Measurement Device Independent Quantum Key Distribution (MDI-QKD)

Joseph Gross, Jack Rich, Adrian Anaemeje, Kate Arutyunova
MIT Department of Electrical Engineering and Computer Science

Abstract
Quantum Key Distribution (QKD) is a secure communication method that, in principle, has its security rooted in the laws of quantum physics [1]. In reality, this unconditional security only holds under certain assumptions about the physical measurement setup—some which are not realistic with our today's technology. Conventional quantum key distribution (QKD) relies on the assumption that the quantum measurement devices used in the communication protocol are trustworthy while quantum source devices are well-characterized [2]. However, this assumption can be easily compromised by an attacker, raising concerns about the security of conventional QKD protocol. To address this issue, one solution is to use Measurement-Device-Independent (MDI) QKD, which provides additional security measures by testing Bell's inequality [3]. The novel protocol can enhance the security of conventional QKD against device imperfections and vulnerabilities, both known and unknown. MDI QKD can prevent an attacker from accessing any information about the transmitted quantum signals and compromising the security of the protocol.

In this project, we introduce a setup for measurement device independent quantum key distribution enabling two parties, a sender ("Alice") and a recipient ("Bob"), to generate a secret key with complete security, even if their equipment for measuring or detecting signals has been tampered with by an untrusted third-party observer and therefore cannot be relied on. We implement Measurement-device-independent quantum key distribution (MDI-QKD) protocol that was proposed to remove all the detector side channel attacks. This can be set up and implemented with standard optical components in the lab to display the ability to truly achieve the desired security. Implementing MDI QKD provides (1) additional security measures to enhance the security of traditional QKD against potential attacks that exploit device imperfections and vulnerabilities, and (2) potential to extend the distance of secure communication over optical fiber networks. One potential direction for future work is to demonstrate MDI QKD via secure distributed Machine Learning computation model. Later, the next step would be to use numerical estimation (QuTip Monte Carlo Solver) to evaluate the effectiveness of the proposed ML model.

Contents

1 Introduction

Cryptography is the practice for secure communication techniques that allow only the sender and intended recipient of a message to access its contents in the public environment. Cryptography is primarily based on encryption algorithms that convert plaintext to ciphertext and decryption algorithms that convert ciphertext back to the original plaintext.

Conventional symmetric cryptographic algorithms rely solely on the secrecy of an encryption key composed of a long random string of secret bits. If the sender and recipient share the same key, they can achieve unconditional security in their communication by using the standard one-time-pad encryption scheme. However, the primary issue with this protocol is the distribution of keys to both parties while ensuring that no one else has access to them. Unfortunately, methods of key distribution based on classical physics are insecure: there is nothing in classical physics that prevents an eavesdropper from copying the key during its transit from sender to receiver. As a result, quantum cryptography was proposed and developed to overcome those security issues inherent in conventional cryptography protocols.

1.1 Motivation

Quantum cryptography or Quantum Key Distribution (QKD) offers a secure communication methods for key distribution by relying on principles of quantum physics. Due to quantum non-cloning theorem, it is impossible for an eavesdropper to create a copy of quantum signals sent in a QKD secret key generation process and, therefore, know secret key. Generally, quantum cryptography ensures that no third-party intervention in the key-generating process can be detected.

BB84 protocol is one of the most widely-used QKD protocols. In BB84, a sender (Alice) generates a random sequence of bits and encodes them onto a stream of photons using a quantum device. She sends these photons to receiver (Bob), who measures them in one of two bases, chosen randomly for each photon. The two possible bases are referred to as the "rectilinear" (horizontal and vertical polarization) and "diagonal" (45-degree and 135-degree polarization) bases.

If Bob measures a photon in the same basis that Alice prepared it in, he obtains the correct bit value. However, if he measures in a different basis, the outcome is random, and he can obtain a bit value that is different from the one that Alice sent. After the transmission, Alice and Bob communicate over public channel to compare a subset of their bit strings and discard the bits measured in different bases. The remaining bits are then used as the secret key. The working principle of QKD BB84 protocol is shown on Fig.1.

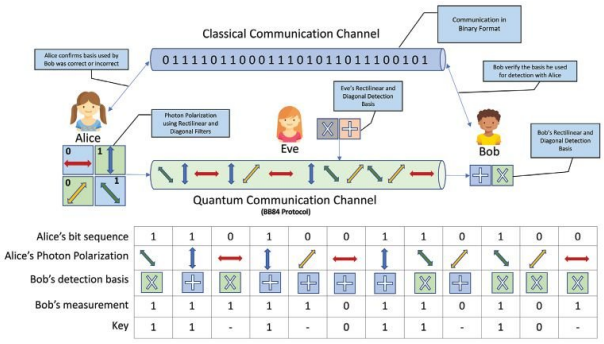

Fig. 1. BB84 Quantum Key Distribution

In conventional BB84 protocol, the security of the key distribution relies on the assumption that the measurement devices used by the sender and receiver are trustworthy and cannot be tampered with. Although this assumption may hold in theory, real-world devices fail to meet its requirements, leaving the protocol vulnerable to quantum hacking attacks. Foe example, those attacks might include intercept/resend attacks, faked state attack, man-in-the-middle attack and photon number splitting attack.

1.2 Main Problem

Implementing Measurement Device Independent QKD (MDI-QKD) is a potential solution to bridge the gap between the theory and

practice of quantum cryptography and achieve secure communication between two parties[1].

MDI QKD (Measurement-Device-Independent Quantum Key Distribution) is an novel quantum communication protocol that enables secure communication between two parties in the presence of tampered (e.g. by an eavesdropper) and, thus, untrusted measurement hardware. By measuring correlations between signals from both parties, rather than the actual signals themselves, MDI QKD ensures perfect security and protects against eavesdropping.

2 Background

2.1 Theory

MDI QKD protocol involves two users, Alice and Bob, who send their polarized single photons to an untrusted third party Charlie. Prior to the transmission, Alice and Bob randomly choose a polarization of each photon from two possible bases: horizontal/vertical (H/V) and diagonal/antidiagonal (D/A). Upon receiving the photons, Charlie makes a measurement on the photon-pair by testing Bell's inequality. In particular, Charlie performs Bell state measurement, projecting the incoming two single-photon signals into a Bell state.

After Charlie projects the incoming signals into a Bell state and broadcasts his measurement results to both Alice and Bob. Alice and Bob then perform post-processing by only keeping the data corresponding to Charlie's successful measurement results while discarding the rest. Also, they post-select the events where they use the same basis and, based on the outcomes announced by Charles, either Alice or Bob flips part of his or her bits to correctly correlate them with another party.

To gain a better understanding of the practical implementation of MDI-QKD, it is useful to consider the main steps of the MDI-QKD protocol, which are depicted in Fig. 2. On the figure, the labels are the following: BS - beam-splitter; PBS - polarization beam-splitter; D1 - D4 - single-photon detector; 1, 2 - input port for photons.

Alice and Bob uses single-photon sources to prepare two pulses. Alice prepares her pulse in mode $\hat{a}$, and Bob prepares his in the mode $\hat{b}$, where

$$\hat{a} = \hat{a}_H + \hat{a}_V = cos(\alpha)\hat{H} + sin(\alpha)\hat{V}$$

and

$$\hat{b} = \hat{b}_H + \hat{b}_V = cos(\beta)\hat{H} + sin(\beta)\hat{V}.$$

In this case, $\hat{H}$ refers to the horizontal polarization of the photon, and $\hat{V}$ - to the vertical.

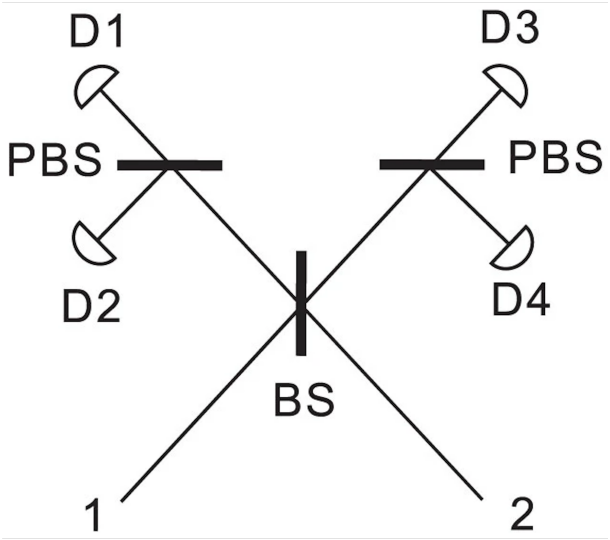

Figure 2. A schematic of the experimental setup.

By properly selecting angles α and β, Alice and Bob prepares their photons in four BB84 polarization state: horizontal ($\hat{H}$), vertical ($\hat{V}$), diagonal ($\frac{1}{\sqrt{2}}\hat{H} + \frac{1}{\sqrt{2}}\hat{V}$) and antidiagonal ($\frac{1}{\sqrt{2}}\hat{H} - \frac{1}{\sqrt{2}}\hat{V}$). Signals from Alice and Bob interfere at a 50:50 beam splitter, resulting in two new modes in two arms after leaving BS.

Left-hand side arm:

$$\frac{\hat{a}+\hat{b}}{\sqrt{2}}$$

or

$$\frac{cos(\alpha)\hat{H}+sin(\alpha)\hat{V}+cos(\beta)\hat{H}+sin(\beta)\hat{V}}{\sqrt{2}}$$

and right-hand side arm:

$$\frac{\hat{a}-\hat{b}}{\sqrt{2}}$$

or

$$\frac{cos(\alpha)\hat{H}+sin(\alpha)\hat{V}-cos(\beta)\hat{H}-sin(\beta)\hat{V}}{\sqrt{2}}.$$

On both output end, 50:50 BS has polarizing beam splitter (PBS) projecting the input photons into either horizontal or vertical polarization states. At each end of PBS, there are two single-photon detectors: $\hat{D}_{1H}$ and $\hat{D}_{1V}$ at the outputs of left-hand side PBS, and $\hat{D}_{2H}$ and $\hat{D}_{2V}$ at the outputs of right-hand side PBS. It can be written as:

$$\hat{D}_{1H}=\frac{cos(\alpha)\hat{H}+cos(\beta)\hat{H}}{\sqrt{2}}$$

$$\hat{D}_{1V}=\frac{sin(\alpha)\hat{V}+sin(\beta)\hat{V}}{\sqrt{2}}$$

$$\hat{D}_{2H}=\frac{cos(\alpha)\hat{H}-cos(\beta)\hat{H}}{\sqrt{2}}$$

$$\hat{D}_{2V}=\frac{sin(\alpha)\hat{V}-sin(\beta)\hat{V}}{\sqrt{2}}$$

A successful Bell state measurement corresponds to the observation of two clicks on two detectors that are associated to orthogonal polarizations. Clicks on $\hat{D}_{1H}$ and $\hat{D}_{2V}$, or $\hat{D}_{2H}$ and $\hat{D}_{1V}$ correspond to a projection into Bell state

$$|\Psi^{-}\rangle=\frac{|HV\rangle-|VH\rangle}{\sqrt{2}}.$$

Clicks on $\hat{D}_{1H}$ and $\hat{D}_{1V}$, or $\hat{D}_{2H}$ and $\hat{D}_{2V}$ correspond to a projection into another Bell state

$$|\Psi^{+}\rangle=\frac{|HV\rangle+|VH\rangle}{\sqrt{2}}.$$

After communication and measurement stage, Charles uses a public channel to announce his measurement result.

Alice and Bob keep the data that correspond to successful measurements and discard the rest of data Charlie shared with them. In the post-selection, they select only those events where the same basis in their transmission was used, announcing them over public channel. Finally, to guarantee that their bit strings are correctly correlated, Alice or Bob applies a bit flip to her/his data, except for the cases where both Alice and bob used diagonal basis. The remaining bits are then used as the secret key for future secure communications over public channel.

It is important to note that the experimental setup contains sources of imperfections, such as dark counts in the single-photon detectors and losses due to optical elements, decreasing the secret key generation rate. However, for simplicity purposes, the theoretical model outlined above assumes an ideal setup without any imperfections or losses accounted. This simplifying assumption allows us to evaluate the system's theoretical performance under optimal conditions. However, any expected errors that may arise due to these imperfections will be accounted for in the simulation section of this work.

2.2 Relevant variables and figures of merit

As for many QKD protocols, MDI-QKD's key figure of merit is the secret key rate, which describes the rate at which two parties can generate 1 bit in the secret key per second. High photon generation rate of single photon source including collection efficiency (10^5 photons per second), high polarizer switching rate (20ms) and high single-photon detection efficiency (around 98%) enable an exceptional key generation rate to be around 9 bits per second. The performance of a measurement-device-independent (MDI) quantum key distribution (QKD) protocol depends on several

key variables. These variables include the wavelength of the laser source used to generate the single-photons (810nm), the speed of the motors controlling the half-wave and quarter-wave plates (0.33 Hz) and detection efficiency (10%). Optimizing these variables is essential to achieve a high secret key rate and ensure the security of the QKD system.

2.3 State-of-the-Art

MDI-QKD protocols have been extensively studied in recent years, and various improvements and modifications have been proposed to enhance their performance[2,3,4].

The conventional MDI-QKD protocol assumes that the source is well-characterized and there is no information leakage from the transmitter devices of both senders. Recent literature has focused on relaxing this unrealistic assumption and proposing a practical solution, ensuring that leaky sources can still be used in the protocol[2]. This important development proved to increase key generation rate, which is crucial for practical implementation of QKD.

One of the challenges of MDI-QKD protocol is the attenuation of the quantum signal when it travels through the communication channel. This leads to a decrease in the signal-to-noise ratio and limits the distance over which reliable communication can be achieved. In 2019, researchers have proposed experimental realization of memory-enhanced quantum communication, which resulted in increase in the secret key rate the protocol over the loss-equivalent direct-transmission method[3].

In 2020, group of researchers have proposed a new approach to implement MDI-QKD using integrated silicon photonic systems[4]. This approach allows for the integration of all the necessary components of the MDI-QKD protocol on a single chip, leading to a compact, reliable, and scalable quantum communication system.

Overall, these recent advancements in MDI-QKD demonstrate its potential for practical applications in secure communication. MDI-QKD's resilience against various attacks and experimental imperfections, increase in secret key rate over long distances, and its compatibility with on-chip designs, make it a promising candidate for secure communication in the future.

3 Experiment description

3.1 Setup

Traditional experimental setups to perform MDI QKD use a 50:50 beam splitter (BS), two polarizing beam splitters (PBS), and four single photon detectors to perform the Bell State Measurement on the randomly selected BB84 polarization states sent by Alice and Bob. However, the experimental setup here is limited to 3 detectors. Consequentially, one of the three detectors acts as two detectors, utilizing a time delay between optical paths to distinguish between counts on the same physical detector.

The experimental setup for this experiment can be viewed in Fig. 3.

Photons generated for both Alice and Bob are sent through a half-wave plate (HWP) to set random BB84 polarization states for each. Each path is then sent through a 50:50 BS, each output of which is then sent through a PBS.

The outputs of one PBS are connected to two detectors, as in traditional MDI QKD. The other PBS outputs are sent though another PBS, but with one line delayed by a long optical fiber extension. This allows one of two perpendicular polarizations to be delayed and arrive at the same detector at a noticeably later time, so that detections for both polar-

izations can be measured.

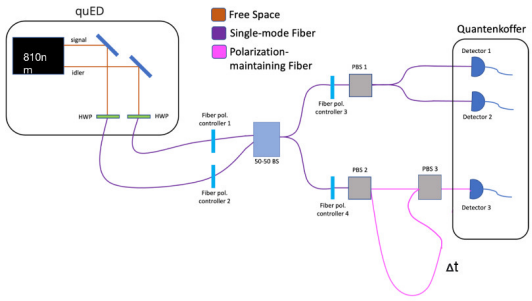

Figure 3. MDI-QKD Experimental setup

		d1V (c/s)	d1H (c/s)	d2V (c/s)	d2H (c/s)	Total (c/s)	Loss
Alice	Bob						
H	H	3,200	13,300	1,700	9,700	27,900	88.47%
	V	9,400	8,100	7,300	5,500	30,300	87.48%
	D	5,800	11,000	4,100	7,900	28,800	88.10%
	A	6,400	10,600	4,600	7,400	29,000	88.02%
V	H	7,600	8,800	5,900	5,700	28,000	88.43%
	V	13,800	3,600	10,100	1,600	29,100	87.98%
	D	10,400	6,600	7,400	4,000	28,400	88.26%
	A	10,900	6,100	8,700	3,600	29,300	87.89%
D	H	5700	10700	4100	7200	27,700	88.55%
	V	12,000	5,200	9,300	3,000	29,500	87.81%
	D	8,400	8,200	6,300	5,400	28,300	88.31%
	A	9,000	7,800	7,100	5,000	28,900	88.06%
A	H	5,500	11,000	3,900	7,500	27,900	88.47%
	V	11,700	5,600	9,300	3,400	30,000	87.60%
	D	8,100	8,600	6,300	5,600	28,600	88.18%
	A	8,800	8,200	7,000	5,200	29,200	87.93%
Avg						28,806	88.10%

Figure 4. Photon count per detector for each combination of states

One challenge of a polarization dependent, fiber implementation of MDI QKD is the polarization rotation that occurs in fiber. As a result, to maintain polarization of photons throughout the experimental setup, polarization correction is needed. Fiber polarization controllers 1 and 2 as seen in Fig. 3 are implemented with quarter-wave plates (QWP) in free space directly after the HWPs that set Alice and Bob's polarization.

These QWPs correct for polarization rotation that occurs before the 50:50 BS. Fiber polarization controllers 3 and 4 are implemented with fiber paddle polarization controllers on each path in between the 50:50 BS and each line's PBS to correct for polarization rotation in fiber before the PBS.

A final challenge to consider with this experimental setup was that the 50:50 BS was implemented on a board that included a transition from fiber to free space and back. This not only introduced significant loss, but also required accurate alignment of the free space components.

3.2 Data

Below is a table of our results.

3.3 Statistical analysis

The data shown above contains a significant amount of loss, with an average loss of 88% of Alice and Bob's data through each combination of BB84 polarization states. This is due to a number of components of the experimental setup, most notably the transition from fiber to free space and back before the first 50:50 BS.

Additionally, there are a number of sources of error that significantly impacted our results, making them largely diverge with expected results from what is expected in MDI QKD theory. One such source of error was the polarization rotation mentioned previously. Correction methods were used but unable to fully account for changes in each BB84 state's polarization.

Another hugely damaging source of error which was not anticipated was the inability to locate a dip in coincidence counts in the 50:50 BS outputs due to the Hong-Ou-Mandel (HOM) Effect[5]. A clear example of this can be seen Fig. 4 in the section above in the scenario where both Alice and Bob sent horizontally polarized light. The expected result of this should be that all light goes to one output of the 50:50 BS. However, the split between the two outputs of the 50:50 BS is far

from so one sided. This is because of the time difference between when photons from Alice and Bob arrive at the BS. The time difference prevents HOM interference from sending all light into one BS output.

4 Simulation

4.1 Model

In this section, we present the detailed simulation model of the measurement-device-independent (MDI) quantum key distribution (QKD) protocol. The model is based on a realistic description of the physical components of an MDI-QKD system, including the sources, channels, optical elements, and detectors. The model is used to study the performance of MDI-QKD systems under various conditions, including channel and optical element losses along with low detector and single-photon source efficiencies. The results of the simulations show that MDI-QKD can achieve high key rates, even in the presence of significant noise and imperfections.

The MDI-QKD protocol is depicted in Figure 4. Alice ($\hat{a}$) and Bob ($\hat{b}$) each have a source that emits single photons in a coherent superposition of polarization states $|H\rangle$ and $|V\rangle$.

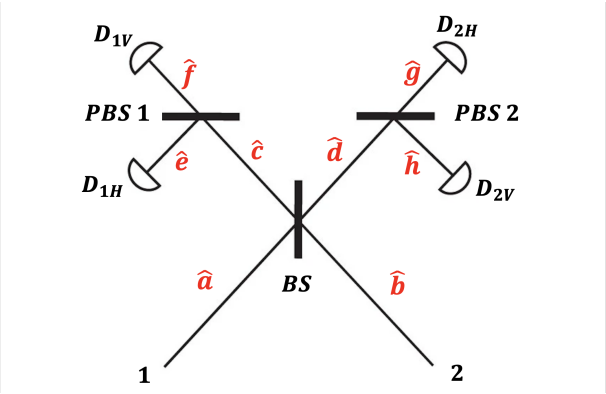

Figure 5. A labeled schematic of the setup used to model the simulation

$$\hat{a} = a_h |H\rangle + a_v |V\rangle$$
$$\hat{b} = b_h |H\rangle + b_v |V\rangle$$

The photons are then sent through a 50:50 beam splitter (BS), before passing through one of two polarizing beam splitters (PBS 1 or PBS 2) and finally being measured at one or two of the detectors (which are controlled by a third party). To simulate the MDI-QKD protocol, we can characterize the efficiency of each component and calculate the expected photon count at each detector. We can do so using the following expressions:

$$\hat{c} = \frac{1}{\sqrt{2}}(\hat{a} - \hat{b})$$
$$\hat{d} = \frac{1}{\sqrt{2}}(\hat{a} + \hat{b})$$

$$\hat{e} = |V\rangle\langle V|\,\hat{c} \qquad \hat{g} = |V\rangle\langle V|\,\hat{d}$$
$$\hat{f} = |H\rangle\langle H|\,\hat{c} \qquad \hat{h} = |H\rangle\langle H|\,\hat{d}$$

Our simulation contains two major components that can be used to calculate the secret key rates for two important cases: without and with system loss. Later, by doing simulation result analysis, we characterize the importance of each component for secret key rate generation.

In our models, we first calculate a bits per photon rate that allows us to decouple the photon generation process from the physical behavior of our setup. Then, we use the specifications of a single-photon source (i.e. single-photon generation rate) and the polarizer switching time (i.e. photon encoding rate) to calculate a photons per second rate. Finally, we can combine the two to calculate a secret key rate in units bits per second.

4.1.1 Without Loss

To better understand our system, we first modeled a lossless setup. We define lossless setup to have no loss at any point in the simulation. We calculated the expected photon

counts for each detector and simulated the experiment to steady state.

Working through the expressions described in the section above, we can calculate an expected photon count per detector.

$$n_{d1h} = \hat{e}^\dagger \hat{e} = \frac{(a_v - b_v)^2}{2}$$
$$n_{d1v} = \hat{f}^\dagger \hat{f} = \frac{(a_h - b_h)^2}{2}$$
$$n_{d2h} = \hat{g}^\dagger \hat{g} = \frac{(a_h + b_h)^2}{2}$$
$$n_{d2v} = \hat{h}^\dagger \hat{h} = \frac{(a_v + b_v)^2}{2}$$

Then, we can use these expectation values to simulate our lossless setup and analyze the results.

		d1v	d1h	d2v	d2h
Alice	**Bob**				
States.H	**States.H**	0.00	0.00	0.00	2.00
	States.V	0.50	0.50	0.50	0.50
	States.D	0.25	0.04	0.25	1.46
	States.A	0.25	0.04	0.25	1.46
States.V	**States.H**	0.50	0.50	0.50	0.50
	States.V	0.00	0.00	2.00	0.00
	States.D	0.04	0.25	1.46	0.25
	States.A	1.46	0.25	0.04	0.25
States.D	**States.H**	0.25	0.04	0.25	1.46
	States.V	0.04	0.25	1.45	0.25
	States.D	0.00	0.00	1.00	1.00
	States.A	1.00	0.00	0.00	1.00
States.A	**States.H**	0.25	0.04	0.25	1.45
	States.V	1.46	0.25	0.04	0.25
	States.D	1.00	0.00	0.00	1.00
	States.A	0.00	0.00	1.00	1.00

Figure 6. Photon count per detector

We can observe that, as it was expected, this is almost identical to our expected photon counts per detector. Here, we can see the effect of interference between two indistinguishable photons, and can notice that there are no coincidence effects when the two are indistinguishable.

4.1.2 With Loss

While a lossless setup would be fantastic, the real world is not perfect. Our experimental setup has many non-idealities and in order to better simulate our physical setup, we had to develop a more accurate model that incorporated channel loss, optical element losses, and low detector efficiency. To do so, we can characterize all of our components and assign an efficiency coefficient to each, where the efficiency of each component represents the percent of photons that get through.

- Detector Efficiency (e_d)
- PBS 1 Efficiency (e_{pbs1})
- PBS 2 Efficiency (e_{pbs2})
- 50:50 BS Efficiency (e_{bs50})
- Fiber $\leftrightarrow$ Free Space (e_{fff})
- HWP A Efficiency (e_{hwp_a})
- QWP A Efficiency (e_{qwp_a})
- HWP B Efficiency (e_{hwp_b})
- QWP B Efficiency (e_{qwp_b})

As described in section 3, Alice ($\hat{a}$) and Bob ($\hat{b}$) each have a source that emits single photons in a coherent superposition of polarization states $|H\rangle$ and $|V\rangle$. To generate this state, we use an SPDC source (the quED) that emits horizontally polarized light. For each of Alice and Bob, we then use a HWP to polarize the light into a superposition of $|H\rangle$ and $|V\rangle$. Then, we use a QWP to correct for polarization rotation in fiber. This process of photon source generation can be characterized as follows:

$$\hat{a} = \overbrace{\left[e_f \cdot e_{\text{hwp\_a}} \cdot e_{\text{qwp\_a}}\right]}^{a_e} \left[a_h \left|H\right\rangle + a_v \left|V\right\rangle\right]$$

$$\hat{b} = \overbrace{\left[e_f \cdot e_{\text{hwp\_b}} \cdot e_{\text{qwp\_b}}\right]}^{b_e} \left[b_h \left|H\right\rangle + b_v \left|V\right\rangle\right]$$

Now that we have a more accurate representation of our photon sources $\hat{a}$ and $\hat{b}$, we can follow a similar process as in section 4.1.2 to calculate an expected photon count at each detector, but incorporating efficiency coefficients for each component. The results can be seen below.

$$n_{d1h} = e_d * \hat{e}^\dagger \hat{e} = e_d * \frac{(e_{bs50} * e_{pbs1})^2 (a_e a_h - b_e b_h)^2}{2}$$

$$n_{d1v} = e_d * \hat{f}^\dagger \hat{f} = e_d * \frac{(e_{bs50} * e_{pbs1})^2 (a_e a_v - b_e b_v)^2}{2}$$

$$n_{d2h} = e_d * \hat{g}^\dagger \hat{g} = e_d * \frac{(e_{bs50} * e_{pbs2})^2 (a_e a_h + b_e b_h)^2}{2}$$

$$n_{d2v} = e_d * \hat{h}^\dagger \hat{h} = e_d * \frac{(e_{bs50} * e_{pbs2})^2 (b_e a_v + b_e b_v)^2}{2}$$

Finally, we can use these relationships to model our system, and implement an end to end simulation that is characterized by our physical setup. This allows us to simulate the MDI-QKD protocol end-to-end and analyze the secret key rate based on the efficiency of our physical components.

4.2 Results

To understand the results of our simulation, we consider two case: the state of the art and the 6.2410 MIT design lab setup. We characterize the components for each case and can then analyze the results, primarily the secret key rate.

4.2.1 State of the Art

For the State of the Art, we assume we can get our hands on the most advanced equipment available, no matter the cost. This allows us to acquire a superconducting nanowire single photon detector with 98% efficiency and a polarizer from Thorlabs with a switching time of 20ms. Additionally, we assume we have no loss from the 50/50 beamsplitter, the polarizing beamsplitters, the fiber to free space conversion, and our photon generation source.

First, we can calculate a photon per second rate which is simply the rate at which we can encode photons. While the photon generation rate of our detectors is 10^5 photons / second, we are actually limited by our polarizer switching time. That leaves us with a photon generation rate of $\frac{1}{0.002} = 50$ photons / second.

Then, we can use our simulation to generate a secret key rate. Doing so, we see that our bits per photon rate is 0.1848 and our secret key rate is about 9 bits / second.

4.2.2 MIT 6.2410 Lab

For the setup we have available to us in the 6.2410 optics lab, we have much lossier components. Our avalanche photodetectors are only 10% efficient, our quED polarizer switching time is 3 seconds (taken from BB84 lab), our 50/50 beamsplitter is only 50% efficient, our polarizing beamsplitters are only 75% efficient, and our half wave plates used for photon source generation are only 75% generation.

First, we can calculate a photon per second rate which is simply the rate at which we can encode photons. Again, the photon generation rate of our detectors is 10^5 photons / second, but in reality, we are actually limited by our polarizer switching time. That leaves us with a photon generation rate of $\frac{1}{3} = 0.33$ photons / second.

Then, we can use our simulation to generate a secret key rate. Doing so, we see that our bits per photon rate is 0.0014 and our secret key rate is about 0.0005 bits / second.

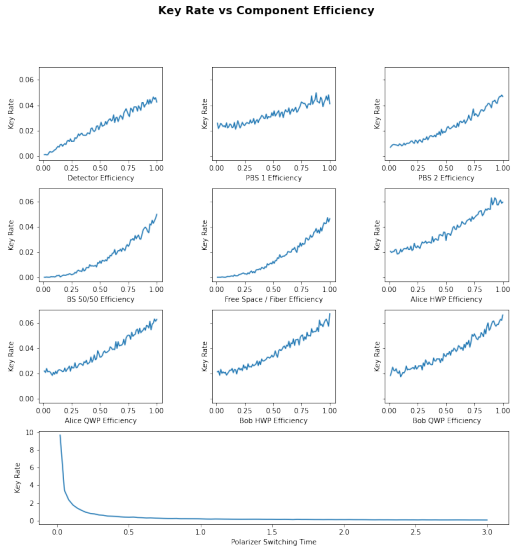

Figure 7. Comparison of key rate vs component efficiency for each component

There are two primary takeaways from this visualization. First, we see that far and away the most important factor in secret key generation is polarizer switching time. As a result, if we had a budget and wanted to optimize our secret key rate, we would aim for a state of the art motorized polarizer that would allow us to achieve switching rates that are fractions of a second, not 3 seconds like the quED. Second, we can see that the components that are involved in every path also have a great effect. For example, the 50/50 beamsplitter, which handles every single photon that is generated has a greater effect than the PBS 1. Intuitively this makes sense and gives us yet another way to optimize our component selection and lab setup.

5 Discussion

5.1 Experimental results

One previously mentioned challenge in the experimental implementation was polarization correction. This was particularly difficult to do when Alice and Bob sent diagonal and anti-diagonal polarization states. This was partially due to the birefringence within polarization maintaining (PM) fiber. Additionally, the physical implementation of our experimental setup was unable to accommodate for a QWP in both Alice and Bob's paths, which was intended to help correct polarization rotation. This was another reason our experimental results were far different from our simulated results.

5.2 Numerical simulation

State of the Art SKR: 9 bits / second
6.2410 Optics Lab SKR: 0.0005 bits / second

While this may seem poor, it is important note that using MDI-QKD, we are generating symmetric keys, and due to the nature of symmetric they tend to be shorter that public/private key pairs. As a result, a good symmetric key length can be around 512 bits. At the rate of our optics lab setup, this would take 2.8 hours which is around what we achieved during the BB84 lab.

However, we are not satisfied just yet. We can see that the inefficiencies of our components has a significant effect on secret key rate. To better understand this, we are going to analyze the effect of each component independently on secret key rate.

5.3 Remaining challenges

In this particular implementation of MDI-QKD, there are two primary sources of errors that can cause a reduction in the secret key rate: imperfect visibility of the Hong-Ou-Mandel (HOM) effect and disturbance of polarization maintenance in fiber.

The first possible source of error is due to HOM effect. The Hong-Ou-Mandel (HOM) effect is a quantum interference phenomenon that occurs when two indistinguishable photons are incident on a beam splitter from opposite directions. The photons can either both pass through one output port or one photon

can pass through each output port. The visibility of the HOM effect is a measure of the indistinguishability of the incident photons.

When the visibility of the HOM effect is not maximized, it means that the probability of detecting the photons at the same output port is less than 100. In other words, there is a non-zero probability that one photon will be detected at one output port while the other photon is detected at the other output port.

If two clicks are observed on two detectors in this scenario, it means that both photons have been detected at different output ports. Since a successful Bell state measurement corresponds to the observation of precisely two detectors being triggered, the not maximized visibility of HOM experiment might cause Charlie to report false results back to Alice and Bob. Two clicks on detectors instead of one might happen due to imperfections in the experimental setup, such as imperfect matching of the optical paths or non-ideal beamsplitter characteristics. This ultimately leads to decrease in the secret key rate.

The second source of error is due to disturbance of polarization maintenance in fiber. It refers to the degradation or corruption of the polarization state of light as it travels through an optical fiber. This can occur due to various factors, such as fiber bending, temperature changes, and mechanical stress, which can introduce birefringence and cause the polarization to fluctuate. When the polarization state of the transmitted photons is disturbed, it can cause errors in the measurement of the polarization by the detectors, leading to a reduction in the number of correct detection events. This, in turn, leads to a reduction in the signal-to-noise ratio and lowers the secret key rate.

6 Conclusions

References

[1] Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." Physical review letters 108.13 (2012): 130503.

[2] Wang, W., Tamaki, K. Curty, M. Measurement-device-independent quantum key distribution with leaky sources. Sci Rep 11, 1678 (2021).

[3] Bhaskar, Mihir K., et al. "Experimental demonstration of memory-enhanced quantum communication." Nature 580.7801 (2020): 60-64.

[4] L. Cao, W. Luo, et al. "Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems." Phys. Rev. Applied 14, 011001 (2020).

[5] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. Physical Review Letters, 59(18):2044–2046, November 1987. Publisher: American Physical Society. URL: https://link.aps.org/doi/10.1103/PhysRevLett.59.2044 (visited on 2022-07-13), doi:10.1103/PhysRevLett.59.2044.