5-2018

Toward Polarization Encoding Measurement-Device-Independent Quantum Key Distribution in Free-Space

Jeffrey Ivan Garcia
University of Tennessee, jgarcia1@vols.utk.edu

To the Graduate Council:

I am submitting herewith a thesis written by Jeffrey Ivan Garcia entitled "Toward Polarization Encoding Measurement-Device-Independent Quantum Key Distribution in Free-Space." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Physics.

George Siopsis, Major Professor

We have read this thesis and recommend its acceptance:

Raphael C. Pooser, Bing Qi

Accepted for the Council:
Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Toward Polarization Encoding Measurement-Device-Independent Quantum Key Distribution in Free-Space

A Thesis Presented for the
Master of Science
Degree
The University of Tennessee, Knoxville

Jeffrey Ivan Garcia
May 2018

Acknowledgements

To my parents and family for the endless support and encourage to reach milestones in my life. To them I am forever grateful.

I also would like to acknowledge the guidance of my advisor and our collaborating scientists to whom many insights were pivotal to moving forward in this endeavor. This project has also been generously supported by the U.S. Office of Naval Research under award number N00014-15-1-2646.

Abstract

Quantum Key Distribution (QKD) allows two trusted parties the ability to exchange a secret cryptographic key with unconditional security guaranteed by the fundamental laws of quantum mechanics. The transmission and measurement of sequences of quantum bits, or qubits, between two parties is the underlying mechanism in QKD. Security proofs, theoretically assume ideal single-photon sources and perfect single-photon detectors.

In practice, imperfections in the state preparation of qubits or those in single-photon detectors may be exploited to expose security loopholes. A relatively new protocol, Measurement-Device-Independent QKD (MDI-QKD), has been proposed which is immune to detector side-channel attacks, thus eliminating the need to have trusted single-photon detectors. However, in MDI-QKD near-perfect state preparation by the two parties is required to prove security in postprocessing.

This thesis outlines a proof-of-principle demonstration of polarization-encoded MDI-QKD using attenuated weak coherent pulses and investigate imperfections to the state preparation of qubits from certain parameters.

Table of Contents

1. Introduction

- **A. Background** 3
- **B. The BB84 Protocol** 5
- **C. BB84 Protocol Implementation** 7
- **D. Quantum Hacking and Security Vulnerabilities** 9
- **E. Measurement-Device-Independent QKD** 12
- **F. Hong-Ou-Mandel Interference** 15
- **G. Bell-State Measurements** 16

2. Experimental Setups 22

- **A. Experimental Instruments and Components** 22
- **B. Experimental Layout** 26
- **C. Polarization Encoding via the Polarization Modulator (Pol-M))** 28
- **D. Polarization Modulation calibration** 30
- **E. Instrument Control and Data Acquisition Integration within Matlab** 33
- **F. Technical Challenges** 34

3. Experimental Results 36

- **A. HOM Visibility** 36
- **B. Effects of Measurement Device Imperfections on HOM** 37
- **C. Effects of State Preparation Imperfections** 39
- **D. Bell State measurements** 40

4. Conclusions and Further Studies 42

Works Cited 44

Vita 47

List of Figures

Figure 1: The Bloch Sphere **4**

Figure 2: Bell State Measurement configuration with a 50/50 Beam-splitter and Polarizing Beam-splitter **15**

Figure 3: Experimental set-up of the HOM interference **27**

Figure 4: Polarization Modulator (Pol-M) schematic. **29**

Figure 5: Experimental setup for MDI-QKD **30**

Figure 6: Signature HOM dip corresponding to a count-rate approaching one-half of distinguishable photon pair coincidences **35**

Figure 7: Results of HOM vs DeadTime at 6MHz. **36**

Figure 8: HOM vs Polarization Angle **38**

Figure 9: Coincident count- rates for each case of input polarization states **39**

Chapter 1: Introduction

Quantum information science (QIS) is a relatively new field and area of active research that merges information theory with the laws of quantum mechanics. Exploiting the quantum properties of light at the single-photon level, information can be encoded into (and extracted from) the physical states of light.

Cryptography is the study of encoding and decoding information in a manner that is incomprehensible to third parties. This is usually implemented by the creation of a secret cryptographic key, which is a set of instructions for encoding and decoding a string of information. The strength of the encryption is usually proportional to the length of the key. The amount of information, or bits, stored in a key also influences the security. If a key is used that has the same length as the plain text, the key is referred to as a 'one-time pad'. If a one-time pad is used disposably, it has been proven impossible to decrypt [22]. The key generation process must be a process that is extremely difficult to guess and therefore usually involves random numbers. The second condition of traditional cryptography is the requirement that the transmission, or distribution, of the secret key between parties must be safeguarded from interception by a third-party. Should an eavesdropper intercept the key, it could potentially be copied cleanly without evidence of tampering. This was a so-called "key distribution problem". Later in the 1970's, public key distribution became prevalent using encryption algorithms that were based on complex calculations. The security of the key was reliant upon the length of the key as well as the difficulty in the computation. [21] In addition, the problem of an eavesdropper copying the key contents without detection remains.

Quantum Key Distribution (QKD) is the practice of two parties exchanging qubits with the aim of validating the successful transmission of information without tampering. Whereas in traditional algorithmic cryptography implemented today, such as the NSA's Secure Hash Algorithm, the security is dependent upon a computationally intensive mathematical problem which would require nearly unlimited combinational resources to decrypt. QKD is provably secure and guaranteed by the well-established laws of quantum mechanics.

In 1984, Bennett and Brassard first described a protocol for Quantum Key Distribution (QKD) that has since become known as the BB84 protocol [10]. This was the first such protocol proposed that could feasibly provide a provably-secure quantum encryption key. From this initial protocol, many subsequent clever QKD schemes have been proposed and experimentally implemented. Newer approaches proposed account for vulnerabilities to components (such as the detectors) of the distribution network. The latest and most promising is the relatively-new Measurement-Device-Independent (MDI-QKD) protocol. A key distinction of this protocol is the use of the well-known Hong-Ou-Mandel interference arising from indistinguishable photons interacting on a 50-50 beam-splitter[2]. Exploiting a time-reversed Einstein-Podolsky-Rosen QKD scheme, Charlie collects Bell-State Measurements on the strings of qubits then broadcasts the results publicly. Alice and Bob compare entanglement data to their own and verify the security based on their transmitted qubit data. The advantage over traditional QKD is the senders/receivers need not assume the measurement devices are secure [2]. Indeed, a necessary prerequisite for this protocol is near-perfect state preparation on behalf of Alice and Bob.[1] The following thesis outlines the state preparation optimization, detector characterization, and technical challenges needed to demonstrate a proof-of-principle MDI-QKD system.

A.) Background

The fundamental unit of quantum information processing (QIS) is the qubit, which is the quantum equivalent of the classical bit. A classical bit is always represented as one of two states: the $|0\rangle$ and $|1\rangle$ states (or as a 0 and 1). These states may be stored as two distinct voltage levels on a circuit. The quantum bit can exist as either of these two states, as well as a superposition of these two states. This superposition can be defined as a unit vector over a two-dimensional Hilbert space as:

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

Where the states

$$|0\rangle = \binom{1}{0}, |1\rangle = \binom{0}{1}$$

Span the Hilbert space $\mathcal{H}_2$, which is the computational basis. The values α and β represent probability amplitudes in the form of complex numbers and satisfy:

$$|\alpha|^2 + |\beta|^2 = 1$$

With $|\alpha|^2$ and $|\beta|^2$ the probabilities of the qubit to be in either the $|0\rangle$ or $|1\rangle$ state.

The key distinction of qubits from classical bits is that a qubit can take on values of 0, 1, or a superposition of both. The states $|0\rangle$ and $|1\rangle$ are computational basis states that form an orthonormal basis for the vector space [9].

We can also write equation 1.1 as:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Where θ and φ define a point on the surface of the Bloch sphere, which is depicted below in *figure 1*. All possible qubit states can be represented as a point on the surface of the sphere of radius 1. Qubits with equal probabilities of being in the $|0\rangle$ or $|1\rangle$ state lie on the equator.

It may appear that an infinite number of states exist on the surface of the Bloch sphere, however this assumption is incorrect when a measurement is performed on the qubit state. A measurement of the qubit state collapses the state of the qubit from its superposition of $|0\rangle$ and $|1\rangle$ to either $|0\rangle$ or $|1\rangle$ in whichever measurement basis it is conducted. This collapse of the superposition state is a fundamental postulate in quantum mechanics. The result is that a single measurement leads to a single bit of information of the qubit state. [9]

Using two photons in orthogonal polarization states, we can consider four possible states:

$$|0,0\rangle_{ab} \quad |0,1\rangle_{ab} \quad |1,0\rangle_{ab} \quad |1,1\rangle_{ab}$$

Now suppose this procedure is carried out for two pure states, $|\Psi\rangle$ and $|\varphi\rangle$.

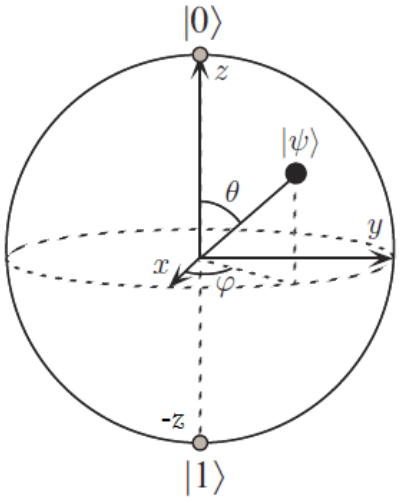

Figure 1: The Bloch Sphere

Due to the indistinguishability of photons in the $|0,1\rangle_{ab}$ and $|1,0\rangle_{ab}$ states, there are only three distinct states that can exist when considering two photons:

$$|2,0\rangle_{ab} \quad |0,2\rangle_{ab} \quad |1,1\rangle_{ab}$$

B.) The BB84 Protocol

Quantum Key Distribution is a protocol in which the security is proven according to the fundamental laws of quantum mechanics [16]. Two parties create qubits over a public channel, which may be not be secure, to produce a private key much like a classical private key. This is contingent upon the error rate of qubit communication is below a tolerable threshold. The underlying principle of QKD thus is the fundamental realization that an eavesdropper cannot acquire information from transmitted qubits without altering each qubit's state. This can be proven from two fundamental proofs resulting from the formulation of quantum mechanics: 1) the no-cloning theorem and 2) gaining information is possible only at the expense of introducing a disturbance to the measured state [16].

No-Cloning Theorem. Suppose we would like to create a quantum copying machine used to create an exact copy of an unknown pure quantum state, $|\Psi\rangle$, from a data slot, A. We assign slot B to be the target slot, to which the state from slot A will be copied. We assume slot B is also in a pure state, $|s\rangle$. The copy machine's initial state would be:

$$|\Psi\rangle \otimes |s\rangle$$

this initial state undergoes a unitary transformation of the form:

$$|\Psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\Psi\rangle \otimes |s\rangle) = |\Psi\rangle \otimes |\Psi\rangle$$

$$U(|\Psi\rangle \otimes |s\rangle) = |\Psi\rangle \otimes |\Psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Performing an inner product results in:

$$\langle\Psi|\varphi\rangle = (\langle\Psi|\varphi\rangle)^2$$

this result has two solutions: either $|\Psi\rangle = |\varphi\rangle$, or $|\Psi\rangle$ is orthogonal to $|\varphi\rangle$. This result means the copying machine can only clone orthogonal states [16]. Further studies have been performed questioning the possibility of cloning mix states, allowing imperfect copies tolerable under some threshold, and non-unitary copying machines [16]. As *Quantum Computation and Quantum Information* describes, "even if one allows non-unitary cloning devices, the cloning of non-orthogonal pure states remains impossible unless one is willing to tolerate a finite loss of fidelity in the copied states. Similar conclusions hold also for mixed states, although a somewhat more sophisticated approach is necessary to even define what is meant by the notion of cloning a mixed state" [16]. Thus, Eve cannot intercept the qubit without changing its state.

Information gain implies disturbance. Consider the following proposition: In any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing a disturbance to the states.

A proof: Allow $|\Psi\rangle$ and $|\varphi\rangle$ to be two *non-orthogonal* states in which Eve is attempting to intercept. We assume Eve uses an ancilla prepared in the state $|u\rangle$ to interact unitarily with either states $|\Psi\rangle$ and $|\varphi\rangle$ to obtain information. We assume the states are undisturbed. For each case:

$$|\Psi\rangle|u\rangle \rightarrow |\Psi\rangle|v\rangle$$

$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle|v'\rangle$$

Eve requires $|v\rangle$ and $|v'\rangle$ be different to acquire information about the state. We know inner products are preserved under unitary operations, such that:

$$\langle v|v'\rangle\langle\Psi|\varphi\rangle = \langle u|u\rangle\langle\Psi|\varphi\rangle$$

$$\langle v|v'\rangle = \langle u|u\rangle = 1$$

This implies $|v\rangle$ and $|v'\rangle$ are identical which also implies distinguishing between $|\Psi\rangle$ and $|\varphi\rangle$ must disturb one of the two states.

This intuitive result is used as a check on transmitted qubit states when Alice and Bob transmit non-orthogonal qubits. Alice and Bob can establish an upper bound on noise from state preparation or if any eavesdropping was occurring during qubit exchange. These nonorthogonal states are inserted randomly into the qubit stream such that the upper bound applies to data qubits as well. After information reconciliation and privacy amplification they sort a secret key from the total string.

C.) BB84 Protocol Implementation

Alice uses two conjugate bases (the z and x bases) to send Bob states in one of the following four prepared states:

$$|0\rangle_Z = |0\rangle$$

$$|1\rangle_Z = |1\rangle$$

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

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

Bob has two measurement bases, the rectilinear and the diagonal. Bob also randomizes his choice of measurement basis for each incoming pair of photons. After measuring all the qubits, Alice announces the bases she used for each pair via a classical communication channel. Only qubits measured in the agreeing basis are considered. This becomes known as the sifted key.[9] A portion of the sifted key is then compared by Alice and Bob. From the sifted key, and by comparing with their own known randomized states, each of Alice and Bob can estimate the rate of errors created during the transmission. If the error rate is higher than a predetermined threshold, the users abort communication until a secure connection can be established. [9]

In QKD, an eavesdropper is usually referred to as Eve who attempts to measure each pair of incoming photons. Should Eve measure a qubit, she forces a collapse of the qubit to either the $|0\rangle$ or $|1\rangle$ state. Eve is not able to make an exact copy of the qubit due to the no cloning theorem. [9]

Suppose Eve were to intercept an incoming photon. She randomly chooses a measurement basis. She records the measurement state and resends the state she measures to Bob. Inevitably evil introduce errors to the sequence of qubits. Suppose Eve chooses the same to measurement bases as Alice and Bob, about half the time she chooses the correct basis and the other half incorrect. When Alice chooses the correct basis, there is no measurement error introduced and all information can be obtained. The other times she chooses the incorrect basis

she projects the wrong state to Bob. [9] If Eve intercepts every photon in this way, she obtains half of the correct information while introducing 25% errors. Alice and Bob will then compare a significant portion of the transmitted qubits (which will not be used for the key itself) estimate the quantum bit error rate (QBER). [9] this error rate is the number of incorrectly transmitted qubits over the total number of trends qubits. Both Alice and Bob can statistically ascertain that an eavesdropper was present during the transmission. Thus, when an eavesdropper is detected, Alice and Bob will know the key is compromised and will not be used as their one-time pad.

D.) Quantum Hacking/Security Vulnerabilities

In practical implementation of QKD, the security of communication may contain vulnerabilities, or side-channels, that could be used to obtain information about the transmitted key without detection. Recent attacks developed target the imperfections in QKD setups, most commonly the single-photon detectors themselves. Eve also may attempt to attack the state preparation devices together some knowledge of the prepared states. However, state preparation can be under protective supervision without disturbance from an eavesdropper. Another reason the state preparation is less of a concern is that Alice/Bob can verify their transmitted qubits by randomly sampling a subset of the distributed key. It is therefore more likely the state preparation of qubits is well-characterized.

A more common quantum hacking approach is to exploit the detectors' imbalance in detection efficiency. One such attack is the detector blinding attack. In this scenario Eve saturates the receivers single-photon detector such that it no longer distinguishes single-photon pulses but instead stronger light pulses. Eve could essentially induce detections for each pulse

buy shining additional brighter pulses. [20) Other well-known attacks have been documented such as the photon-number splitting attack and an attack exploiting the dead time of the detectors. Photon number splitting attacks can occur when state preparation is not attenuated such that will photons have a reasonable probability of emission in each pulse.

Ideally, fully characterizing all devices to recognize potential side channel attacks is impractical in a real laboratory setting. [2] another proposed solution is a fully device-independent QKD set up which can be proved with Bell State inequality violations. This approach has been shown to be non-practical due to the need for near unity detection efficiency.

Quantum Bit Error Rate. The quantum bit error rate is defined simply as the ratio of wrong bits to the total number of transmitted bits. Converting from total number to a rate per unit time, it is explicitly:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{error}}{R_{sift} + R_{error}} \approx \frac{R_{error}}{R_{sift}}$$

Where R_{sift} or the bits in which Alice and Bob had the same basis choice. On average this is about one half therefore, the sifted key rate is half that of the raw key rate. The Rocky rate is the pulse repetition rate multiplied by the photon number for pulse times the probability of success or arrival to the detector times the probability a photon being detected (quantum efficiency).

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} q \cdot f_{rep} \cdot \mu \cdot t_{link} \cdot \eta$$

The factor q is introduced to correct for non-interfering combinations in phase coding systems. Their contributions to the error rate: the first is due to photons arriving at the wrong detector, the

second arises from dark counts detector, and the third arising from uncorrelated photons due to imperfect sources.

$$R_{opt} = R_{sift} \cdot p_{opt} = \frac{1}{2} q \cdot f_{rep} \cdot \mu \cdot t_{link} \cdot \eta \cdot p_{opt}$$

$$R_{det} = \frac{1}{2}\frac{1}{2} \cdot f_{rep} \cdot p_{dark} \cdot n$$

$$R_{acc} = \frac{1}{2}\frac{1}{2} \cdot f_{rep} \cdot p_{acc} \cdot t_{link} \cdot n \cdot \eta$$

The full QBER is now expressed as:

$$QBER = \frac{R_{opt} + R_{det} + R_{acc}}{R_{sift}}$$

$$= p_{opt} + \frac{p_{dark} \cdot n}{t_{link} \cdot n \cdot 2 \cdot q \cdot \mu} + \frac{p_{acc}}{2 \cdot q \cdot \mu}$$

$$= QBER_{opt} + QBER_{det} + QBER_{acc}$$

E.) Measurement-Device-Independent QKD

Although in principle, QKD is provably secure via statistical analysis based on the laws of quantum mechanics. [12] Statistically, the well-established laws of quantum mechanics manifests itself in the probabilistic outcomes of qubit measurements. But as is the case with realistic detectors and state preparation devices, real-world measurements do not completely comply with the theoretical predictions [10]. This lead to the development of attack schemes capitalizing on the imperfections of single-photon detectors, (SPDs) in particular [10]. Some groups have developed protocols which counteract these vulnerabilities in SPDs from detector side-channel attacks [2]. The first such protocol is known as Measurement-Device-Independent

QKD (MDI-QKD). This protocol is a modification of a time-reversed entanglement-based QKD [12].

In the proposed MDI-QKD protocol, Alice and Bob each send polarized, attenuated laser pulses to a third party, Charlie, who may or may not be a trusted party. The two have agreed to prepare their qubits in one of the four BBB84 polarization states. One measurement basis is defined by the polarizing axes of Charlie's polarizing beam-splitter (PBS). The two orthogonal states in this basis are aligned with Charlie's PBS outputs. In the second basis, they agree upon a third polarization state, referred to as the diagonal state. Alice and Bob must align their diagonal polarization before the randomized qubits are transmitted. Special consideration needs to be taken to align the diagonal basis such that HOM interference occurs at the 50-50 beam-splitter.

They now send Charlie a randomized sequence of the three polarizations to the input ports of his 50-50 beam-splitter. Charlie then has one of the outputs of the 50-50 BS sent to the input of his PBS. The outputs of the PBS (H and V) are sent to his two single-photon-detectors. Charlie performs Bell State Measurements (BSMs) using coincident events between his two detectors (within a certain time window). Charlie subsequently announces his BSM results publicly to Alice and Bob, who combine this information with their known, randomly-encoded polarization states to correlate the results. [2]

The underlying principle is based upon the time-reversed EPR-based QKD protocol [1]. Charlie is broadcasting entanglement events that occurred at the 50-50 beam-splitter. Since Alice and Bob can verify the entanglement events, the presence of an eavesdropper with complete control of the detection devices is inconsequential for this protocol [1]. Information about the key cannot be reconstructed without knowing the polarization states of Alice and Bob. [1]

Therefore, in this scheme, knowledge of the measurement devices is unnecessary, as well as the need to trust the security of the measurement devices. This proves reliably more secure over other QKD protocols [2].

Quantum Bit Error Rate in MDI-QKD. Modelling the errors: an implementation of MDI-QKD may involve various error sources such as the mode mismatch resulting in a non-perfect Hong-Ou-Mandel (HOM) interference. An important question to answer is how much the mismatch incoming photon pairs affects modes of MDI-QKD [5]. This leads to further investigations into the origin of the error rate. The purity of the state preparation must be characterized as well as the detector parameters. In most QKD setups, weak coherent pulses used in which single-photon contributions are estimated by the decoy-state protocol[2]. There is also limitation that QKD experiments are run in a fixed time, meaning the output key length is finite. This leads to the estimation of relevant parameters that suffer from statistical fluctuations[2]. This is the origin of the finite key effect[19]. Thus, a finite key analysis must be performed. From Kwong, Curty, et al. , their findings indicate polarization misalignment is the major source contributing to the QBER and mode mismatch.

The error bit rate in the rectilinear basis

$$E_Z = \frac{C_{HH} + C_{VV}}{C_{HH} + C_{VV} + C_{HV} + C_{VH}}$$

And the rate in the diagonal basis:

$$E_X = \frac{C_{DD}^{-} + C_{AA}^{-} + C_{DA}^{+} + C_{AD}^{+}}{C_{DD} + C_{AA} + C_{DA} + C_{AD}}$$

Where E_z is the QBER of Z- and E_x the QBER of X- basis. $C_{ij} = C_{ij}^{+} + C_{ij}^{-}$ is the coincidence count rate associated with $|\Psi^{\pm}\rangle$ and the *ij* subscripts are the encoding polarization states of Alice and Bob. Theoretical QBER for the Z-basis is 0% while for the X-basis, the expected rate is 25%.

Since weak coherent pulses are Poisson-distributed, the probability of two photons being sent by Alice as a vacuum pulses semi-Bob is half the probability of a single-photon being emitted simultaneously by each [19 qte]. This property of WCPs manifests itself in the diagonal basis causing 25% of $|\Psi^{-}\rangle$ events to occur when their polarizations are identical and 25% of $|\Psi^{+}\rangle$ events to occur when sending orthogonal polarizations. For identical polarization states (DD), 75% of $|\Psi^{+}\rangle$ events should occur while for the orthogonal states (AD), 25% of $|\Psi^{+}\rangle$ events should occur.

F.) The Hong-Ou-Mandel Interference

The interaction to consider is the input and output states of photons upon a 50/50 beamsplitter, depicted in *Figure 2*. Let the operators $a^{+}, b^{+}, c^{+}, d^{+}$ represent the creation of single photons in their respective ports. When two photons are incident in the two input ports (a and b), the beam-splitter input state can be written as:

$$|in\rangle = a^{+}b^{+}|0,0\rangle = |1,1\rangle_{ab}$$

Where $|0,0\rangle$ is the two-photon vacuum state for perfectly identical photons. A unitary

, symmetric beam splitter transformation can be described mathematically as:

$$B = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$

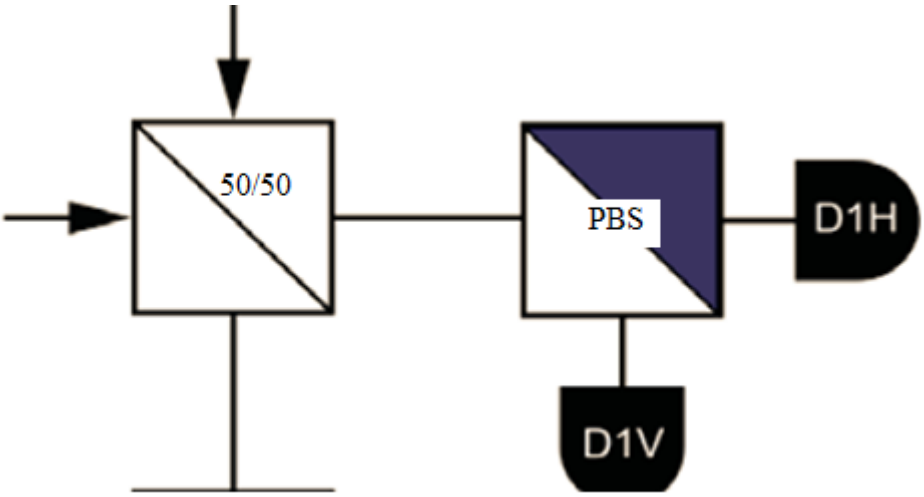

Figure 2: Bell State Measurement configuration with a 50/50 Beam-splitter and Polarizing Beam-splitter

After applying the beam-splitter transformation to this input state we have:

$$|out\rangle = \left(\frac{c^+ + id^+}{\sqrt{2}}\right)\left(\frac{ic^+ - d^+}{\sqrt{2}}\right)|0,0\rangle_{cd}$$

$$= \frac{1}{2}(c^+ + id^+)(ic^+ + d^+)\,|0,0\rangle_{cd}$$

$$= \frac{i}{2}(c^+c^+ + d^+d^+)\,|0,0\rangle_{cd}$$

$$= \frac{i}{2}\,(|2,0\rangle_{cd} + |0,2\rangle_{cd})$$

This indicates that the two photons will both appear in output port c or d. The cases where the photons each are reflected or transmitted are indistinguishable and, therefore, not observed. [11]

If we were to measure the coincident counts from the output of the beam-splitter with completely distinguishable photons, a certain coincident count-rate would be observed. This value would represent the case of minimally-entangled photons and, therefore, our maximum coincident count-rate. As the polarization state of the two incident photons become more indistinguishable, the coincident count-rate would drop and approach approximately the limit of one half of the original coincident count rate. When plotting the coincident count-rate as a function of polarization angle, we can see the well-known HOM dip first observed by Hong, Ou, and Mandel [11]. This effect is critical for the MDI-QKD protocol, since coincident events are dependent upon the projection onto the $|\Psi^+\rangle$ state.

G.) Bell-State Measurements

The Bell basis consists of four maximally entangled states. For rectilinear polarization, these states can be expressed as:

$$|\psi^{\pm}\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_X|1\rangle_X \pm |1\rangle_X|0\rangle_X)$$

$$|\Phi^{\pm}\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_X|0\rangle_X \pm |1\rangle_X|1\rangle_X)$$

Figure 3 depicts the configuration required a Bell State Measurement. HOM interference occurs at the first beam-splitter and thus the photons exit the same port. A coincidence detection on the detectors D1H and D1V indicate a successful projection to the $|\Psi^+\rangle$ state. For our setup, perform partial BSMs as the $|\Psi^+\rangle$ state is the only projection state we measure from the outputs of a single PBS.

To measure the outcome probabilities in different bases, a rotation of the polarization state functions is needed. For example, the following state

$$|*\rangle_X = \alpha|0\rangle_X + \beta|1\rangle_X$$

in basis X. We wish to express this state and the basisY, or $|*\rangle_Y$.

Defining X and Y as:

$$X = \{|0\rangle_X , |1\rangle_X \}$$
$$Y = \{|0\rangle_Y , |1\rangle_Y \}$$

For a rotation through an angle θ, the transformation from X to Y can be the be written as:

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}_{X,Y} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}_X = \begin{bmatrix} \gamma \\ \delta \end{bmatrix}_Y$$

And for

$$|*\rangle_Y = \gamma|0\rangle_Y + \delta|1\rangle_Y$$

Now we can write $|*\rangle_X$ in the Y basis as:

$$|*\rangle_X = (\alpha\cos\theta + \beta\sin\theta)|0\rangle_Y + (\beta\cos\theta - \alpha\sin\theta)|1\rangle_Y$$

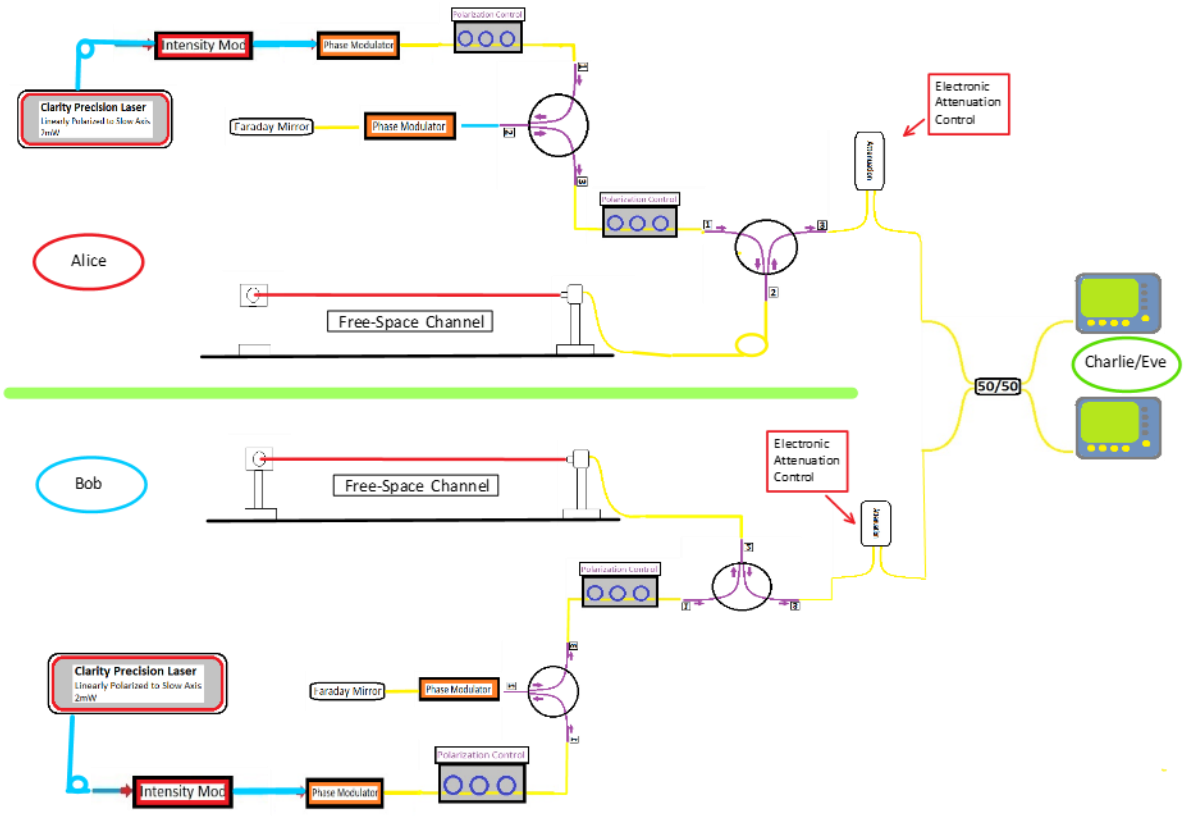

Figure 3: Experimental set-up of the HOM interference investigations.

Defining the Rectilinear basis $\oplus$, and the Diagonal basis $\otimes$:

$$\oplus = \{|H\rangle, |V\rangle\}$$

$$\otimes = \{|D\rangle, |A\rangle\}$$

Where $|D\rangle = |45°\rangle$ and $|A\rangle = |135°\rangle$. To make a measurement in the rectilinear basis $\oplus$ from a diagonal state, we set $\theta = -\pi/4$ and:

$$|D\rangle = \cos\left(\frac{-\pi}{4}\right)\left|H\right\rangle - \sin\left(\frac{-\pi}{4}\right)\left|V\right\rangle$$

$$= \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

Now we look at a two-photon state $|D\rangle|A\rangle$ which is not entangled, and express it in the $\oplus$ basis:

$$|D\rangle|A\rangle = \left[\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)\right]\left[\frac{1}{\sqrt{2}}(-|H\rangle + |V\rangle)\right]$$
$$= \frac{1}{2}(-|H\rangle|H\rangle + |H\rangle|V\rangle - |V\rangle|H\rangle + |V|V\rangle)$$

This expression indicates an equal probability of being measured in each of the four possible two-photon states in the $\oplus$ basis.

We can similarly define a transformation matrix for the two-photon states in the X basis to the Y basis. Defining W and V:

$$\mathrm{V} = \{|0\rangle_X|0\rangle_X, |0\rangle_X|1\rangle_X, |1\rangle_X|0\rangle_X, |1\rangle_X|1\rangle_X\}$$

$$\mathrm{W} = \{|0\rangle_Y|0\rangle_Y, |0\rangle_Y|1\rangle_Y, |1\rangle_Y|0\rangle_Y, |1\rangle_Y|1\rangle_Y\}$$

the transformation matrix becomes:

$$[T]_{\mathrm{V,W}} = \begin{bmatrix} cos^2\theta & sin\theta cos\theta & sin\theta cos\theta & sin^2\theta \\ -sin\theta cos\theta & cos^2\theta & -sin^2\theta & sin\theta cos\theta \\ -sin\theta cos\theta & -sin^2\theta & cos^2\theta & sin\theta cos\theta \\ sin^2\theta & -sin\theta cos\theta & -sin\theta cos\theta & cos^2\theta \end{bmatrix}$$

Now, we are interested in the maximally-entangled Bell states in the V basis

$$|\Phi^{\pm}\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_X|0\rangle_X \pm |1\rangle_X|1\rangle_X)$$

$$|\psi^{\pm}\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_X|1\rangle_X \pm |1\rangle_X|0\rangle_X)$$

Written in vector form, the states $|\psi^+\rangle_V$, $|\psi^-\rangle_V$, $|\Phi^+\rangle_V$, and $|\Phi^-\rangle_V$ become:

$$|\psi^+\rangle_V = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}_V \qquad |\psi^-\rangle_V = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}_V \quad |\Phi^+\rangle_V = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}_V \quad |\Phi^-\rangle_V = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\-1\end{bmatrix}_V$$

Projecting the W basis results in:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}_W, \frac{1}{\sqrt{2}}\begin{bmatrix}cos^2\theta - sin^2\theta\\-2sin\theta cos\theta\\-2sin\theta cos\theta\\sin^2\theta - cos^2\theta\end{bmatrix}_W, \frac{1}{\sqrt{2}}\begin{bmatrix}2sin\theta cos\theta\\cos^2\theta - sin^2\theta\\cos^2\theta - sin^2\theta\\-2sin\theta cos\theta\end{bmatrix}_W, \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}_W$$

To find the probability of each outcome, we square the above vectors. We are most interested in measuring a diagonally encoded Bell state in the $\oplus = \{|H\rangle, |V\rangle\}$ basis, with $\theta = -\pi/4$

$$|\Phi^+\rangle_\otimes = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}_\oplus \qquad |\Phi^-\rangle_\otimes = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\1\\0\end{bmatrix}_\oplus \quad |\psi^+\rangle_\otimes = \frac{1}{\sqrt{2}}\begin{bmatrix}-1\\0\\0\\1\end{bmatrix}_\oplus \quad |\psi^-\rangle_\otimes = \frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\\-1\\0\end{bmatrix}_\oplus$$

The last two are most relevant for our setup, especially the third. Since we are measuring in the rectilinear basis (defined by Charlie's polarization beam-splitter), we are interested in the result of measuring $|\psi^+\rangle_\otimes$ in Charlie's basis. Qubits initially in the $|\psi^+\rangle_\otimes$ state will exit the same port of the first 50-50 beam-splitter, due to the HOM interference, and both be diagonal to Charlie's measurement basis. Therefore, the coincident event would occur between Charlie's two detectors.

Four Cases of the Bell State Measurement (BSM). The four measurement cases for projections of the input states to the measurement basis of the single-photon detectors are described individually in the following four cases.

Case 1: Alice and Bob send identical polarizations in the rectilinear basis

Due to the HOM effect, incident identical photons exit through the same output port of the 50/50 Beam-Splitter(BS) and into the input port of the Polarizing Beam-Splitter (PBS). The result is non-detection between detectors D1H and D1V since the photons have identical polarizations (H or V). [6]

Case 2: Alice and Bob send Orthogonal polarizations in the rectilinear basis

In this case, the photon pairs exit the same output port of the 50/50 BS randomly one-fourth of the time. These photons will then be directed to the PBS where a coincidence detection would be detected due to the orthogonality of the photons. This results in a successful Bell-State Measurement (BSM) of the $|\Psi^+\rangle$ state. [6]

Case 3: Alice and Bob send identical polarizations in the diagonal basis

If the incident photons have identical polarizations in the diagonal basis, the photons will exit the same port of the 50/50 BS via the HOM interference. At the PBS, there is now a 50% probability the two photons will collapse to orthogonal $|H\rangle$, $|V\rangle$ states and a 50% probability of collapsing to identical polarization states. In this scenario, a successful BSM of the $|\Psi^+\rangle$ state occurs for half of incident photon pairs. [6]

Case 4: Alice and Bob send orthogonal polarizations in the diagonal basis

In this scenario, just as in case 2 above, the photons exit the same port of the 50/50 BS randomly. At the PBS, coincident detections are made, however, the results lead to indistinguishable results.

Chapter 2: Experimental setups

In this section, two experimental setups are described. The first setup was configured for investigations of the Hong-Ou-Mandel (HOM) interference and the effects of certain parameters on the HOM visibility. The other experimental layout was used to demonstrate a proof-of-principle MDI-QKD using weak coherent pulses (WCPs).

A.) Experimental Instruments and Components

I begin with a brief overview of instruments used in each experiment depicted in *figure 4* and *figure 5*. signal generators, single-photon avalanche detectors, and optical components.

The ID210 Single-Photon Avalanche Detector from Idquantique is the model used for all experiments presented here. Photodiodes are essentially photodetectors that convert detected photons into current signals. Avalanche photodiodes is composed of a semiconductor device capable of triggering avalanche multiplication utilizing the photo-electric effect. By setting a high reverse bias voltage, a current gain effect occurs internally due to the ionization caused from impinging photons. Commonly known as the avalanche effect. A higher gain is a result of a higher reverse voltage in most cases. For typical APDs, the reverse voltage is set below the breakdown voltage which prevents it from detecting individual photons. Our detector, the ID210 from Idquantique, is a "solid-state photodetector based on a reverse biased p-n junction in which a photo-generated carrier can trigger an avalanche correct due to the impact idolization mechanism." [21] An SPAD is like an APD in that it relies on an avalanche current (photo-triggered) of a reverse biased p-n junction to detect photons. The key distinction from APDs is that SPADs are designed to operate with a reverse bias below the breakdown voltage. [21]

Typically, the APD has a bias voltage above the breakdown voltage until a primary charge carrier is created. This is a meta-stable state in which a charge carrier causes the amplification to essentially become infinite such that the absorption of a single-photon causes a current pulse which can be detected by internal electronic circuitry. This current can damage the device if the current flowing is not quenched to reset the device. After specific time has elapsed, the bias voltage returns to its initial level above the breakdown voltage. The time that lapses between the quenching and the restoration is referred to as the dead-time. [21]

The efficiency of the SPAD is defined as the probability of detecting a photon that impinges on the photodiode. Two factors played into the probability: 1) the probability of photon reaches the InGaAs layer and 2) the probability a photon-induced primary charge carrier triggers an avalanche across the multiplication zone. [21] In general the detection efficiency increases with an increase of the excess bias voltage.

In addition to photons creating avalanches, charge carriers randomly generated from either thermal fluctuation, tunneling effects, or trapping processes in the junction may trigger an avalanche as well. These spontaneous events are referred to as *dark counts* and have an impact on the quantum efficiency of the detector. [21]

Another limitation to the performance of SPADs is the effect of *afterpulsing.* This occurs when charge carriers are trapped inside the high field region during an avalanche event. These trap charge carriers have a lifetime probability of a few microseconds. The probability of these events increases dramatically when the dead time is lower the longest lifetimes of trapped carriers. This value is typically below 5 μs.

For our experiments, we operated the detectors in gated mode which is when the bias voltage is set above the breakdown voltage for short time windows or gate windows. Only during these gate windows, will a detection occur. This operation mode mitigates the effects of spurious dark counts.

SPAD Detection Rate. Modeling the detector of efficiency, ε, as a virtual beam splitter of transmittance, ε, and an ideal detector, the detection probability is:

$$P = 1 - e^{-\varepsilon n}$$

Where n= |υ|^2 is the average photon number of the input beam. The average photon number is the average number of photons per pulse. For a single input arm, no interference occurs, and we can use Poisson probability distribution. The detection rate of the SPAD is given by:

$$R_d = P \cdot N_g$$

Where N_g is the effective gate rate (in Hz). The effective gate rate is the rate of true gates open for detection. The gating frequency is the rate of gate triggering ($1/T_g$). The effective gate rate is less than the gating frequency due to the deadtime (~9μs) applied after each detection. We can write N_g as:

$$N_g = \frac{1}{T_g} - R_d \frac{T_d}{T_g} + R_d$$

Therefore, the rate of detection becomes:

$$R_d = (1 - e^{-\varepsilon n}) \cdot \left(\frac{1}{T_g} - R_d \frac{T_d}{T_g} + R_d \right)$$

And we can solve for the average photon number:

$$n = |v|^2 = \frac{1}{\varepsilon} \ln\left(\frac{1 - R_d T_d + R_d T_g}{1 - R_d T_d}\right)$$

For our ID 210 SPADs, the efficiency setting we chose for all measurements was 10%. Of course, the true efficiency could differ slightly from this value.

ID Quantique Time-Interval-Analyzer (ID 810). The output of the detection signals from the ID210s are sent to a time interval analyzer. This device records incoming signals and assigns time tags for triggered events with resolution of 81ps. Each event is given a specific time tag recorded in integer bin numbers, each of bin size equal to 81ps. Software is included with the device enabling real-time plotting of detection rates, coincident events, data logging, as well as creating histograms. This device can be interfaced via a USB connection, which allows for command line control. A typical file output produces two columns the first of which logs events according to bin number and the second column with the input channel number.

Keysight Arbitrary Waveform Generator 33622A. The arbitrary waveform generator (AWG) used for modulating the polarization state in the Pol-M configuration was synchronized with the delay generator pulses at the phase modulator. Any waveform shape can be uploaded as well as several preset functions. For remote control, a basic model designed for Matlab's instrument control toolbox was modified from the basic version for full command-line functionality.

Stanford Research Systems Digital Delay Generator (DG645) – 'SRS'. This instrument generates the electronic modulation for the IM which produces the WCPs. It also provides the synchronous clock rate for all the major modulator signals and detection triggering. It is also our triggering signal for detection gates and synchronizing pulse events between instruments. The resolution of better than 10ps provides fine adjustment of pulse arrival times and shape profile

B.) Experimental Layout

We begin with a CW laser source (Clarity NLL-1550-LP) frequency-locked at 1550nm. A signal delay generator (Stanford Research Systems Digital Delay Generator DG645) sends electrical pulses at ~2ns FWHM to a $LiNbO_3$-based intensity modulator to produce weak coherent pulses at 1MHz. The output of which is directed to the polarization modulator (Pol-M) configuration which includes an optical circulator, phase modulator, and Faraday mirror. (The functionality of the polarization modulator is described in a subsequent section with a schematic diagram.) The output from the polarization modulator is sent to a second optical circulator which outputs the beam from the second output to the free space channel. The free-space channel consists of a collimating optical lens from the circulator and a 99% reflecting mirror which directs the beam back into the collimating lens to fiber-couple the light and through the third output of the optical circulator. The third output of this circulator is first sent to a manual variable attenuator for course attenuation, then subsequently a digital variable attenuator for fine attenuation control. The output of this attenuator is sent to a single-mode 50/50 beam-splitter. Each beam-splitter output pigtail is then connected to each of the two single photon detectors. The schematic of this setup is depicted in *figure 3.*

Polarization controller paddles (PCs) are placed before input 1 of the first circulator to deliver optical pulses into the phase modulator of the Pol-M at 45° polarization relative to the phase modulator's optical axis of maxima modulation (the slow-axis of the fiber). The phase modulator within the Pol-M schematic is modulated by an arbitrary waveform generator (Agilent 33622A) with electrical pulses of approximately 20ns at 1MHz. Electrical pulses from the AWG are matched in phase to the optical pulse with unattenuated light using an oscilloscope. The

instruments are matched in phase to the optical pulse with unattenuated light using an oscilloscope. The instruments are matched to the 10 MHz signal generated by the SRS delay generator. The SRS maintains a single clock rate for all instruments.

After the optical pulses and modulating pulses are synchronized, the intensity in each arm is first attenuated coarsely with the manual variable optical attenuator (VOA) to single-photon attenuation. We added an additional digital attenuator to fine-tune the detector count-rate (and photon number). The next step in the procedure is to synchronize the gating windows of the SPADs with the attenuated optical pulses. The SRS delay generator is used to send the gating signal to the SPADs with electrical pulses of 10ns width at 1MHz.

Initially, we had used the ‘external triggering’ setting for the SPADs, which left control of the gating window size to the SPAD electronics. We found the gating windows for each SPAD to be inconsistent with the user interface settings. We then transitioned to using the ‘free gating’ option, which allowed us to control the gating window size directly using the SRS. The gating functionality of the SPADs is preferred to limit the effects of dark counts. [21] A dead time of 10μs is used to limit the effects of after-pulsing in the SPADs.

Initially, we had used the ‘external triggering’ setting for the SPADs, which left control of the gating window size to the SPAD electronics. We found the gating windows for each SPAD to be inconsistent with the user interface settings. We then transitioned to using the ‘free gating’ option, which allowed us to control the gating window size directly using the SRS. The gating functionality of the SPADs is preferred to limit the effects of dark counts. [21] A dead time of 10μs is used to limit the effects of after-pulsing in the SPADs.

C.) Polarization Encoding via the Polarization Modulator (Pol-M)

In QKD, it is necessary to control the output states of the photons rapidly and in a controlled, predictable manner. The polarization encoding mechanism is a crucial component in MDI-QKD for delivering precise polarization orientations for both Alice and Bob. For instance, in the two-photon diagonal polarization state $|D\rangle|D\rangle$, both Alice and Bob must align their diagonal polarization states well enough to have consistent HOM interference on the 50-50 beam-splitter. This effect produces detectable photon pairs at Charlie's PBS, which is a successful BSM measurement of the $|\Psi^+\rangle$ projection. This modulation must also be at the repetition rate of 1 MHz. F*igure 4* depicts the polarization modulation scheme, Pol-M.

For the input to the phase modulator, we require the polarization angle to be 45° to the TE axis of the waveguide in the PM. We connect a PBS to output 2 of the circulator and use a polarization controller (PC) to adjust the polarization such that the PBS output intensities are equal. Input pulses pass through the PM and are reflected by the Faraday Mirror where they undergo a 90° rotation in polarization. They travel back through the PM and out port three of the circulator. An electrical pulse is applied to the PM that is synchronized with the optical pulse. In the waveguide, the TE and TM modes have differing modulation parameters for a given applied voltage. This creates a net phase difference between the TE and TM modes. The output state can be written as:

$$|\Psi\rangle = \frac{|TE\rangle + e^{i\Psi}|TM\rangle}{\sqrt{2}}$$

where Ψ is the phase difference added along the TE and TM directions [4]. Polarization states

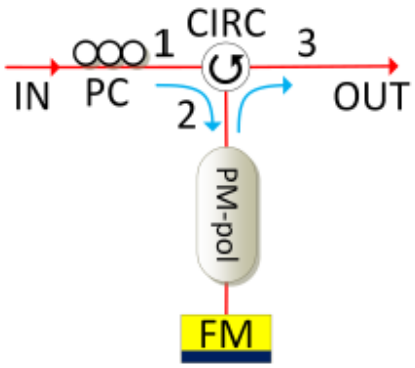

Figure 4: Polarization Modulator (Pol-M) schematic. The input is rotated by the first PC to 45° relative to the modulation axis of the phase modulator.

along the TE TM modes are represented by $|TE\rangle$ and $|TM\rangle$. The phase difference Ψ is a function of the voltage applied to the PM. For our PM (EO Space $LiNbO_3$ Phase Modulator) the V_π is 3.5V. By varying the peak voltage to the PM, the output polarization can be modulated.

D.) Polarization Modulation Calibration

To set the specific V_{pp} needed to set the polarization state to a given angle, a calibration of the V_{pp} was performed using the configuration in *Figure 5*.

The SRS sends electrical pulses to the intensity modulator (IM), which produces weak coherent pulses of width 2 ns at 1 MHz. A DC voltage generator is also connected to the IM to minimize the background CW intensity. The first polarization controller aligns these pulses to 45° relative to the modulation axis of the phase modulator. An electrical pulse of width 20 ns from the AWG is sent to the phase modulator and is synchronized with the weak coherent pulse from the intensity modulator. The SPADs are set two external triggering by the SRS with 10 ns gate widths. The efficiency is set to 10%. The gates are synchronized with the optical pulses and

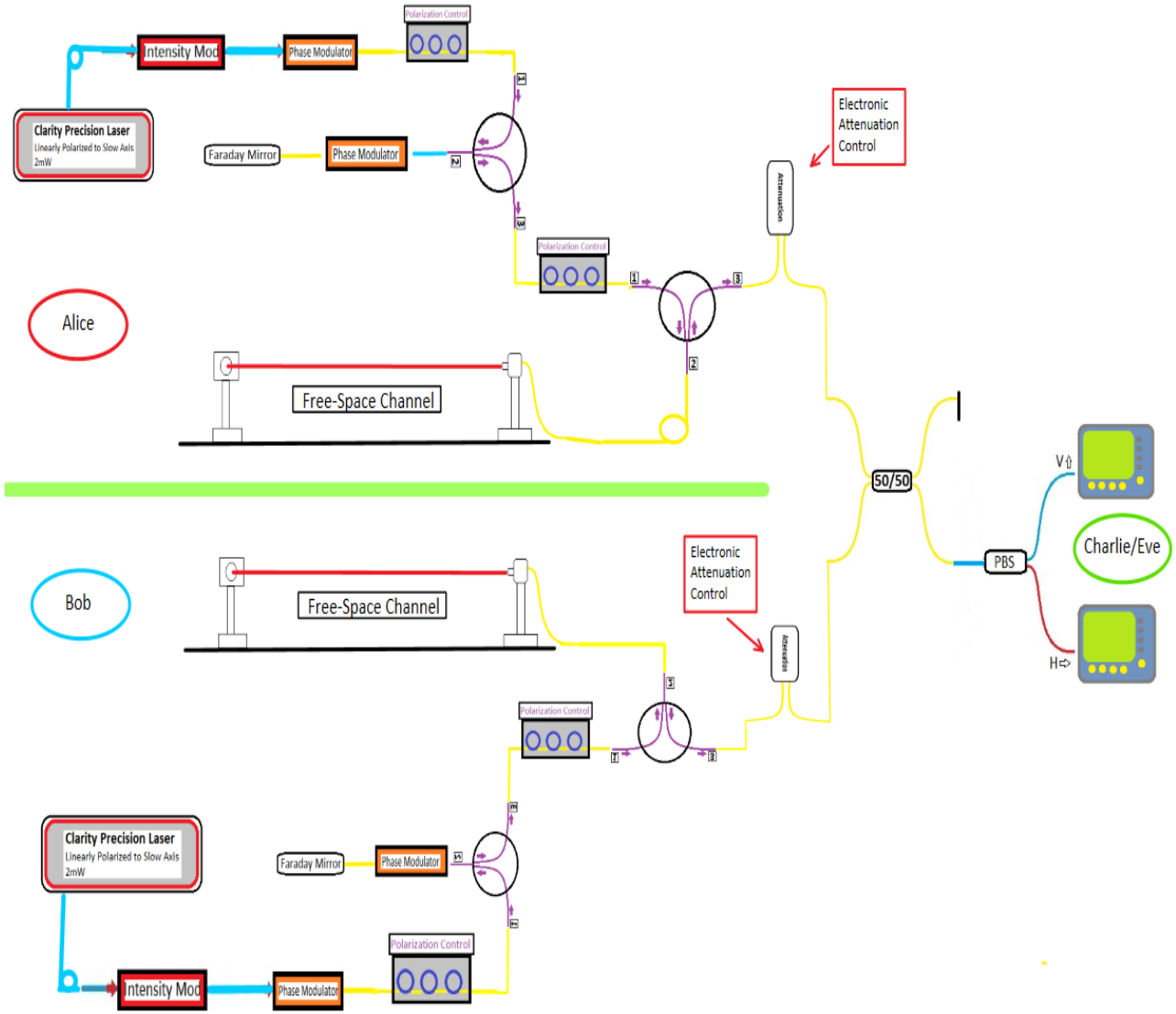

Figure 5 Experimental setup for MDI-QKD

The DC offset to the intensity modulator is adjusted to minimize photon counts not attributed to the pulse. We now use the second PC to align the pulses to the vertical PBS pigtail by adjusting state for a maximum count rate on that detector. We then increment the V_{pp} in increments of 0.1V on the AWG by command line argument from Matlab such that the count rate transitions from the detector 1 transitions to approximately the count rate from detector 2.

E.) Instrument Control and Data Acquisition Integration within Matlab

Early-on in the project, the need to control the various instruments remotely via command-line input was deemed useful in developing scripts that may automate tasks in state preparation and/or acquire data from instruments for analysis. I have written in a few instances where we have sent command-line arguments via Matlab, but here I describe a little further the extent to which we are able to control our instruments used in state preparation. This would include data acquisition from the oscilloscope, the timing interval analyzer (TIA), and querying values from instruments (such as SRS delays, AWG V_{pp}, digital attenuation levels, etc).

Matlab's Instrument Control Toolbox is an add-on package included that provides a seamless integration of instrument control into the workspace. There are several instrument control I/O APIs that are industry standard for several test and measurement companies. Two of which were used for our lab equipment specifically, Keysight and Tektronix. Each API has remote versions with standard libraries for communication over USB, LAN, GPIB, etc. A local-area-network was established in the laboratory to integrate communication with the Oscilloscope, AWGs, and SRS from a Matlab terminal. The custom API models for the individual instruments are stored in the shared Google folder. In addition to these, USB

communication was used for data acquisition from the Thorlabs PM100D energy meter console and control for an Arduino motor used to block the free-space channels of Alice and Bob independently.

Several functions for querying and setting specific parameters on the instruments were developed during this project that I do not mention here. I developed dozens of easy-to-use functions available for the instruments which could be used for easy scripting to perform certain routines such as one described below.

Eventually, implementation of a self-stabilizing state preparation feedback control could provide more continuous operation of key generation. Due to temperature fluctuations and other instabilities in the fiber, drifts in the polarization on the order of a few minutes to one hour occur. A feedback loop for monitoring and adjusting the un-modulated polarization state of Alice and Bob (for maintaining alignment of measurement bases) could provide a more continuous functionality of key generation.

F.) Technical Challenges

For a truly secure quantum key to be generated, the sequence of random polarization orientations for Alice and Bob must be calibrated and implemented into our QKD setup. The polarization orientations of $|H\rangle$, $|V\rangle$, and $|D\rangle$ are modulated by specific peak-to-peak voltages (V_{pp}) determined by the calibration procedure described above. Pulse waveforms are generated by uploading specific pulse shapes to the AWG in memory storage, which require waveforms of 1us in length at 1Gsps. The randomization comes a Matlab random number generating function to cycle the three waveform shapes 1 to 3, where each coincides to one of the three specific Vpp

separately for Alice and Bob. The maximum number of randomized pulses able to be uploaded successfully at the moment is roughly 10,000, using the full sample rate of 1 Gs/s. Other schemes for implementing the randomization have been proposed though we are exploring a more efficient data storage scheme for waveform data on the AWG, including reducing sample rates and utilizing binary as opposed to csv text files.

Chapter 3: Experimental Results

A.) The Hong-Ou-Mandel Visibility

For the HOM interference setup, we used the SRS to modulate the intensity modulator with ~4ns pulses which result in ~2ns weak coherent pulses from the IM. The SRS has resolution of ~10ps such that the leading-edge of pulses can be overlapped accurately with the WCPs from the other arm. The gating window on the SPADs are synchronized with the WCPs after matching the arrival times on the 50-50 beam-splitter. The polarization controller of one arm is adjusted to match the polarization state of the opposing arm. In the TIA software, we set a coincidence window of ~20ns and plot out coincident events between the detectors. We also independently match the count rate in each detector from each arm. In *Figure 6* we see the well-known signature HOM dip arising from matching polarization states on the beam-splitter. For WCPs, maximum HOM interference is indicated by a drop in the coincident event rate to one-half the count rate of completely distinguishable photons. For *Figure 6*, the coincident rate initially is ~825 cts/s then drops to ~410 cts/s. The figure serves as a visual aid when attempting to match the polarization states. We then record time tag events from the TIA and calculate quantitatively the coincident probability with HOM interference. This probability theoretically approaches 0.5 for WCPs. A Matlab script is used to calculate this probability using deadtime, pulse frequency, and coincidence window input parameters.

Typically, normalized HOM probabilities below 0.55 are reliably achievable. Approaching a probability of 0.52 involves further fine-tuning of the polarization paddle positions, but can be done relatively easily and consistently with some scrutiny. Below a

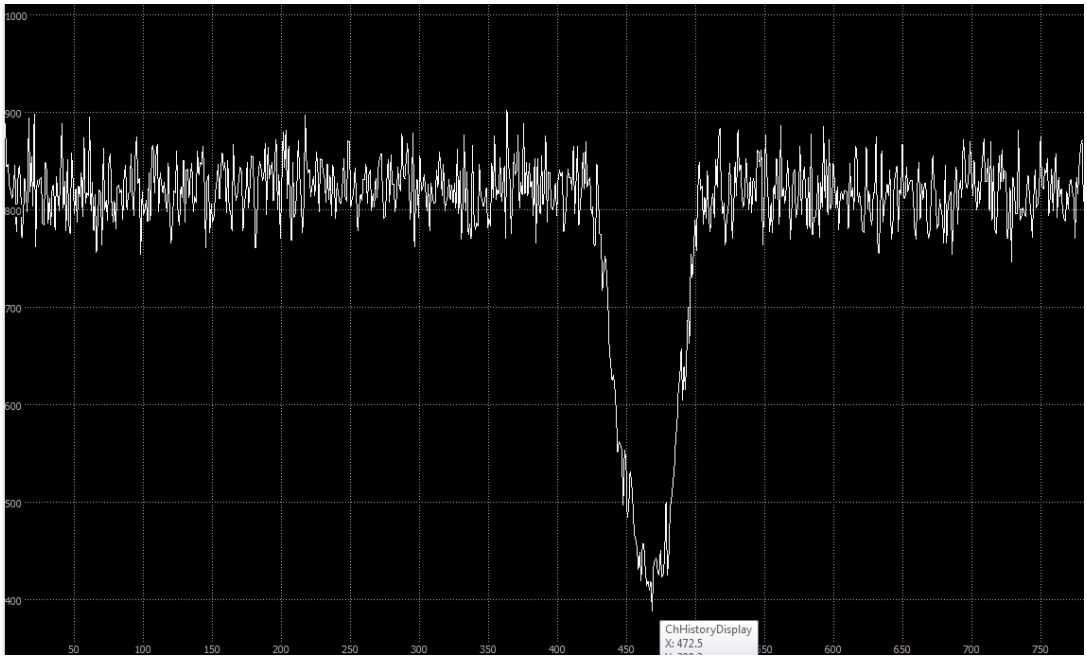

Figure 6: Signature HOM dip corresponding to a count-rate approaching one-half of distinguishable photon pair coincidences

probability of 0.52 more challenging and less reliable. However, values below 0.51 have been achieved on numerous occasions. We suspect the inconsistency of values below 0.51 is due to an unknown parameter that minimizes the indistinguishability of the incoming photon pairs at the beam-splitter.

We have also been to achieve HOM probabilities below 0.52 for the $|H\rangle$ and $|V\rangle$ polarization states using the Pol-M configuration independently for Alice and Bob.

B.) Effects of Measurement Device Imperfections on HOM

We investigated the effects of lowering the dead time values on the SPADs on the HOM probability. We used a pulse rate of 6 MHz for this study. As is shown on the plot in *figure 7*,

each data point is a calculation of the HOM probability versus the deadtime set on the SPAD. At higher deadtime values (above ~4μs), our HOM probabilities were approximately 0.52. The exponential rise of the HOM probability is apparent and coincides with an exponential model. Assuming the afterpulse probability can be fitted with an exponential of the form [22]:

$$P^{aft}(t) = P_o^{aft} e^{-bt}$$

Where P_o is the afterpulse probability at the minimal deadtime and b the decay constant. Here we have used $P_o = 0.005$ and b= 0.1, which were determined from an experimental fit. The data in *figure 7* was taken for a 6MHz pulse rate. The decreasing deadtime values set on the SPADs dramatically lowers the HOM visibility for when all other factors are constrained.

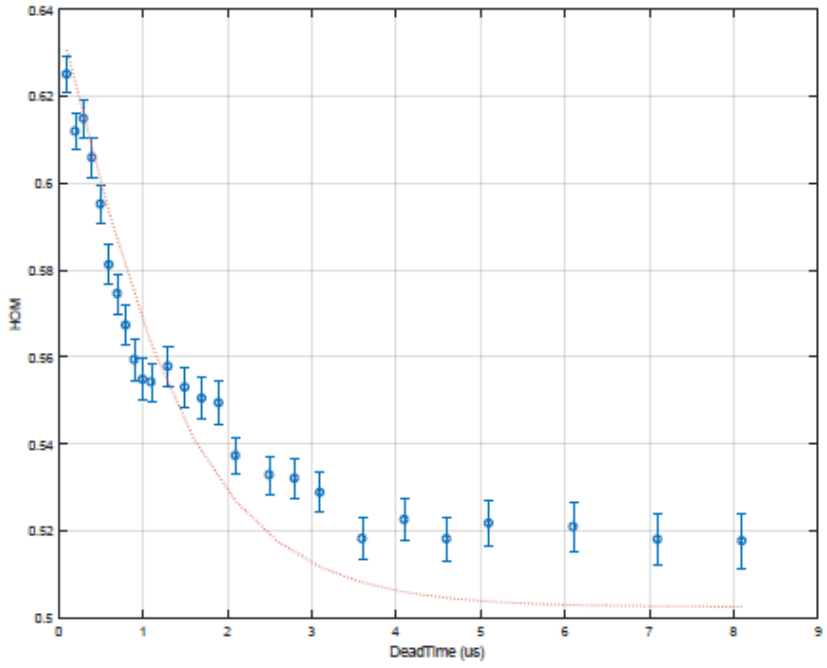

Figure 7: Results of HOM vs Dead-Time at 6MHz. Model depicted in red dashed plot

C.) Effects of State Preparation Imperfections

Polarization Input states. Using the calibrated voltage to the polarization angle values, *figure 8* plots the HOM probability versus polarization angle. The solid curve is predicted behavior. Note for these data points the HOM visibility approaches 0.52. Modeling the coincident probability as:

$$\hat{\epsilon}_1 = \frac{1}{\sqrt{2}}|TE\rangle + \frac{1}{\sqrt{2}}e^{\imath\phi_0}|TM\rangle$$

$$and$$

$$\hat{\epsilon}_2 = \frac{1}{\sqrt{2}}|TE\rangle + \frac{1}{\sqrt{2}}e^{\imath\phi_0}e^{\imath\phi_M}|TM\rangle$$

$$\bar{P}^{coin} = \frac{1}{2\pi}\int_0^{2\pi} d\Theta\left[1 - e^{-|\nu|^2}2\cosh\left(|\nu|^2\cos(\Theta)\right) + e^{-2|\nu|^2}\right]$$

$$\bar{P}'^{coin} = \left(1 - e^{-|\nu|^2}\right)^2$$

$$\cos\Phi = \sqrt{|\hat{\epsilon}_1 \cdot \hat{\epsilon}_2|^2} = \sqrt{\frac{1}{2}\left(1 + \cos\frac{V_g}{V_\pi}\pi\right)} = \cos\frac{V_g\pi}{2V_\pi}$$

We plot the expected line with calibrated polarization angle values using the Pol-M configuration described above. *Figure 8* plots the results of this expected relationship with the calibrated polarization state using the Pol-M.

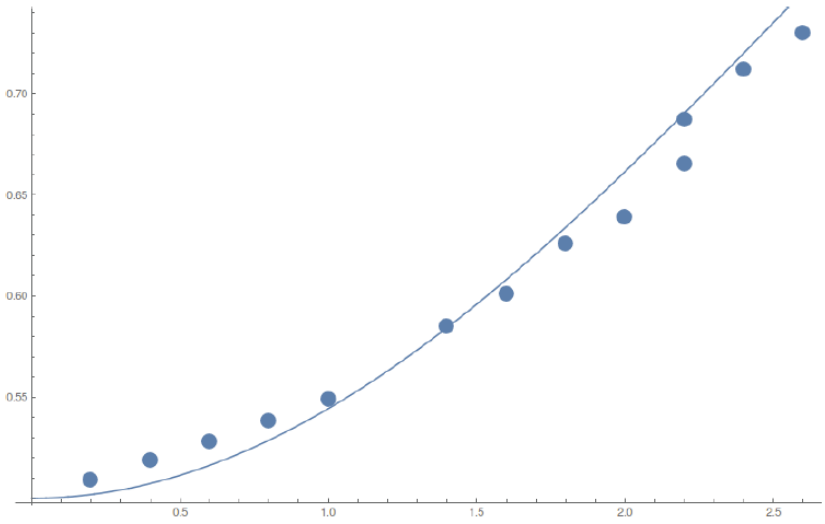

Figure 8: HOM vs Polarization Angle (calibrated polarization)

D.) Bell State measurements

The plot in *Figure9* depicts the coincident count rates for each combination of input states. The polarization states were altered via command line to the AWG instantaneously. For each combination of polarization states from Alice and Bob, the coincident count rate (coincidence window:250bins ~ 20ns). Each polarization state is held constant for 20 seconds, then altered digitally via command line input to the AWG. The Vpp for each Alice/Bob's polarization state is calibrated previously to three specific values corresponding to Vertical, Horizontal, and Diagonal polarizations. The sequence of polarizations was the following:

AV-BV, AV-BD, AV-BH, AD-BV, AD-BD, AD-BH, AH-BV, AH-BD, AH-BH

where AV = "Alice Vertical", BD = "Bob Diagonal", etc.

The anticipated coincident rates for the prepared states coincide with the expected probabilities for the given input states. We can see that Alice and Bob have the rectilinear bases aligned properly and a rotation of polarization from the Pol-M for each result in the anticipated coincident rate at Charlie's PBS.

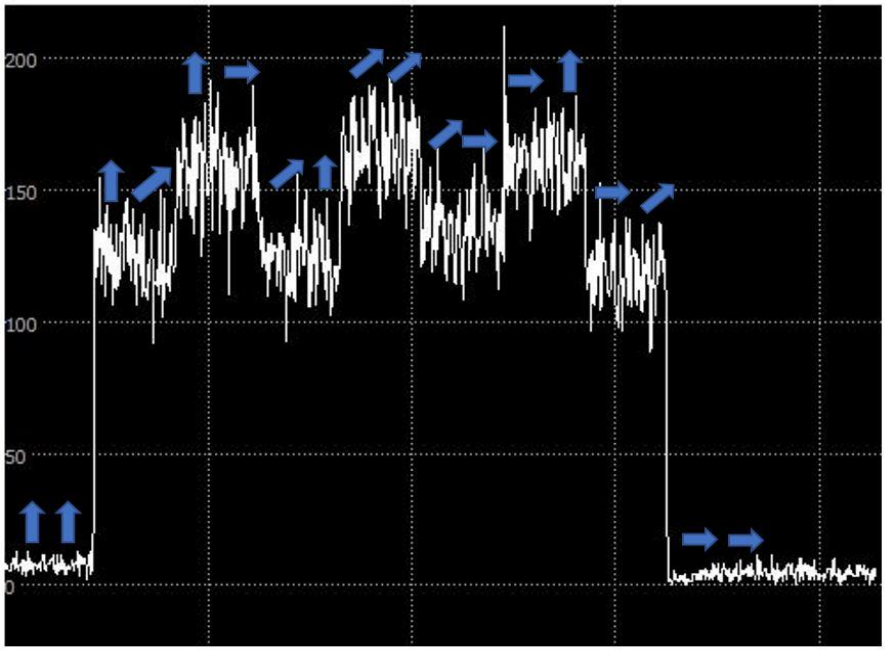

Figure 9: Coincident count- rates for each case of input polarization states

Chapter 4: Conclusions and Further Studies

At this juncture in the experiment, the most immediate obstacle we have is implementing polarization randomization at 1 MHz repetition in an efficient manner for the AWG. The challenge is creating a random sequence long enough to create enough coincidences for a significant quantum bit rate. Currently we can create "slow keys" which are a sequence of command-line arguments altering the polarization state in 100ms intervals. Each state is then held constant for 100ms to attain at least one coincidence per state. Furthermore, quantum bit error rates (QBER) would need to be calculated post-measurement.

At higher rates, a key sifting analysis would need to be performed to correlate detection events with specific polarization orientations at 1 MHz. This this has proved more challenging than initially conceived. One proposed solution is to send bursts of a known number of pulses (and polarization states) that also trigger the triggering of the gates on the detectors. This would make for easier synchronization of detection events to polarization states. A second solution is to send marker signals to the TIA at regular intervals that will serve as a clock for the randomized pulses. At 1 MHz, and with detection efficiency of 10%, we calculate we will have roughly one coincident detection for every 1,000 pulses. Sharing a significant number of qubits between Alice and Bob, about 1000 bits, would require $1x10^6$ pulse waveforms. At the time writing, we first create entire waveform shapes that span 1μs using the full sample rate of 1Gs/s. This means $1x10^9$ data points for each waveform. From the described proposal of 1,000 successful qubit detections, the files would contain a number samples (and file size) to be efficiently stored as csv text file on the AWG. Thus, this specific technical hurdle, as well as the sifting needed post

measurement, is the limiting factor in a creating a true randomized quantum key, using the MDI-QKD protocol.

Beyond the full MDI-QKD implementation, we still look towards extending our free-space quantum channel. We currently have limited a free space channel of about 1 m. This is mostly treated to our limited lab size. Coupling our free space channel over large distances will require construction of custom telescopes designed for our intended use. Eventually, the effects of atmospheric dispersion on key generation and bit error rate are intended to be study over larger free space channels.

Beyond that, a reconfigurable QKD network still needs to be implemented. Intentions would be to implement a synthesis of our nearly-realized MDI-QKD system with a the more efficient decoy state BB84 QKD protocol. We would need to investigate implementation of other decoy states, which are random pulses of a variant photon number, into the encoded pulses.

Works Cited

[1] Tang, Zhiyuan, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. "Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution." *Phys. Rev. Lett*. 112, 190503 (2014).

[2] H.-K. Lo, M. Cury and B. Qi, "Measurement Device Independent Quantum Key Distribution", *Phys. Rev. Lett.*, 108, 130503 (2012).

[3] Roberts, G.L., M. Lucamarini, Z. L. Yuan, J.F. Dynes, L. C. Comandar, A. W, Sharpe, A.J. Shields, M. Curty, I.V. Puthoor, and E. Andersson. "Experimental measurement-device-independent quantum digital signatures." *Nature Communications* 8, 1098 (2017).

[4] Zhiyuan Tang, Kejin Wei, Olinka Bedroya, Li Qian, and Hoi-Kwong Lo. "Experimental measurement-device-independent Quantum Key Distribution with Imperfect Sources" *Phys. Rev. A* 93, 042308.

[5] V.R.R. Valivarthi, P. Chan, I. Lucio-Martinez, D. Korchinski, C. Duffin, J.A. Slater and W. Tittel. "Measurement-Device-Independent Quantum Key Distribution with ID210 Detectors." *IDQuantique.* March 2014, https://www.idquantique.com/wordpress/wp-content/uploads/app_note_MDI-QKD.pdf

[6] M.B. Russell, L.O. Mailloux, D.D. Hodson, M.R. Grimaila. "A Bell State Analyzer Model for Measurement-Device-Independent Quantum Key Distribution." *Intn'l Conf. Scientific Computing*,

[7] Bourgoin, Jean-Philippe, Nikolay Gigov, Higgins, Yan, Meyer-Scott, Khandani, Lutkenhaus, Jennewein. "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations." *Phys. Rev. A* 92, 052339 (2015)

[8] Lucio-Martinez, I., P. Chan, X. Mo, S. Hosier, and W. Tittel. "Proof-of-concept of Real-World Quantum Key Distribution with Quantum Frames". *New J. Phys.* 11 095001.

[9] Lo, Hoi-Kwong, Marcos Curty, and Kiyoshi Tamaki. "Secure Quantum Key Distribution". *Nature Photonics* 8, 595-604 (2014).

[10] Bennett, C. H. and G. Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing." IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179,1984.

[11] Hong, C. K. , Z. Y. Ou, and L. Mandel. "Measurement of Sub-Picosecond Time Intervals between two Photons by Interference." *Phys. Rev. Lett.*, vol. 59, no. 18, pp. 2044-2046, 1987.

[12] Valivarthi, Raju, Itzel Lucio-Martinez, Philip Chan, Allison Rubenok, Caleb John, Daniel Korchinski, Cooper Duffin et al. "Measurement-Device-Independent Quantum Key Distribution: From Idea Towards Application." *Journal of Modern Optics* 62, 1141-1150 (2015).

[13] Xu, Feihu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo, "Practical Aspects of Measurement-Device-Independent Quantum Key Distribution." *New J. Phys*. 15 113007 (2013).

[14] Xu, Feihu, Bing Qi, Zhonga Liao, and Hoi-Kwong Lo. "Long Distance Measurement-Device-Independent Quantum Key Distribution with Entangled Photon Sources." *Appl. Phys. Lett*. 103, 061101 (2013).

[15] Shor, Peter W., and John Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol." *Phys. Rev. Lett.* 85, 441.

[16] Nielsen, Michael A., and Chuang, Isaac L. *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press, 2016.

[17] K. Ekert. "Quantum Cryptography Based on Bell's Theorem." *Phys. Rev.Lett.* 67, 661 (1991).

[18] Biham, Eli, Bruno Huttner, and Tal Mor. "Quantum Cryptographic Network Based on Quantum Memories." *Phys. Rev. A* 54, 2651 (1996).

[19] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der WeidPhys. "Proof of principle demonstration of Measurement-Device-Independent Quantum Key Distribution using Polarization Qubits." *Phys. Rev.* A 88, 052303 (2013).

[20] Ma, Xiongfeng. "Quantum Cryptography: From Theory to Practice." Doctor of Philosophy Thesis, University of Toronto, 2008.

[21] Idquantique ID210 Infrared single-photon detector brochure.

[22] Chao Wang, Fang-Xiang Wang, Hua Chen, Shuang Wang, Wei Chen, Zhen-Qiang Yin, De-Yong He, Guang-Can Guo, and Zheng-Fu Han. "Realistic Device Imperfections Affect the Performance of Hong-Ou-Mandel Interference with Weak Coherent States." *J. Lightwave Technol.* 35, 4996-5002 (2017).

Vita

Jeffrey Iván Garcia was born in Los Angeles, California in 1986, the son of Javier and Socorro Maria Garcia. His family relocated to west Tennessee when Jeff was four, where he grew up in Brownsville, TN through his high school years. At Haywood High, Jeff was active in several extracurriculars including the mock trial team, varsity soccer, academic decathlon, state mathematics competitions, and school musical productions. He completed high school in the top ten percent of his class academically and received an offer to attend Vanderbilt University in Nashville, TN

Jeffrey matriculated at Vanderbilt in the fall of 2004, where he majored in Physics and had active roles in the department with positions as an undergraduate teaching assistant and as a research assistant in the Applied Optical Physics and Nuclear Physics groups.

After his undergraduate studies, Jeffrey joined the LIGO Scientific Collaboration as an operations specialist at the Hanford Observatory in Washington state. During his time at LIGO, he was part of a team keeping optimal performance of the interferometer for the final run of the first-generation detector. His subsequent years were involved with the numerous upgrades to the detector to the now-running Advanced LIGO interferometer. In February 2015, the observatory announced the first direct detection of gravitational waves simultaneously at the detectors in Washington state and Louisiana. The discovery lead to subsequently lead to three of its founders awarded the 2017 Nobel Prize in Physics.

Jeffrey enrolled at the University of Tennessee in 2014 for graduate studies in Physics. He anticipates completing a Master's Degree with a Quantum Information Science concentration