, Oct 2004.

[14] "Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum," *Optics Communications*, vol. 260, no. 1, pp. 340 – 346, 2006.

[15] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Phys. Rev. Lett.*, vol. 113, p. 060503, Aug 2014.

[16] W. Commons, "File:sphere bloch.jpg — wikimedia commons, the free media repository," 2016.

[17] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*. Wiley-Interscience, second ed., 2007.

[18] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[19] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, pp. 3018–3021, Oct 1998.

[20] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[21] M. Curty, M. Lewenstein, and N. Lütkenhaus, "Entanglement as a precondition for secure quantum key distribution," *Phys. Rev. Lett.*, vol. 92, p. 217903, May 2004.

[22] R. Colbeck, "Quantum and relativistic protocols for secure multi-party computation," *arXiv preprint arXiv:0911.3814*, 2009.

[23] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, p. 140501, Sep 2014.

[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[25] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Phys. Rev. A*, vol. 92, p. 052339, Nov 2015.

[26] R. Gallager, "Low-density parity-check codes," *IRE Transactions on information theory*, vol. 8, no. 1, pp. 21–28, 1962.

[27] D. J. C. MacKay and R. M. Neal, "Near shannon limit performance of low density parity check codes," *Electronics Letters*, vol. 33, pp. 457–458, Mar 1997.

[28] O. Maroy, M. Gudmundsen, L. Lydersen, and J. Skaar, "Error estimation, error correction and verification in quantum key distribution," *IET Information Security*, vol. 8, pp. 277–282(5), September 2014.

[29] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT '93* (T. Helleseth, ed.), (Berlin, Heidelberg), pp. 410–423, Springer Berlin Heidelberg, 1994.

[30] J. L. Carter and M. N. Wegman, "Universal classes of hash functions (extended abstract)," in *Proceedings of the Ninth Annual ACM Symposium on Theory of Computing*, STOC '77, pp. 106–112, 1977.

[31] M. Varnham, D. Payne, R. Birch, and E. Tarbox, "Single-polarisation operation of highly birefringent bow-tie optical fibres," *Electronics Letters*, vol. 19, no. 7, pp. 246–247, 1983.

[32] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, "Robust polarization-based quantum key distribution over a collective-noise channel," *Phys. Rev. Lett.*, vol. 92, p. 017901, Jan 2004.

[33] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Efficient quantum key distribution over a collective noise channel," *Phys. Rev. A*, vol. 78, p. 022321, Aug 2008.

[34] "Quantum key distribution protocols with six-photon states against collective noise," *Optics Communications*, vol. 282, no. 20, pp. 4171 – 4174, 2009.

[35] A. Laing, V. Scarani, J. G. Rarity, and J. L. OBrien, "Reference-frame-independent quantum key distribution," *Phys. Rev. A*, vol. 82, no. 1, p. 012304, 2010.

[36] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.

[37] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, p. 30, 2017.

[38] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, "Airborne demonstration of a quantum key distribution receiver payload," *Quantum Science and Technology*, vol. 2, no. 2, p. 024009.

[39] QEYSsat. https://uwaterloo.ca/institute-for-quantum-computing/qeyssat, 2018.

[40] S. Rashleigh, "Origins and control of polarization effects in single-mode fibers," *Journal of Lightwave Technology*, vol. 1, no. 2, pp. 312–331, 1983.

[41] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, "Measurement of qubits," *Phys Rev A*, vol. 64, p. 052312, 2001.

[42] A. Dresden, "The fourteenth western meeting of the american mathematical society," *Bull. Amer. Math. Soc.*, pp. 385–396, 06.

[43] R. Jozsa, "Fidelity for mixed quantum states," *Journal of modern optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[44] M. B. Plenio and S. Virmani, "An introduction to entanglement measures," *arXiv preprint quant-ph/0504163*, 2005.

[45] W. K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," *Phys. Rev. Lett.*, vol. 80, no. 10, p. 2245, 1998.

[46] C. Pugh, B. Higgins, J. P. Bourgoin, R. Tannous, and T. Jennewein, "Towards quantum sensing with optical photons," tech. rep., University of Waterloo, 2017.

[47] C. C. Gerry, *Introductory quantum optics*. Cambridge, UK ; New York: Cambridge University Press, 2005.

[48] C. K. Hong and L. Mandel, "Theory of parametric frequency down conversion of light," *Phys. Rev. A*, vol. 31, pp. 2409–2418, Apr 1985.

[49] N. Quesada and J. E. Sipe, "Why you should not use the electric field to quantize in nonlinear optics," *Opt. Lett.*, vol. 42, pp. 3443–3446, Sep 2017.

[50] D. J. Griffiths, *Introduction to electrodynamics*. Englewood Cliffs, N.J.: Prentice-Hall, 1981.

[51] G. K. Kitaeva and A. N. Penin, "Spontaneous parametric down-conversion," *Journal of Experimental and Theoretical Physics Letters*, vol. 82, pp. 350–355, Sep 2005.

[52] M. M. Fejer, G. Magel, D. H. Jundt, and R. L. Byer, "Quasi-phase-matched second harmonic generation: tuning and tolerances," *IEEE Journal of Quantum Electronics*, vol. 28, no. 11, pp. 2631–2654, 1992.

[53] Hamel, D. R., "Realization of novel entangled photon sources using periodically poled materials," Master's thesis, University of Waterloo, 2010.

[54] M. Yamada, N. Nada, M. Saitoh, and K. Watanabe, "First-order quasi-phase matched LiNbO3 waveguide periodically poled by applying an external field for efficient blue second-harmonic generation," *Applied Physics Letters*, vol. 62, no. 5, pp. 435–436, 1993.

[55] Y. S., "Entangled biphoton source - property and preparation," *Reports on Progress in Physics*, vol. 66, no. 6, p. 1009.

[56] J. P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Huebel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, *et al.*, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics*, vol. 15, no. 2, p. 023006, 2013.

[57] M. D. Feit and J. A. Fleck, "Light propagation in graded-index optical fibers," *Applied optics*, vol. 17, no. 24, pp. 3990–3998, 1978.

[58] D. Marcuse and . Marcuse, Dietrich, *Theory of dielectric optical waveguides.* Quantum electronics–principles and applications, New York: Academic Press, 1974.

[59] J. Noda, K. Okamoto, and Y. Sasaki, "Polarization-maintaining fibers and their applications," *Journal of Lightwave Technology*, vol. 4, no. 8, pp. 1071–1089, 1986.

[60] R. Stolen, W. Pleibel, and J. Simpson, "High-birefringence optical fibers by preform deformation," *Journal of Lightwave Technology*, vol. 2, no. 5, pp. 639–641, 1984.

[61] T. Okoshi and K. Oyamada, "Single-polarisation single-mode optical fibre with refractive-index pits on both sides of core," *Electronics Letters*, vol. 16, no. 18, pp. 712–713, 1980.

[62] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. DeMicheli, D. B. Ostrowsky, and N. Gisin, "Ppln waveguide for quantum communication," *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, vol. 18, no. 2, pp. 155–160, 2002.

[63] P. Vergyris, F. Kaiser, E. Gouzien, G. Sauder, T. Lunghi, and S. Tanzilli, "Fully guided-wave photon pair source for quantum applications," *Quantum Science and Technology*, vol. 2, no. 2, p. 024007, 2017.

[64] Thorlabs. https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=10772, 2018.

[65] Vermeyden, L., "Fundamental tests of quantum mechanics using two-photon entanglement," Master's thesis, University of Waterloo, 2014.

[66] M. Karpiński, C. Radzewicz, and K. Banaszek, "Dispersion-based control of modal characteristics for parametric down-conversion in a multimode waveguide," *Optics Letters*, vol. 37, no. 5, pp. 878–880, 2012.

[67] P. J. Mosley, A. Christ, A. Eckstein, and C. Silberhorn, "Direct measurement of the spatial-spectral structure of waveguided parametric down-conversion," *Phys. Rev. Lett.*, vol. 103, no. 23, p. 233901, 2009.

[68] A. Amphawan, F. Payne, D. O'Brien, and N. Shah, "Derivation of an analytical expression for the power coupling coefficient for offset launch into multimode fiber," *Journal of Lightwave Technology*, vol. 28, no. 6, pp. 861–869, 2010.

[69] Thorlabs. https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_ID=343, 2018.

[70] D. Marcuse, "Curvature loss formula for optical fibers," *JOSA*, vol. 66, no. 3, pp. 216–220, 1976.

[71] C. D. Stacey, R. M. Jenkins, J. Banerji, and A. R. Davies, "Demonstration of fundamental mode only propagation in highly multimode fibre for high power edfas," *Optics communications*, vol. 269, no. 2, pp. 310–314, 2007.

[72] C. Antonelli, M. Shtaif, and M. Brodsky, "Sudden death of entanglement induced by polarization mode dispersion," *Phys. Rev. Lett.*, vol. 106, no. 8, p. 080404, 2011.

[73] A. V. Binterference with a multimode pump," *Phys. Rev. A*, vol. 63, p. 053801, Apr 2001.

[74] A. K. Jha, M. N. O'Sullivan, K. W. C. Chan, and R. W. Boyd, "Temporal coherence and indistinguishability in two-photon interference effects," *Phys. Rev. A*, vol. 77, p. 021801, Feb 2008.

[75] G. Kulkarni, P. Kumar, and A. K. Jha, "Transfer of temporal coherence in parametric down-conversion," *J. Opt. Soc. Am. B*, vol. 34, pp. 1637–1643, Aug 2017.

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

[77] M. Arsenijević, J. Jeknić-Dugić, and M. Dugić, "Generalized kraus operators for the one-qubit depolarizing quantum channel," *Brazilian Journal of Physics*, vol. 47, no. 3, pp. 339–349, 2017.

[78] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A*, vol. 76, p. 012307, Jul 2007.

[79] C. Erven, X. Ma, R. Laflamme, and G. Weihs, "Entangled quantum key distribution with a biased basis choice," *New Journal of Physics*, vol. 11, no. 4, p. 045025.

Appendix A

Further Notes of Sagnac Alignment

A.1 Pump spectra

This appendix is to be used in addition to the material provided in [65]. They provide very good alignment techniques and information that can be used when making an Sagnac entangled photon source.

The pump spectra has a major effect on the visibility of an entangled photon source, as can be seen in the following figures and plots. The spectra must contain a single Gaussian peak with no side peaks. These side peaks create a loss in visibility due to the ability to potentially frequency correlate and distinguish the path in which the photon traveled. This also plays a factor in the bandwidth of the source.

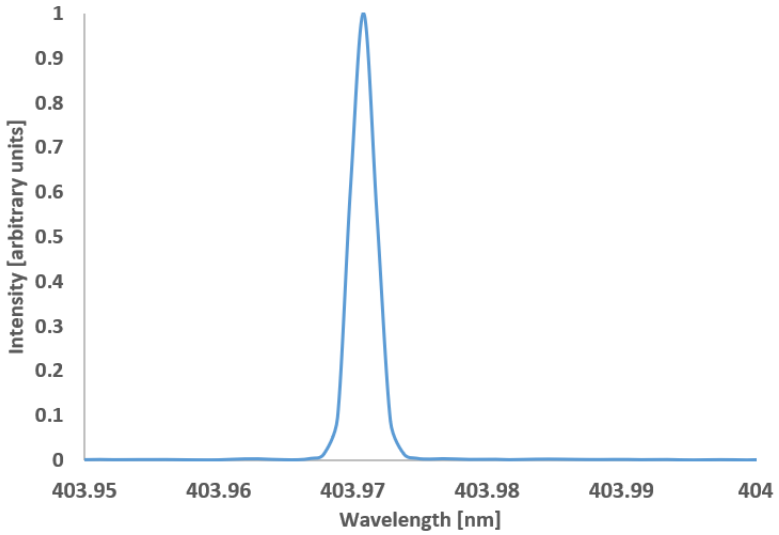


Figure A.1: Proper pumps Gaussian spectra that is critical for high visibility and entanglement purity.

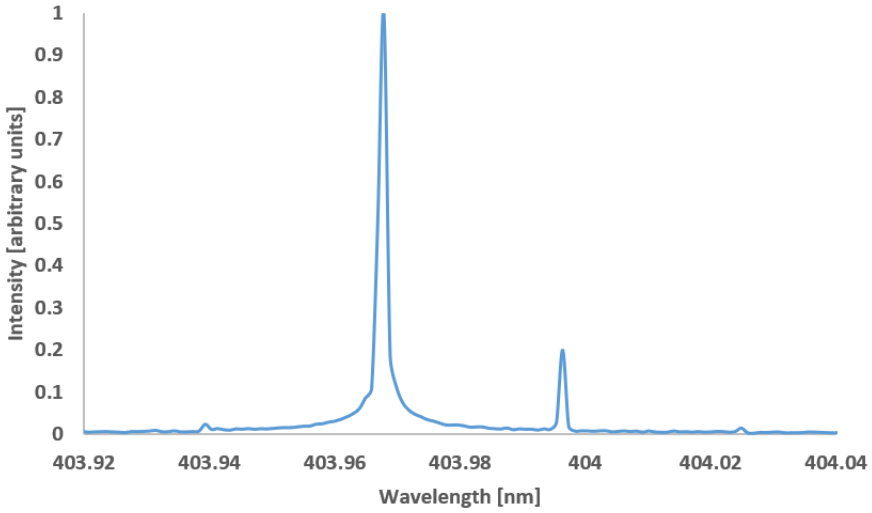
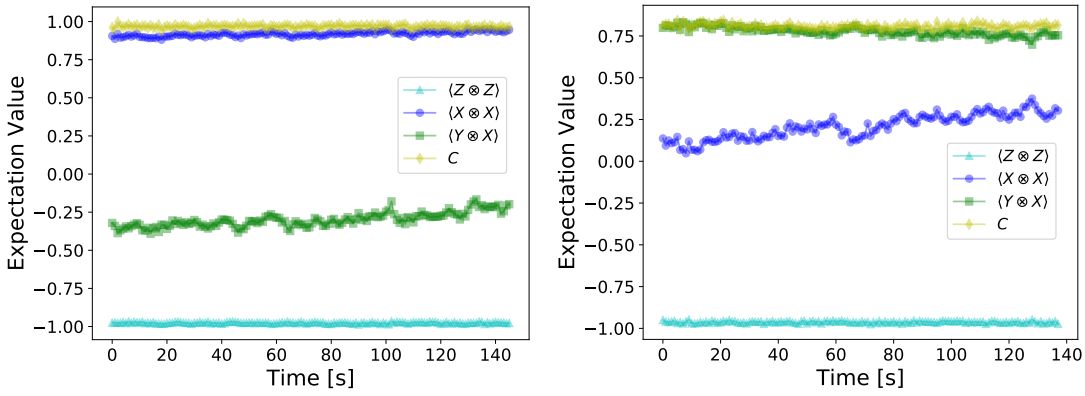


Figure A.2: Pump spectra that includes side peaks and causes a loss in visibility and entanglement purity.



(a) (b)

Figure A.3: (a) Results obtained using the pump spectra of Fig. A.1. (b) Results obtained using the pump spectra of Fig. A.2, it is apparent that there is a loss in entanglement quality because the C parameter has dropped to around 0.75 as opposed to ≈ 1 as in (a).

Given these results above, it is critical that the pump spectra be a definite single Gaussian peak. To ensure this, one should ideally have a pump pick off as seen in Fig. 3.3. This allows for a user to check and adjust the spectra accordingly before each data acquisition or alignment attempt.

Appendix B

Further Notes on C Parameter and Measurements of 3-2 Basis Protocol

The C parameter from Eq.(3.11) is used throughout our protocol as a measure of the entanglement quality and can be used to determine the level of information that an eavesdropper (Eve) has gained [35]. No formal security proof is given here, however, I will show some general calculations for the bounds of C.

B.1 Analysis for Pure States

For an entangled pure state we get, $C = 1$. This is true for all pure entangled states and is not dependent on any relative rotational phase similar to what we have in Eq.(3.1). We can show this by starting with a general pure state,

$$|\varphi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{B.1}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ and $\|\alpha\|^2 + \|\beta\|^2 + \|\gamma\|^2 + \|\delta\|^2 = 1$ is required for the normalization of the state. If we compute C we get,

$$C = \sqrt{4\|\alpha\|^2\|\delta\|^2 + 4\|\beta\|^2\|\gamma\|^2 + 8\|\alpha\|\|\beta\|\|\gamma\|\|\delta\|} \tag{B.2}$$

For any values of $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ satisfying the normalization condition and applied to our general state $|\varphi\rangle$, we get that $C \leq 1$. Only two special cases yield $C = 1$:

1. when $|\varphi\rangle$ is a maximally entangled state i.e. $\|\alpha\| = \|\delta\| = \frac{1}{\sqrt{2}}$ or $\|\beta\| = \|\gamma\| = \frac{1}{\sqrt{2}}$
2. when $|\varphi\rangle$ is completely depolarized or the identity i.e. $\|\alpha\| = \|\beta\| = \|\gamma\| = \|\delta\| = \frac{1}{2}$

while all other values of $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ yield the case of $C < 1$. The second case of $C = 1$ is problematic if we are limited to observing C since a completely depolarized state can be mistake to be maximally entangled. However, to combat this, one simply has to observe the expectation value of $\langle \rho(Z \otimes Z) \rangle$ and if $\langle \rho(Z \otimes Z) \rangle \neq 1$, then the state is not a maximally entangled state. Hence, ideally observing both C and $\langle \rho(Z \otimes Z) \rangle$ can verify whether or not Alice and Bob share a maximally entangled state.

B.1.1 Pure State with Relative Phase

The above analysis does not account for any rotational phase. Thus, if we apply a relative phase, i.e. the phase from Eq.(3.1) between horizontal and vertical polarizations, we get that

$$C = \sqrt{4\|\alpha\|^2\|\delta\|^2 + 4\|\beta\|^2\|\gamma\|^2 + 8\|\alpha\|\|\beta\|\|\gamma\|\|\delta\| \cos 2\phi} \tag{B.3}$$

for a maximally entangled state this again will give the value of $C = 1$. However, any other pure state that has $\|\alpha\|, \|\beta\|, \|\gamma\|, \|\delta\| < \frac{1}{\sqrt{2}}$ but still satisfying $\|\alpha\|^2 + \|\beta\|^2 + \|\gamma\|^2 + \|\delta\|^2 = 1$ will have $C \leq 1$ and C will vary with the relative phase. Thus Alice and Bob may use the value of C to determine whether or not the state is a maximally entangled state. An important result here is that the introduction of a relative phase eliminates the need to observe $\langle \rho(Z \otimes Z) \rangle$. Therefore, if Alice and Bob are able to guarantee a relative phase, they only need to monitor C to ensure the state they share is maximally entangled.

For our experimental implementation, we find that the calculated value of C is not always exactly $C = 1$. However, it is relatively close and most of the time within experimental error. For times when this is not the case, it can be attributed to a reduced visibility in the "diagonal" basis or quality of the entangled state which relates directly to the QBER in the "diagonal" basis given by Eq. (3.10). Without turning into a formal security proof, the value of C can help determine whether or not there is an eavesdropper since we can attribute a deviation from the maximally entangled state to Eve. The optimal value of $C = 1$ with $\langle Z \otimes Z \rangle = \pm 1$ indicates a maximally entangled state. While $C < 1$ indicates non maximally entangled state or some other problem.

Another interesting analysis is to see how the various parameters of the model in Eq. (3.9) effect the C parameter. If we take the density matrix in Eq. (3.9) and compute C we get:

$$C = \sqrt{4a^2\left(1 - a^2\right) vis_{DA}^2 \left(1 - p\right)^4}. \tag{B.4}$$

Recall that $0 \leq vis_{DA}, p \leq 1$, and that $\|a\| \leq 1$. Now any deviation from the perfect situation of $vis_{DA} = 1$, $p = 0$ and $\|a\| = \frac{1}{\sqrt{2}}$ will reduce the value of C.

B.2 Measurement Outcome in each basis

In the following section we will derive the measurement outcomes for each of the basis measurements that we get in the protocol. We will assume that there is no noise in the detectors and that the entangled state of the system is pure. We start with the state of Eq. (3.2) and apply it to the three possible joint measurements that Alice and Bob can make.

B.2.1 H/V basis

The H/V basis measurement is isomorphic to a Z spin measurement:

$$\langle Z \otimes Z \rangle = \mathrm{Tr}(\rho(Z \otimes Z)) \tag{B.5}$$

Now $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$ so applying Eq. (B.5) to the positive state of Eq. (3.2) we get,

$$\rho = |\Psi\rangle\langle\Psi|$$
$$= \frac{1}{2}\left(|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B + e^{-i\phi}|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B + e^{-i\phi}e^{i\phi}|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B + e^{i\phi}|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B\right)$$

so taking the dot product with the measurement and the trace we get the measurement results[1]

$$\langle Z \otimes Z \rangle = \mathrm{Tr}(\rho(Z \otimes Z))$$
$$= \mathrm{Tr}(\frac{1}{2}(|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B + e^{-i\phi}|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B$$
$$+|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B + e^{i\phi}|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B)(Z \otimes Z))$$
$$= \mathrm{Tr}(\frac{1}{2}(-|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B - e^{-i\phi}|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B$$
$$-|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B - e^{i\phi}|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B)$$
$$= -\frac{2}{2}$$
$$\langle Z \otimes Z \rangle = -1$$

[1] This is by no means the only approach to take. Another convenient approach is to write the state in terms of the Pauli matrices[11] and compute the various outcomes.

B.2.2 D/A basis

The D/A basis measurement is isomorphic to a X spin measurement:

$$\langle X \otimes X \rangle = \mathrm{Tr}(\rho(X \otimes X)) \tag{B.6}$$

Now $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$ so applying Eq. (B.6) to the positive state of Eq. (3.2) we get,

$$\begin{aligned}
\langle X \otimes X \rangle &= \mathrm{Tr}(\rho(X \otimes X)) \\
&= \mathrm{Tr}(\frac{1}{2}(|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B + e^{-i\phi}|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B \\
&+|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B + e^{i\phi}|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B)(X \otimes X)) \\
&= \mathrm{Tr}(\frac{1}{2}(|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B + e^{-i\phi}|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B \\
&+|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B + e^{i\phi}|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B)) \\
&= \frac{1}{2}\left(e^{-i\phi} + e^{i\phi}\right)
\end{aligned}$$

$$\langle X \otimes X \rangle = \cos(\phi) \tag{B.7}$$

B.2.3 Rotational basis

The R/L or rotational basis measurement is isomorphic to a Y spin measurement, however, Bob only has a 4-state analyzer and is thus unable to make a rotational measurement. Therefore Bob still makes a measurement in the diagonal basis, i.e. the basis that is not fixed:

$$\langle Y \otimes X \rangle = \mathrm{Tr}\left(\rho(Y \otimes X)\right) \tag{B.8}$$

Now $Y|0\rangle = i|1\rangle$ and $Y|1\rangle = -i|0\rangle$ so applying Eq. (B.8) to the positive state of Eq. (3.2) we get,

$$\begin{aligned}
\langle Y \otimes X \rangle &= \mathrm{Tr}\left(\rho(Y \otimes X)\right) \\
&= \mathrm{Tr}(\frac{1}{2}(|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B + e^{-i\phi}|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B \\
&+|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B + e^{i\phi}|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B)(Y \otimes X)) \\
&= \mathrm{Tr}(\frac{1}{2}(i|0\rangle_A|1\rangle_B\langle 1|_A\langle 0|_B + ie^{-i\phi}|1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B \\
&-i|1\rangle_A|0\rangle_B\langle 0|_A\langle 1|_B + -i^{i\phi}|0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B)) \\
&= \frac{1}{2}\left(ie^{-i\phi} - ie^{i\phi}\right)
\end{aligned}$$

$$\langle Y \otimes X \rangle = \sin(\phi) \tag{B.9}$$

B.2.4 C-parameter

If we now take the results of the expectation values in Eq. (B.7) and Eq. (B.9), we can calculate what to expect with the C-parameter for a noiseless system that implements the 6-4 state protocol.

$$\begin{aligned}
C &= \sqrt{\langle X \otimes X \rangle^2 + \langle Y \otimes X \rangle^2} \\
&= \sqrt{\cos\phi^2 + \sin\phi^2} \\
&= 1
\end{aligned}$$