To the Graduate Council:
I am submitting herewith a dissertation written by Brian Joseph Rollick entitled "Overcoming Atmospheric Effects in Quantum Cryptography." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Physics.

George Siopsis, Major Professor

We have read this dissertation
and recommend its acceptance:

George Siopsis

Bing Qi

Jaan Mannik

Husheng Li

Raphael Pooser

Accepted for the Council:

Dixie L. Thompson

Vice Provost and Dean of the Graduate School

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

Overcoming Atmospheric Effects in Quantum Cryptography

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Brian Joseph Rollick

August 2022

© by Brian Joseph Rollick, 2022
All Rights Reserved.

Acknowledgements

I would like to thank:

All my friends who worked with me on class and generally made my time in grad school more enjoyable. Also, Corey Gilbert, Xiaobin Lu and Chengru Chang for studying tirelessly with me in the library for the qualifying exam. I estimated that I doubled my knowledge of physics in the first year, and that is partially why.

Jeff Garcia, Lefty, and Brian Williams for teaching me what I know in the lab. Our experiments seemed quite intimidating when I first arrived, but you guys helped me get up to speed quickly.

Chrisanne and Dr. Breinig for always providing me useful advice on the graduate program in general.

Dr. Jing Wang from Cablelabs for providing me an opportunity to test what I knew about QKD. In addition to showing me many EE tricks in the lab, you forced me to understand all the nitty gritty details of QKD since you hadn't worked with it before.

Drs. George Siopsis and Bing Qi for all their research help and advisorship. There are smarter graduate students than me, but you guys were always patient with my understanding of the concepts. Dr. Qi, I especially appreciate the time you spent helping me after you went to Cisco and probably didn't have much time to worry about your past adjunct professorship.

My parents for providing encouragement and support throughout my higher education and PhD

A journey of a thousand miles begins with the first step. -Lao Tzu

Abstract

Quantum Computers will have the potential to greatly assist us in problems such as searching, optimization and even drug discovery. Unfortunately, among these newfound capabilities is one which allows one to break RSA encryption in orders of magnitude less time. One promising countermeasure to secure our communication today and in the future is the one time pad, although it is very difficult to generate and distribute. Quantum Key Distribution offers a practical method for two authenticated parties to generate a key. Whereby the parties, Alice and Bob, share quantum states and use physical laws to place an upper bound on the information an eavesdropper could possibly have. QKD has matured tremendously since it was proposed in 1984, but gaps still remain between the device models used in security proofs and what can be achieved in deployments.

In particular, the atmosphere presents a challenging environment for QKD, and due to the wireless nature of communications today, we cannot avoid it. QKD must be robust to atmospheric loss as well as transmittance fluctuation due to turbulence. In this dissertation, I perform an experiment to make the BB84 protocol more robust in turbulence by monitoring the transmittance of a channel and finding time periods where the transmittance is low, hence error rate is high and discard data collected during such timeframes. We conduct an experiment to test Hong Ou Mandel visibility, which is at the heart of Measurement Device Independent QKD, by varying the detector parameters and the input photons' level of identity. I use an observation where we find that the interference effect is highly dependent on the similarity of photon numbers at the measurer's beamsplitter to develop a scheme

in MDI QKD where the key rate is kept high through tethering the transmittance fluctuations of Alice and Bob's channels with dynamic attenuation. The results show an improvement when in a turbulent atmosphere, even when accounting for nonzero minimum loss.

Table of Contents

1 Introduction **1**

1.1 Why We Need Quantum Cryptography 1

1.2 Putting QKD into Practice 4

1.3 Challenges Posed by Free Space 6

1.3.1 Extinction 7

1.3.2 Turbulence 12

2 BB84 in a Turbulent Atmosphere **18**

2.1 Decoy States 19

2.2 Finite Size BB84 24

2.3 BB84 in Turbulence 29

2.4 Testing PRTS and ARTS in Simulated Turbulent Conditions 33

2.4.1 Experimental Setup and Procedure 35

2.4.2 Results 38

3 Hong Ou Mandel Interference with Device Imperfections **42**

3.1 HOM Visibility in Coherent States 45

3.2 Effects of Imperfections on HOM Visibility 48

3.2.1 Detector Imperfections' Effects on HOM 50

3.2.2 HOM and Source Imperfections 51

4 Measurement Device Independent QKD with Dynamic Attenuation **57**

4.1 MDI QKD 57

4.2 Effects of Asymmetry on MDI QKD 60
4.3 Dynamic Attenuation Background 63
4.4 Using Dynamic Attenuation 66
4.5 Results of Applying Dynamic Attenuation to Statistically Identical, Independent Channels 69

5 Future Work **74**
5.1 Thoughts on Implementing Dynamic Attenuation with Nonzero Insertion Loss 74
5.2 Combining Postselection with Dynamic Attenuation in MDI QKD . . 75

A BB84 Key Calculation **92**

B Noise Model and Finite Key Calculation in MDI QKD **94**
B.1 Noise Model 94
B.1.1 Z Basis 94
B.1.2 X Basis 95
B.2 Secure Key Calculation 96

Vita **99**

List of Tables

2.1 Decoy Parameters for our experiment in [1] 39

4.1 Decoy parameters for dynamic attenuation simulations. 68

List of Figures

1.1 Visualizing QKD Security 5
1.2 Layers of the atmosphere and average temperature. 8
1.3 Turbulent Eddies Diagram 13

2.1 Key Rate Improved by Decoy States 25
2.2 Postprocessing Steps 26
2.3 ARTS diagrams 31
2.4 Meaning of the optimal cutoff in PRTS 34
2.5 Our experimental setup for BB84 with adaptive postselection 36
2.6 ARTS vs PRTS in BB84 for various atmospheric conditions 39
2.7 Robustness of optimal cutoff for PRTS 40

3.1 Possible outcomes for two single photons incident on a beamsplitter . 43
3.2 Quantum mechanical description of a beamsplitter 43
3.3 Diagram for the HOM with imperfections experiment. 49
3.4 Decay of afterpulse probability after a detection 52
3.5 HOM visibility as a function of deadtime 52
3.6 HOM visibility for source imperfections 53
3.7 The HOM visibility with respect to the intensity mismatch 55

4.1 A typical measurement setup for polarization encoding MDI QKD. . 59
4.2 Transmittance mismatch's effects on error in each basis 62
4.3 Implementing dynamic attenuation in Polarization Encoding MDI QKD 64
4.4 Effect of attenuating an overly strong channel 68
4.5 Appearance of the lookup table and effects on key rate 70
4.6 Dynamic attenuation applied to statistically symmetric channels . . . 72
4.7 Dynamic Attenuation with Nonzero Minimum Loss 73

OTP	One Time Pad
QKD	Quantum Key Distribution
BB84	Bennett Brassard 1984
PNR	Photon Number Resolving
SPAD	Single Photon Avalanche Detector
HOM	Hong Ou Mandel
MDI	Measurement Device Independent
PDTC	Probability Density of the Transmittance Coefficient
QBER	Quantum Bit Error Rate
VOA	Variable Optical Attenuator
Arb	Arbitrary Waveform
AWG	Arbitrary Waveform Generator
PM	Phase Modulator
FM	Faraday Mirror
IM	Intensity Modulator
Pol-M	Polarization Modulator
AOM	Acousto optical Modulator
DWDM	Dense Wavelength Division Multiplexer
PBS	Polarizing Beam Splitter
BS	Beam Splitter
TIA	Time Interval Analyzer
ARTS	Adaptive Real Time Selection
PRTS	Prefixed-threshold Real Time Selection

Chapter 1

Introduction

1.1 Why We Need Quantum Cryptography

One of human history's most ancient problems is the secure delivery of messages which only the intended recipient can read. Historically, cryptography appears to be a cat and mouse game where the parties sharing messages must continue to find ways to protect their communications from equally clever eavesdroppers.

In certain instances, one wants information to stay secure forever. For example, a former drug user may need their information to be accessible by a medical professional, but they may want to keep it from their future employer or family. Such cases obviate a protocol which is unbreakable. This scheme arrived in 1917, when Vernam devised a One-Time-Pad[2](OTP) where two parties would use a key which would be at least as long as the data transferred. Shannon proved its security in 1949[3].

The OTP is extremely powerful, albeit impractical. If the encryption on the Internet used OTP's, our data rates would drop by at least half due to the long key length. Furthermore, how might a banking website exchange a OTP with customers? It could keep caches of OTP's for each customer, who could likewise keep long books of OTP's for each website login they use. What if the bank or other institution suffers a data breach through a phishing attack? The keys would have to be securely reset by both parties.

Because it is unwieldy, the OTP is not widely used. Rather, the aforementioned banking website above likely uses RSA encryption, a technique which relies on the immense computational difficulty of factoring prime numbers.

Prime factorization is hard because it requires the brute force dividing of numbers by every smaller prime number. Perhaps a mathematician in the future will discover a new, much more efficient algorithm for prime factorization. Today's information security relies on there not being one.

That day became imminent when Peter Shor proposed an algorithm[4] using quantum mechanical operators and "qubits" which would allow one to factor extraordinarily faster than with a classical computer. Rather than requiring a time-scale on the order of the age of the universe, a sufficiently powerful quantum computer would only require several years to break RSA encryption.

Quantum computers capable of running Shor's algorithm have not yet been built at the time of writing, but cryptographers need to start planning for a "Post Quantum Future" sooner rather than later. Shor's algorithm was made to use fewer qubits in [5] and quantum computers made the news in 2019 when Google reached so-called "Quantum Supremacy"[6].

The threat becomes much more immediate if a "Download now, Decrypt later" attack is utilized where encrypted ciphertext is obtained now with the intention of decrypting it once quantum computing power becomes cheaper. National security secrets and medical information need to stay secure for long periods of time, so society already needs countermeasures for the Post-Quantum future.

There are two such varieties of countermeasures. The first is aptly called "Post-Quantum Cryptography" where cryptographic protocols are designed invulnerably to Shor's algorithm. For instance, Lamport Signatures[7] are digital signatures which Shor's algorithm cannot crack[8]. Additionally, a hardened, albeit computationally expensive, version of RSA was also proposed in [9].

Post quantum protocols are useful and will likely play an important role in the future of communications[10]. Unfortunately, although they are secure against Shor's

algorithm, there is no guarantee a new quantum algorithm will not be discovered that is equally disruptive. Indeed, it is unproven they cannot be attacked even by a classical computer. Recently, a popular post-quantum candidate called Rainbow was successfully attacked in 53 hours on a laptop[11]. This suggests Tomorrow's encryption standards require another ingredient.

A second countermeasure is to revisit the OTP. However, the aforementioned difficulty of key distribution remains, unless we turn again to quantum mechanics. In the '70s and '80s, some interesting applications of fundamental quantum mechanics were proposed, such as money[12], and also cryptography[13] (computing[14] was previously mentioned).

The basic idea of quantum key distribution (QKD) is that two parties, Alice and Bob, encode their key bits on quantum states. Each party measures and sends the states in different bases and through a combination of classical communication and error correction, they can arrive at a key which is provably secure. Of course, details vary for each protocol, whether it be BB84[13], Coherent One Way[15], Twin-Field[16], etc.

Alice and Bob encode their quantum states in different bases to thwart a potential eavesdropper(s) we shall name Eve. If she tries to intercept qubits, she must choose the basis correctly to obtain any usable information. Furthermore, she cannot reliably copy them due to the no cloning theorem[17]. Thus, she essentially gets one chance per qubit to measure correctly.

Eve knows if she simply intercepts the qubit, then it will not appear in the final key and her efforts will be useless. Suppose she stubbornly tries to resend the qubit just after she measures it. Her "intercept-resend" trick will unavoidably introduce errors because if she guesses the measurement basis incorrectly, she will introduce errors, which Alice and Bob will notice in the other basis. This is why Alice and Bob should encode in at least two different bases. At the end of transmission, Alice and Bob sacrifice parts of their key to check the error rate and if it is above a threshold, they abort the protocol due to the potential presence of an eavesdropper.

The principles behind QKD are powerful, but in the next section we will discuss some challenges that arise when we deploy it.

1.2 Putting QKD into Practice

Although QKD makes big promises for encrypted communications, it is difficult to build setups that perfectly exemplify the theoretical models comprising the proofs. For example, one cannot just send a single photon at will(even for pseudosingle photon sources[18]); there is always nonzero probability that multiple photons will be sent, in which case Eve would be able to intercept one without revealing her presence. Detectors are not ideal and most cannot discriminate between a single photon pulse and the two photon pulse it would have received.

Perhaps better detectors are needed? Photon Number Resolving (PNR) detectors are able to better resolve photon number than Single Photon Avalanche Detectors (SPAD). However, this additional feature complicates the device's theoretical model, thereby increasing the number of ways in which the experimental device can differ. Then, because the device is more complex, an attacker may have more potential attack vectors.

QKD security is nicely illustrated in Figure 1.1. Here, subset A is a set of conditions for which QKD is provably secure and experimental devices are perfectly characterized. A goal of QKD research is to expand this subset. In region C, we have setup conditions which are known to be unsecure, such as the obvious case of sending multiple photons.

It is desirable to shrink Region B. Here, we have conditions which produce expected results between Alice and Bob, but where Eve can nevertheless obtain information on the final key. Attacks on the setup happen here. Suppose we have a very noisy channel, with wavelength dependent attenuation, and a time varying transmittance. Region B in such a channel might be quite large.

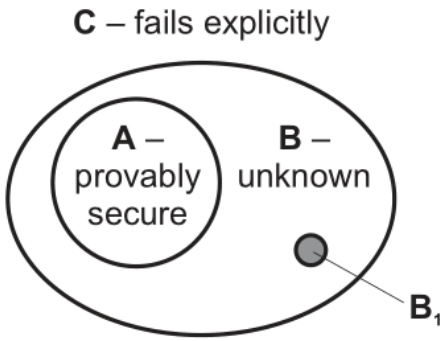


Figure 1.1: Taken from [19]. An attempt to visualize the security of QKD setups. The security proofs assume operation in region A and region C is knowably unsecure. Region B exists because of real deployments' deviations from ideal models in the proofs.

A free space channel has all of these characteristics, and we must find ways to grapple with the challenges. Wireless communication has changed the world in innumerable ways and it is becoming easier than ever to stay connected. Even when wifi is absent, we have cellular data. Even without that, the SpaceX project, Starlink®even seeks (or sought) to provide satellite based internet globally*.

In short, we must make Quantum Key Distribution robust in free space if we wish to keep our wireless communication secure in a post quantum world. Part of this goal requires us to ensure that QKD can withstand the fluctuating transmittance caused by atmospheric turbulence. In this dissertation, we will review work whose goal was to improve the secure key rate of the BB84 and Measurement Device Independent(MDI) protocols. In the former case, a scheme was tested where one systematically discards blocks of data where atmospheric transmittance is low and error rate is therefore high. We also investigated the two photon interference Hong-Ou-Mandel(HOM) effect relied on by MDI QKD and how it could be impacted by experimental imperfections. Finally, knowledge from the HOM experiment was used to produce a dynamic attenuation scheme, which effectively tethers the transmittance fluctuations of Alice and Bob to ensure the key rate is suffers minimally when turbulence becomes severe.

In the next section, we will review some of the challenges encountered in free space optical communication. In particular, we will discuss loss and its sources and the effects of atmospheric turbulence.

1.3 Challenges Posed by Free Space

QKD can appear somewhat more straightforward in fiber. Fibers often give fixed losses per unit length(usually .2dB per km). Thus, yields and gains can be easily calculated. Background light is minimal and there is no pointing or beam alignment required, unlike in free space. Much of the challenge is in very long fibers (100's of km)

*https://web.archive.org/web/20150213044054/http://seattletimes.com/html/businesstechnology/2025480750_spacexmuskxml.html

and when polarizations drift[20]. Nevertheless, if we are to build QKD successfully into our technology, it must be wireless capable.

1.3.1 Extinction

The atmosphere poses formidable challenges to any method of QKD we choose. It is a mixture of many different gases and each will have its own set of transition lines. Additionally, it is generally a dirty environment compared to a clean, manufactured optical fiber with constant attenuation.

It is common to use a parameter γ in Beer's law (for example, see [21]) to describe the loss in intensity where $I(z) = I_0 \times 10^{-\gamma z}$ where I_0 is the original intensity and z is the distance the beam propagates. γ is determined from four different sources as shown in[22]:

$$\gamma = \alpha_{ml}(\lambda) + \alpha_{al}(\lambda) + \beta_{ml}(\lambda) + \beta_{al}(\lambda) \tag{1.1}$$

Where we see four contributions to the total attenuation. The ml subscripts indicate molecular absorption and scattering, while the al contributions come from aerosol absorption and scattering. Thankfully, we can greatly simplify our analysis if we choose a wavelength within an atmospheric transmittance window, such as 1550 nm. Now, because our extinction is mostly due to scattering we have: $\gamma(\lambda) \approx \beta_{al}(\lambda)$[22]. Other such windows can be found in [23]. The following subsection will very generally describe the concepts behind scattering due to aerosols.

Aerosols

When discussing the types of aerosols that occur in the atmosphere, we must first define its characteristics. We shall assume it consists of concentric spherical shells of air. The temperature, pressure and composition change with height. The temperature variations define different layers[24], as shown in Figure 1.2.

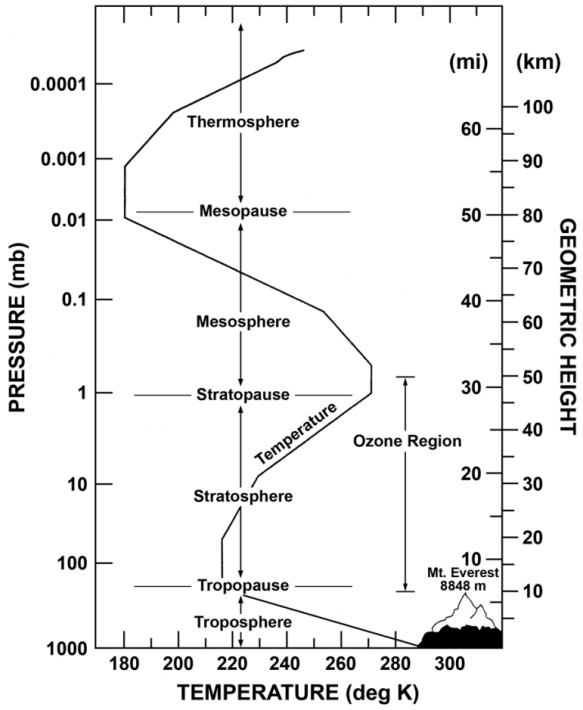


Figure 1.2: Layers of the atmosphere and average temperature. Taken from [24]. Each layer of the atmosphere contains different types of aerosols and gas concentrations. Much everyday wireless communication happens in the troposphere, but satellite links necessitate knowledge of more layers.

The troposphere is defined by the layer in which temperature decreases with height until it reaches a pause, which is called the tropopause. Because this layer is closest to the earth's surface it can have a large variety of aerosols, which are characterized as urban, rural or maritime. Aerosols in the stratosphere are principally volcanic debris and the mesosphere's main component is meteoric dust. Only transmission in the troposphere will be discussed here.

If one uses software, such as MODTRAN®, the user must choose an atmospheric model, such as the tropical model or the US Standard 1976[25]. These models differ, for example, in the thickness of the troposphere or ozone concentration in the stratosphere[26]. Nevertheless, these models are relatively similar in the troposphere so the choice does not affect our analysis.

Due to the variable size of aerosols and larger atmospheric particles like hail, we should determine the characteristic size parameter to decide on the type of scattering. If we use the relation: $x_0 = \frac{2\pi r}{\lambda}$ where r is the particle size, if $x_0 << 1$ such as for smaller haze particles or air molecules[22], we can easily find the loss due to Rayleigh scattering. However, if the characteristic size is closer to 1, phase differences over the surface of the particle cannot be neglected and Mie scattering or the T-matrix method must be used.

Of course, the aerosol particles have different sizes, so distributions must be found for each. Prior to this, we must describe the different aerosol types and where they are found.

At the time of publication of [26], it was believed that the rural aerosols were composed of water soluble substances such as ammonium and calcium sulfates, organic compounds[27] and "dust". Urban aerosols were then assumed to be composed of 80% the rural aerosol model as well as a soot component due to combustion. Maritime models are mainly composed of sea salt and some rural model contribution, particularly near continents.

It is important to have an aerosol model because each type of particle has its own size distribution. Interestingly, humidity has an important role because it causes particles to coagulate and increase in size[26].

To put these ingredients together and provide an illustration of a theoretical fog model, we will follow a Mie Scattering-type derivation from [28]. We begin by defining a scattering efficiency, Q, which is given by:

$$Q = \frac{C}{\pi r^2} \tag{1.2}$$

Where C is the scattering cross section for a particle of radius r. Similar to a relation in van de Hulst[29], the attenuation is given by:

$$\beta_{fog}(\lambda) = 10^5 \int_0^\infty \pi r^2 Q(\frac{2\pi r}{\lambda}, n_r) n(r) \mathrm{d}r \tag{1.3}$$

Here, r is the particle size and n_r is the index of refraction of fog. The difficulty lies in finding the size distribution, n_r. It is common to use a modified gamma distribution, like in [28] where:

$$n(r) = a r^\alpha \mathrm{e}^{-br} \tag{1.4}$$

Where a, α, and b are all statistical parameters. Due to the difficulty in knowing them, it is easier to employ an empirical model than a strictly Mie based one[22]. Models like the Kim[30] and Kruse[31] attempt to relate attenuation to a parameter much easier to find: meteorological visibility.

Visibility is defined as the distance at which the difference in relative intensity of an object against a background falls below some threshold, often called the transmittance

threshold, T, which is commonly 2 or 5%[22]. Kruse produced the first model relating the visibility to the attenuation:

$$V = \frac{10\log_{10}(T)}{\beta(\lambda)}(\frac{\lambda}{\lambda_{sun}})^{-q} \tag{1.5}$$

Where V is visibility, λ is the wavelength in question, and λ_{sun} is 550 nm, the highest intensity wavelength from the sun. The parameter q determines the wavelength dependence of the scattering. In Kruse's model, he gives:

$$\begin{cases} q = 1.6 & \text{for } V > 50\text{km} \\ q = 1.3 & \text{for } 6\text{km} < V < 50\text{km} \\ q = .585 \times V^{-1/3} & \text{for } V < 6\text{km} \end{cases}$$

Kim later modified the model for low visibilities[30]:

$$\begin{cases} q = 1.6 & \text{for } V > 50\text{km} \\ q = 1.3 & \text{for } 6\text{km} < V < 50\text{km} \\ q = .16V + .34 & \text{for } 1\text{km} < V < 6\text{km} \\ q = V - .5 & \text{for } .5\text{km} < V < 1\text{km} \\ q = 0 & \text{for } V < .5\text{km} \end{cases}$$

Kim's model is particularly interesting because he suggests no wavelength dependence for very low visibilities ($V < .5$ km). This point is disputed between [30] and [28].

The goal of this subsection is not to provide a detailed analysis of attenuation in the atmosphere, but merely to describe the principles needed for a satisfactory model. We may choose a simple, horizontal channel in a maritime environment in one experiment, but a researcher considering satellite links would require a different

model. Software such as MODTRAN[32] or FASCODE[33] with an aerosol model is suggested in these cases.

It is worth considering the effects of aerosols on polarization. After all, particles can scatter different polarizations in different directions[34]. Since QKD is done at the single photon level, when a single photon is scattered and depolarized, it is highly unlikely that it will be detected, due to the small solid angle occupied by the receiver. Thus, the photon is simply lost in transit and does not contribute to error rate.

1.3.2 Turbulence

The sun's (or indoor heating and cooling systems') unequal heating of the air causes different turbulent eddies to form. These eddies vary in size and the variance of pressure within and between different eddies causes slight variation in optical properties of the medium.

Modeling the content of each eddy is, of course, quite complicated. Hence, we make use of Taylor's Frozen Flow Hypothesis which states that we can consider each eddy as a fixed, albeit transparent, object which moves according to local wind speed. This is illustrated in Figure 1.3.

We consider the eddies to stay in a "frozen" shape as they move in unison. Thanks to this model, we only need to consider the wind speed and height above ground when computing the effects of turbulence. According to [35], the refractive index in air at optical frequencies is:

$$n = 1 + 77.6(1 + \frac{7.52 \times 10^{-3}}{\lambda^2})\frac{P}{T} \times 10^{-6} \tag{1.6}$$

Where λ is the wavelength in micrometers and P is pressure in millibars. Since pressure variations have a relatively smaller impact on the index of refraction, they can be neglected here[36]. If we assume $\lambda = 1550nm$ like in much of this document, we arrive at:

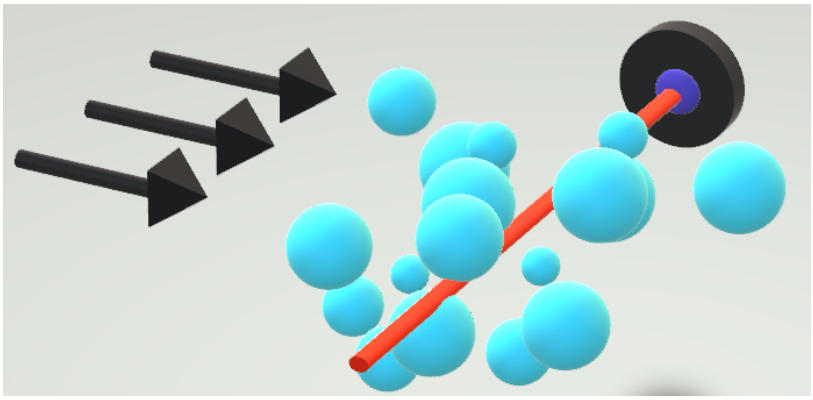


Figure 1.3: Each of the bubbles represents a turbulent eddy of some size. The Taylor Frozen Flow hypothesis asserts that the eddies can be considered to be "frozen in place" and moving together according to the local wind

$$\frac{dn}{dT} = -77.8\frac{P}{T^2} \times 10^{-6} \tag{1.7}$$

Near sea level, the fluctuation is on the order of 10^{-6}. Temperature variations have an impact on long range paths. The pockets of turbulent air with somewhat constant index of refraction are the eddies.

The eddies vary considerably in size, often from the scale of millimeters, to several meters[36]. The eddies' sizes follow a statistical distribution, Φ. If we restrict our analysis to isotropic turbulence, we can describe each eddy with just one wavenumber, $\kappa = \frac{2\pi}{L}$ where L is the size of the eddy.

Kolmogorov originally defined Φ as[37]:

$$\Phi_n(\kappa) = .033C_n^2\kappa^{-11/3} \tag{1.8}$$

Where C_n^2 is for scaling. Technically, Φ spans the region $(0, \infty)$, but eddies larger than the channel in question seldom need to be considered[36] and neither do eddies that contain a larger region than the Earth's atmosphere! More practically, isotropic eddy sizes are limited by the height from the ground at which the experiment is conducted. This upper bounding size is called the outer scale of turbulence and its length is often designated L_0 or wavenumber κ_0.

At the low end, eddies eventually become so small that the viscosity of air dissipates them. Tatarski was able to modify Kolmogorov's model by[36]:

$$\Phi_n(\kappa) = .033C_n^2\kappa^{-11/3}\mathrm{e}^{\frac{-\kappa^2}{\kappa_m^2}} \tag{1.9}$$

The corresponding length for κ_m is a few millimeters and is given by: l_0. If we restrict our analysis to situations where the eddy size is $l_0 \leq l \leq L_0$ we can simply continue to use Kolmogorov's expression for the eddy size Φ.

In Equation 1.8, C_n^2 is often what used to characterize the turbulence severity in the context of transmittance fluctuation. C_n^2 typically ranges from $10^{-17}m^{-2/3}$ for weak turbulence to $10^{-12}m^{-2/3}$ for strong. A typical value is usually $10^{-15}m^{2/3}$. C_n^2 is measured using a scintillometer and different groups such as [38, 39, 40] have measured its diurnal change.

As stated previously, C_n^2 can be modeled using just wind speed and height above ground. A common model describing the relationship is Hufnagel-Valley[41] and is given by:

$$C_n^2(h) = .00594(\frac{v_w}{27})^2(10^{-5}h)^{10}\mathrm{e}^{\frac{-h}{1000}} + 2.7 \times 10^{-16}\mathrm{e}^{\frac{-h}{1500}} + \hat{A}\mathrm{e}^{\frac{-h}{100}} \tag{1.10}$$

Where v_w is the wind speed, h is the height above g round, and $\hat{A}$ is the nominal value of C_n^2 at ground height. In this dissertation, we consider horizontal paths so we can assume constant values for C_n^2.

Lognormal Model of Optical Transmittance

Now we are ready to begin deriving the lognormal distribution for the transmittance fluctuation in turbulence. As shown previously, the beamfront will gradually be corrupted as it propagates through a random medium such as an atmosphere and C_n^2 characterizes the intensity variation. When one uses Maxwell's equations for a spatially variant dielectric, we can arrive at[36]:

$$\nabla^2\vec{E} + k^2n^2\vec{E} + 2\nabla[\vec{E}\cdot\nabla\ln(n)] = 0 \tag{1.11}$$

Where k is the angular wavenumber and n is the index of refraction, including variations due to turbulence. When turbulence is weak, it is unlikely the wave undergoes multiple scatterings and becomes depolarized[42]. Thus, we can ignore the leftmost term to leave:

$$\nabla^2 \vec{E} + k^2 n^2 \vec{E} = 0 \tag{1.12}$$

Tatarski showed that this equation can be solved using the Rytov transformation[43], where the solution takes the form of $\Psi(x) = \ln(E(x))$. Equation 1.12 now looks like:

$$\nabla^2 \Psi + (\nabla \Psi)^2 + k^2 (1 + n_1)^2 \tag{1.13}$$

Where we are approximating the index of refraction as 1+ a perturbation due to turbulence, n_1. If we now substitute for $\Psi = \Psi_0 + \Psi_1$, we can proceed using the method of small perturbations to get:

$$\Psi_1(x) = \Psi(x) - \Psi_0(x) \tag{1.14}$$

$$= \ln(E(x)) - \ln(E_0(x)) = \ln(\frac{E(x)}{E_0(x)}) \tag{1.15}$$

Now, because the total electric field has the form $E(x) = A(x)\mathrm{e}^{i\phi(x)}$ (or E_0, A_0 and ϕ_0 in the static atmosphere case), we have:

$$\Psi_1(x) = \ln(\frac{A(x)}{A_0(x)}) + i(\psi(r) - \psi_0(r)) = \chi + iS \tag{1.16}$$

S will be suppressed in further steps because it is just a phase and χ contains the fluctuations of interest. Since Ψ_1 is Gaussian distributed, χ follows a lognormal distribution which looks like:

$$P(\chi) = \frac{1}{\sqrt{2\pi\sigma_\chi^2}} \mathrm{e}^{-\frac{(\chi-\bar{\chi})^2}{2\sigma_\chi^2}} \tag{1.17}$$

Here P is the lognormal probability density function. We will refer later to it as the Probability Density Function of the Transmittance Coefficient(PDTC). σ_χ^2 is proportional to the σ^2 mentioned copiously in the rest of this document. The former is called the Rytov parameter and $\sigma_l^2 = 4\sigma_\chi^2$. From this point, we will work only with σ_l^2 and abbreviate it as simply σ^2. If we assume our beam front is a plane wave, σ^2 is related to C_n^2 as:

$$\sigma^2 = .14k^{\frac{7}{6}} \int_0^L C_n^2(x)(L-x)^{\frac{5}{6}} \mathrm{d}x \tag{1.18}$$

Where L is the length of the channel. If we further assume a horizontal path, we get the result:

$$\sigma^2 = 1.23C_n^2 k^{\frac{7}{6}} L^{\frac{11}{6}} \tag{1.19}$$

So now σ^2 will used as the parameter which characterizes strength of turbulence.

Chapter 2

BB84 in a Turbulent Atmosphere

The Bennett Brassard 1984 (BB84) protocol[13] is perhaps the most famous method of quantum key distribution. It essentially just requires that bits be encoded on photons in two different bases by Alice, and measured in two different, random bases by Bob. The bits can be encoded in polarizations, time bins, phases, and even a photon's orbital angular momentum[44].

Suppose we are new to quantum mechanics and we are transitioning from classical laser communication. Beamsplitters or half silvered mirrors could be used to simply separate light from a beam. Much communication happens using On Off Keying (OOK) where intensity is modulated. In principle, an eavesdropper could use a beam splitter with some decent quality detectors to collect an entire copy of the signal. Quantum Key Distribution, and also the No Cloning Theorem[17] helps protect against this problem due to the fact that we encode information on single photons; light cannot be split forever.

Still, such a technique is still an omnipresent concern in quantum cryptography. As for the source of quantum level light, we have different choices. Pseudo-single photon sources exist, for example spontaneous four wave mixing or spontaneous parametric downconversion[45], but they emit light in a probabilistic fashion and they can be difficult to set up. As a result, quantum information experiments with single photons may require "frames" of classical communication in order to time and

correlate detection events, like in [46]. Thermal sources of light, such as LED's have also been discussed in [47, 48, 49]. Attenuated laser pulses, also known as weak coherent pulses, remain the most common light source for QKD.

2.1 Decoy States

Because the photon number distribution of coherent states is still Poissonian distributed, we always have some likelihood of sending multiple photons in a pulse. Therefore, we must keep our average number of photons per pulse less than 1. QKD becomes a balancing act, where one must keep the average photon number low to prevent the PNS attack, but high enough to maintain a usable key throughput. One might think to monitor eavesdropping through monitoring detection statistics. However, suppose we have a sophisticated Eve who can block all single photon states and only let the multiphoton pulses through after she steals one of the photons. This might damage the distribution, but she just needs to ensure the number of expected vacuum states remains the same, since most single photon detectors are not able to discriminate multiple photons. Such an attack is described in [50].

Lutkenhaus's sophisticated PNS attack is powerful. Two countermeasures were proposed: the Scarani-Acin-Ribordy-Gisin (SARG) protocol[51], and the inclusion of non-data-carrying decoy states[52, 53]. In the QKD experiments described in this dissertation, decoy states are used.

To describe decoy states in more detail and derive useful quantities, we should first define fundamentals[54]. The probability of Alice's pulse of n photons reaching Bob across a channel where the transmittance is η is given by:

$$Y_n = Y_0 + (1 - (1 - \eta)^n) \tag{2.1}$$

where the second term in parenthesis is the probability of a pulse with n photons reaching the other side. The rationale is that if Alice's pulse has two photons, then the joint likelihood of Bob not detecting any of them is the square of 1 minus the

transmittance for each. Y_0 represents the dark count probability, where Bob gets detections without any input from Alice.

Another quantity called the gain, represented by Q, is also useful. It is interpreted as the likelihood of Alice sending a pulse with a specific number of photons, given some average intensity, μ, and having it reach the other side. As such, it is related to the yield and it is given by:

$$Q_n = Y_n \frac{\mu^n}{n!} e^{-\mu} \tag{2.2}$$

If we try to sum over all the n photon pulses for each given intensity, we get an overall gain of:

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{2.3}$$

Now, let us suppose we have 3 intensities where μ_1, μ_2, and μ_3 are the signal, decoy and vacuum intensities, respectively. The intensities are such that $\mu 1 > \mu_2 + \mu_3$. μ_3 is not quite zero because intensity modulators have a finite extinction ratio, often 20-30 dB. As such, the smallest μ_3 is typically .001 photons.

When we send weak coherent pulses, we also send multiphoton pulses. With decoy states, we also send multiple intensities with their own number distributions in each pulse. However, the decoy state formalism has useful features which allow us to place bounds on the likelihood of sending a vacuum pulse, a single photon pulse, etc. We start by expanding Equation 2.3 like:

$$Q_{\mu_2} = Y_0 e^{-\mu_2} + Y_1 \mu_2 e^{-\mu_2} + Y_2 \frac{\mu_2^2}{2!} e^{-\mu_2} + Y_3 \frac{\mu_2^3}{3!} e^{-\mu_2} + ... \tag{2.4}$$

$$Q_{\mu_3} = Y_0 e^{-\mu_3} + Y_1 \mu_3 e^{-\mu_3} + Y_2 \frac{\mu_3^2}{2!} e^{-\mu_3} + Y_3 \frac{\mu_2^3}{3!} e^{-\mu_2} + ... \tag{2.5}$$

We will subtract these equations, and we do not want Y_0 to cancel because we are trying to bound it. Instead, we should eliminate the single photon terms, so we multiply the top and bottom equations like:

$$\mu_2 Q_{\mu_3} e^{\mu_3} - \mu_3 Q_{\mu_2} e^{\mu_2} = (\mu_2 - \mu_3) Y_0 - \mu_2 \mu_3 (Y_2 \frac{\mu_2 - \mu_3}{2!} + Y_3 \frac{\mu_2^2 - \mu_3^2}{3!} + ...) \tag{2.6}$$

Now, because we made μ_3 less than μ_2, the term in parenthesis is always positive. Consequently, we can claim:

$$\mu_2 Q_{\mu_3} e^{\mu_3} - \mu_3 Q_{\mu_2} e^{\mu_2} \leq (\mu_2 - \mu_3) Y_0 \tag{2.7}$$

so

$$\frac{\mu_2 Q_{\mu_3} e^{\mu_3} - \mu_3 Q_{\mu_2} e^{\mu_2}}{\mu_2 - \mu_3} = Y_0^{min} \tag{2.8}$$

This clever trick establishes a lower bound on the detector noise. Dark counts can count toward a secure key because Eve does not control them.

Of course, the main contributor to our key though is the pulses due to single photons. These are immune to the photon number splitting attack because Eve cannot clone them. The decoy state formalism provides a similar strategy for finding a lower bound on the number of single photon events. We can start similarly to the case where we arrived at 2.6, but we cancel the Y_0 term instead. Then, using an inequality described in [54], we get:

$$Q_{\mu_2}e^{\mu_2} - Q_{\mu_3}e^{\mu_3} = Y_1(\mu_2 - \mu_3) + \sum_{n=2}^{\infty} \frac{Y_n}{n!}(\mu_2^n - \mu_3^n) \tag{2.9}$$

$$\leq Y_1(\mu_2 - \mu_3) + \frac{(\mu_2^2 - \mu_3^2)}{\mu_1^2} \sum_{n=2}^{\infty} Y_n \frac{\mu_1^n}{n!} \tag{2.10}$$

We can then substitute the overall gain of the signal state for the sum and reintroduce a Y_0 term:

$$Y_1(\mu_2 - \mu_3) + \frac{(\mu_2^2 - \mu_3^2)}{\mu_1^2} \sum_{n=2}^{\infty} Y_n \frac{\mu_1^n}{n!} = Y_1(\mu_2 - \mu_3) + \frac{(\mu_2^2 - \mu_3^2)}{\mu_1^2}(Q_{\mu_1}e^{\mu_1} - Y_0 - Y_1\mu_1) \tag{2.11}$$

However, we can use our bound for Y_0. After manipulation, we arrive at:

$$Y_1^{min} = \frac{\mu_1}{\mu_1\mu_2 - \mu_1\mu_3 - \mu_2^2 + \mu_3^2}(Q_{\mu_2}e^{\mu_2} - Q_{\mu_3}e^{\mu_3} - \frac{\mu_2^2 - \mu_3^2}{\mu_1^2}(Q_{\mu_1}e^{\mu_1} - Y_0^{min})) \tag{2.12}$$

A discussion of error estimation is also due. Errors come from two sources in BB84: detector noise and misalignment. Dark counts were discussed earlier, while misalignment is simply the probability that a photon will be detected as the incorrect polarization in a basis. Given some photon number in a pulse, the associated error is:

$$e_n = \frac{\frac{1}{2}Y_0 + e_d\eta_n}{Y_n} \tag{2.13}$$

I am assuming the dark counts on the detectors are the same. Otherwise, the $\frac{1}{2}$ in the first term would be polarization dependent. To gain intuition, we should analyze Equation 2.13. Suppose we shrink our signal down, such that our single photon yield is comparable to the dark counts. Eve would have very few multiphoton pulses at her disposal to split. However, our error rate would be quite large; too large to ascertain if Eve were present anyway. As such, we must choose an optimum between a low error

rate, and having a high probability of sending multiple photon pulses. The overall Quantum Bit Error Rate (QBER) is given by:

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Y_n \frac{\mu^n}{n!} = \frac{1}{2} Y_0 + e_d(1 - e^{-\eta\mu}) \tag{2.14}$$

Just like with gain, each decoy intensity has its own corresponding QBER. Now, we should be concerned with the QBER for the single photon events. We can place an upper bound on them just like what we did with the single photon and vacuum yields:

$$E_{\mu_2} Q_{\mu_2} e^{\mu_2} = \frac{1}{2} Y_0 + e_1 \mu_2 Y_1 + \sum_{n=2}^{\infty} e_n Y_n \frac{\mu_2^n}{n!} \tag{2.15}$$

$$E_{\mu_3} Q_{\mu_3} e^{\mu_3} = \frac{1}{2} Y_0 + e_1 \mu_3 Y_1 + \sum_{n=2}^{\infty} e_n Y_n \frac{\mu_3^n}{n!} \tag{2.16}$$

We can subtract the equations and, again since the sum is always positive, we can establish a bound by discarding it and inserting an inequality. Now we get:

$$e_1^{max} = \frac{E_{\mu_2} Q_{\mu_2} e^{\mu_2} - E_{\mu_3} Q_{\mu_3} e^{\mu_3}}{(\mu_2 - \mu_3) Y_1^{max}} \tag{2.17}$$

Now, instead of calculating the single photon error rate exactly, we are just finding an upper bound using the fact $\mu_2 > \mu_3$ and that we have a bound on the single photon yield, Y_1^{min}.

It must be noted that we have not included any finite size effects in our derivations so far. Normally, when one does QKD in a real scenario, they send a long key and then they must estimate the security of the key by sacrificing a sample of key to determine the error rate. The quality of this sample, and statistical fluctuations give rise to nontrivial uncertainty in our derived terms and, depending on worst case estimates,

they may void our key altogether! In another section, we will discuss how finite size effects should be incorporated.

The decoy state protocol allows us to use coherent states much more securely. In a simulation in [53], the maximum possible distance was expanded considerably as shown in Figure 2.1 using the experimental parameters from the oft-cited experiment in [55].

Decoy states work in part because given a pulse, an eavesdropper cannot tell whether what the intended intensity is, assuming the states' phases are properly randomized[56, 57]. The assumption is valid, and is shown in [58]. They make the source more secure, but there are unaddressed attacks, such as a trojan horse attack where an eavesdropper sends light to Alice to gain phase information from the reflection. A nice overview of different hacking techniques can be found in [59].

Builders of a real life implementation must be mindful of the different known attacks and be prepared with countermeasures. Beyond the photon number splitting attack, the different hacking techniques are not addressed in this work. However a new protocol, Measurement Device Independent(MDI) QKD, which removes all detector side attack vectors, will be discussed in another chapter. To make our BB84 experiment more secure, we must show that it can survive finite size analysis in the next section.

2.2 Finite Size BB84

Alice and Bob have all the necessary equipment and they are ready to generate a secure, unhackable key. What happens next? QKD has postprocessing requirements such as error verification and correction, and privacy amplification. Some information in this step will need to be encrypted. Not to mention, Alice and Bob need to verify whether they are forming keys with each other and not Eve! Postprocessing steps are summarized in Figure 2.2.

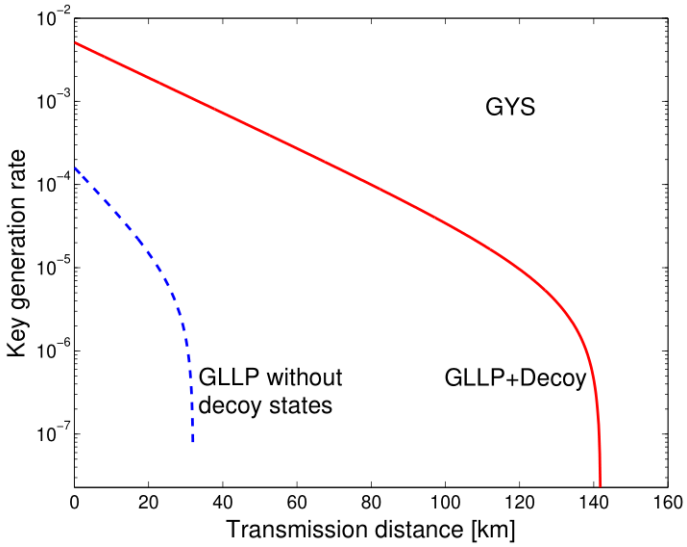


Figure 2.1: Key rate is computed using a security proof assuming some limited control of the detectors and source by Eve[66]. The calculation assumes parameters identical to the experiment in [55]. We see a significant increase in key rate in part because the decoy state protocol allows us to confidently use higher photon numbers. Taken from [53].

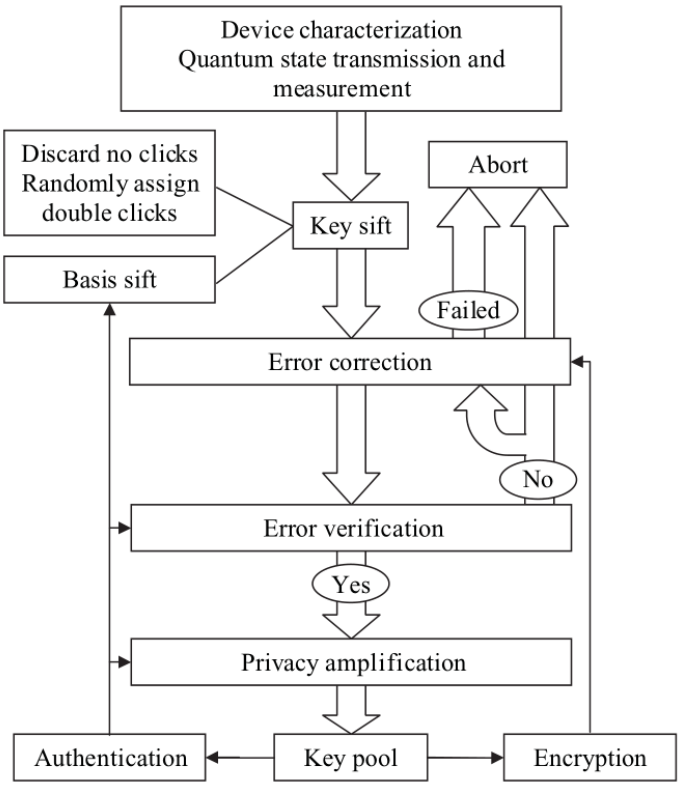


Figure 2.2: Flow chart of all the steps required for a QKD deployment. Our experiment in [1] only completed up to the key sift. We predicted key loss in further steps by assuming postprocessing parameters like error correcting efficiency. Taken from [61].

For the latter problem, Authentication does not have a perfect solution at the time of writing. Quantum Position Verification such as [60] offers a practical technique where Alice and Bob can show that they are communicating with each other based on their location coordinates. In that scheme, Eve would need to possess a quantum computer to defeat the protocol. In these works, we will skip the authentication step.

Alice and Bob will generate a large key using the BB84 protocol, then they must sacrifice part of their exchanged key to ensure it is secure. Once their data is shared, they must announce the basis choices for each bit, but not its value in a procedure called "sifting". At this point, Alice and Bob only have bits measured in the basis they were encoded in.

In addition, errors must be corrected in the key. Two common methods include the Cascade protocol[62], which uses many back and forth communications between Alice and Bob, and a variation of the LDPC protocol[63], which requires a large amount of processing power. Since LDPC is just bottlenecked by computers, we can expect it to become more commonplace as GPU computing becomes more popular. 5G communications also use the LDPC[64], so a future quantum internet may be able to use some existing infrastructure.

Regardless of the error reconcilliation procedure we use, we want to correct the errors in Bob's key while giving away as little information as possible. At a minimum, it costs $nH_2(e)$ bits to correct an error rate of e buried in n sifted bits. However, error correction schemes do not reach this limit, so there is an extra factor of f_{EC} to multiply this term. All the communication required in error correction must be encrypted so Eve cannot make use of it[61]. Ideally, it is encrypted using previously generated quantum keys.

Qubits are quite different from classical bits, because in addition to having a parity, the bits also have phase. The phase errors can be thought of as the error rate had the photons detected in the rectilinear basis been instead detected in the diagonal basis. Indeed, one of the early security proofs of QKD requires a quantum computer[65]. Our error correction step can only correct the bit errors.

Early on in QKD, the qubits would have to have their errors corrected prior to measurement because detecting them would "squash"[66] them into a smaller(in Hilbert space) state. Now, we may measure them prior to correcting errors because of a proof in [67]. Shor and Preskill reduced the problem of measuring EPR pairs of photons to a "Prepare and Measure" scheme. Several conditions need to be met for us to adopt this convenient paradigm shift. They are nicely summarized in [10].

The next step is error verification. Alice and Bob must share a part of their key randomly to determine the error rate. This step is needed to ascertain whether there was eavesdropping and influence the length of the final key after privacy amplification.

The final step is privacy amplification. At this point, Alice and Bob must know how long their final key will be. Thanks to the prepare and measure scheme, instead of correcting phase errors, we can just multiply the sifted, error corrected key by a random Toeplitz matrix to generate the final key.

A Toeplitz matrix has all the same elements diagonally downward from left to right. Due to its symmetry, Alice and Bob only need to share 2w - 1 bits to exchange one, where w is the number of columns; communication would be too costly otherwise. The number of rows is the length of the final key, as determined by Equation 2.18. We cannot encrypt this step simply because the 2w - 1 bits needed to share a Toeplitz matrix is at least twice the size of our final key!

At this point, we are ready to describe the secure key rate while taking into account finite size effects. According to Lim[68], we have:

$$l = [s_{\mathrm{X},0} + s_{\mathrm{X},1}(1 - H_2(\phi_{\mathrm{X}})) - f_{EC} n_X H_2(eRate) - 6\log_2(\frac{21}{\epsilon_{\mathrm{sec}}}) - \log_2(\frac{2}{\epsilon_{\mathrm{cor}}})] \quad (2.18)$$

In Equation 2.18, the first two terms correspond to the lower bound on the number of vacuum events and the lower bound on the number of single photon events. These are the only two types of pulses that are not vulnerable to the photon number splitting attack. The third term describes the number of bits that would be needed to correct phase errors, while the fourth term is those needed to correct bit errors. The last term

is just the bits that must be revealed when error verification is performed. Likewise, ϵ_{cor} is the correctness of the final key.

Because of the possibility of sampling errors, the terms must also assume some confidence interval, determined by the ϵ_{sec}. All the terms in Equation 2.18 are given explicitly in Appendix A.

The fifth term comes from a parameter called the secrecy, which is essentially the confidence of your security. When using finite keys there is some nonzero failure probability. This is reflected by our choice of ϵ_{sec}. A derivation of the secrecy can be found in [69].

2.3 BB84 in Turbulence

Now, we are ready to introduce the effects of turbulence to our BB84 model. Because it causes deformation of the beam front and wandering, there is a large effect on the intensity Bob receives. As shown in Section 1.3.2, it leads to a lognormally distributed intensity, given the turbulence is not extremely strong. A good chunk of the data will have a lower intensity than preferred, and as a result the error rate will be higher. Single photon-level beams still follow this distribution, as shown in [70, 71, 72]. More general studies of qubits in turbulence are given in [73, 74, 75, 76]

Naturally, we want to reduce the error rate and negate the effects of turbulence. It will change the transmittance significantly on the order of milliseconds[77], so one strategy might be to discard detections received during some ms length time bin such that the overall error rate is decreased, despite the decrease in total data size. Erven[78] devised a scheme where detections would be filtered out from some variable time period if there were too few. They devised a noise filtering algorithm to select time periods where transmittance is higher.

The next development by Vallone *et. al.*[79] sent a stronger, beacon laser to probe the turbulence at any given time (this laser will also be interchangeably called probe or classical). This beacon beam does not carry information, and its frequency

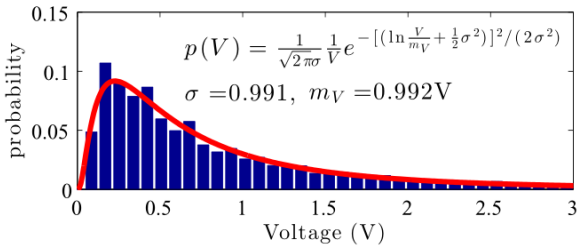
is slightly different from the single photon beam (referred in this document as the quantum channel).

Vallone's group used a 143 km channel between Tenerife and the JKT obervatory on La Palma island. They made qubits by attenuating 850 nm lasers, then in the same path, they sent an 808 nm beacon beam. The beams were separated using a dichroic mirror on Bob's side. They use a similar frequency to accurately predict any diffractive effects in the quantum beam. They then monitor the intensity of the classical beam and use it to identify time bins where the intensity of the quantum channels is likewise low. The fluctuations of the probe beam is given in Figure 2.3a.

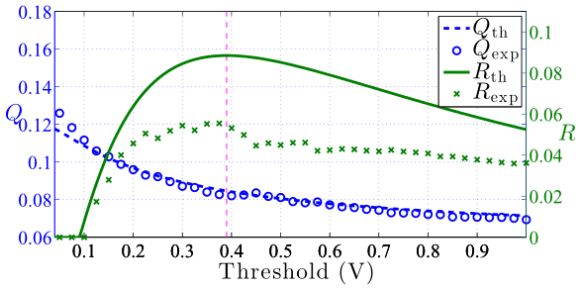
If we know the intensity of the classical laser and we assume it follows the intensity of the quantum beam, we can infer that it follows the error rate in the quantum beam. If the time bins where the quantum beam has low intensity, then we can lower the overall error rate. This method, called Adaptive Real Time Selection (ARTS), works by iterating through different choices of a cutoff value to find the one that gives the best key rate. In Figure 2.3b, the red curve represents the asymptotic key rate (infinite or Shor-Preskill rate) and the blue gives the error rate as a function of the cutoff. The dotted line gives the optimal key rate and takes into account both the discarding of bits and the reduced error.

The result is quite impressive. In some situations, when turbulence induced loss is heavy, the intensity may be too low and the error rate may be too high for a secure key rate to be achievable. In their experiment, through ARTS, they showed we can discard data and obtain a key when it otherwise would not be possible.

The ARTS protocol demonstrated good improvement, but it was further refined by Wang *et. al.*[80]. It was shown that the ARTS' iterative process was unnecessary because the optimal threshold could be determined solely by other experimental parameters (i.e. misalignment, dark counts). This new protocol, the Prefixed-Threshold Real Time Selection(PRTS) also has the advantage of immediately discarding bits where the intensity is below the critical threshold, thus freeing up memory and eliminating some postprocessing.



(a) Probe beam statistics from the ARTS experiment[79]. Detector voltage, follows the expected lognormal distribution.



(b) The QBER and asymptotic key rate as a function of the cutoff voltage.

Figure 2.3: Both taken from [79]. The top panel shows the detector voltage, proportional to intensity follows a lognormal distribution. The bottom panel shows their ARTS method, where intensity cutoffs are iteratively applied to decrease overall error rate and improve security.

To arrive at Wang *et. al.*'s conclusion, we must define important quantities. First, suppose we have a classical detector or power meter with infinite resolution. Suppose also we are sending an infinite key that's given by the Shor-Preskill rate. Using the PDTC, we can find the total key through a variably visible channel using the integral:

$$R_{Ratewise} = \int_0^1 P_{\eta_0,\sigma}(\eta) R(\eta) d\eta \tag{2.19}$$

We shall refer to Equation 2.19 as the Ratewise model. It takes into account all the channel fluctuations. The integration occurs over all infinitesimally thin bins where transmittance is assumed to be constant and the infinite secure key is computed for each bin. Each bin contributes non-negative secure key, so we can confidently integrate from 0 to 1 without worrying about a threshold. In fact, using the Ratewise model with a cutoff would shrink the key rate due to this condition.

Now, in the non optimal model, resolution will not be infinite. It is instead assumed that when we postselect high transmittance data, we are just increasing the average η of the remaining bits, thereby raising the secure key rate(we will continue ignoring finite size effects for now). We would then compute the secure key rate like:

$$R_{Simplified}(\eta_T) = \int_{\eta_T}^1 P_{\eta_0,\sigma}(\eta) R(<\eta>) d\eta \tag{2.20}$$

where η_T represents the cutoff transmittance below which all bits are discarded. We calculate R using the average transmittance which is determined by:

$$<\eta> = \frac{\int_{\eta_T}^1 P_{\eta_0,\sigma}(\eta)\eta d\eta}{\int_{\eta_T}^1 P_{\eta_0,\sigma}(\eta)} \tag{2.21}$$

Let us return to Equation 2.20. At very low transmittances, the secure key rate as a function of average transmittance is quite linear and the situation is similar for decoy BB84. Equation 2.20 becomes:

$$R_{Simplified}(\eta_T) = \int_{\eta_T}^{1} P_{\eta_0,\sigma}(\eta) R(<\eta>) d\eta \tag{2.22}$$

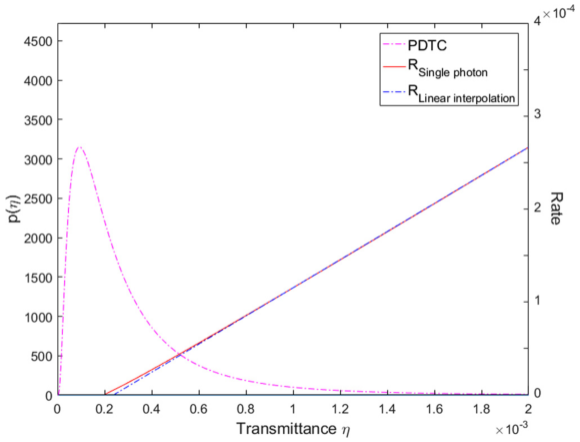
$$\approx R(<\eta>) \int_{\eta_T}^{1} P_{\eta_0,\sigma}(\eta) d\eta \tag{2.23}$$

The optimal η_T is found when $R(\eta)$ goes to zero. If we cut off the time bins where transmittance is lower than this cutoff, we are not eliminating any contributions to the key rate. This effect can be seen in Figure 2.4 for both the Shor Preskill Rate and the GLLP[66] rate.

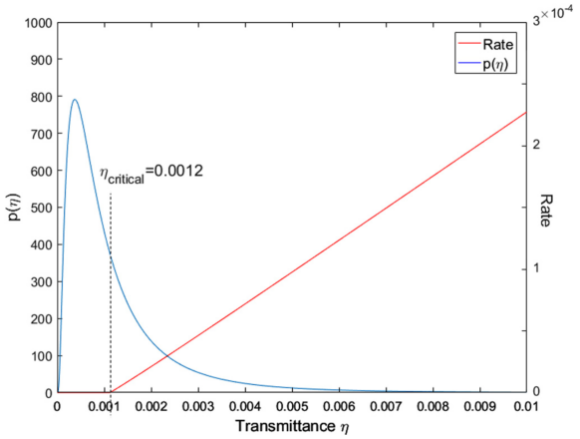
This result has interesting implications because it does not depend on the actual distribution of the transmittance. The optimal threshold can be found using just $R(\eta)$ and seeing where it goes to zero given experimental parameters like detector efficiency. Whereas ARTS finds the optimal cutoff after the intensity distribution is known, the PRTS method finds it a priori.

2.4 Testing PRTS and ARTS in Simulated Turbulent Conditions

In [1], we see how PRTS and ARTS both perform when we simulate turbulence. Although the previous section suggests PRTS is independent of the PDTC, knowledge of it is still important when optimizing the decoy parameters. In turn, this dependence impacts the threshold yielded by PRTS. When we perform an optimization routine to find decoy parameters, we need to have a good idea of the average transmittance.



(a) GLLP key rate linear approximation



(b) Determining optimal cutoff in PRTS

Figure 2.4: Both taken from [80]. If the GLLP key rate is plotted as a function of transmittance η, it can be well approximated by a linear function, as shown in the top panel. To find the optimal cutoff, we look for when the contributions to the positive key stop as shown in the bottom panel. The PDTC, though unused, is also plotted to show where the transmittance threshold may occur on the distribution.

The problem boils down to how well we can predict the transmittance of our atmospheric channel. Since the PDTC is a lognormal distribution, as shown in Equation 2.24, two parameters contribute to the average transmittance: η_0 which is impacted by the static loss of the channel and σ which is the strength of the turbulence.

$$P(I) = \frac{1}{\sqrt{2\pi}\eta\sigma} e^{\frac{(ln(\frac{\eta}{\eta_0}) + \frac{\sigma^2}{2})^2}{2\sigma^2}} \tag{2.24}$$

As shown in Section 1.3, it is not often difficult to predict η_0, assuming one is armed with the right tools like MODTRAN[32] or FASCODE[33], but σ can vary significantly because C_n^2 can vary widely over a 24 hour period[36]. We can make predictions about the strength of the turbulence using Equation 1.19, for instance, but little is possible beyond that.

The decoy parameters are optimized to give the highest secure key rate assuming an average loss. The optimal threshold for PRTS is determined at the same time. Our experiment compared the performance of PRTS, handicapped by our ignorance of the channel, to ARTS.

2.4.1 Experimental Setup and Procedure

The full setup is given in Figure 2.5. The light source was a modelocked 1550 nm laser (Wavelength References). 2ns pulses were formed using an intensity modulator(IM) where DC bias was controlled using feedback to a null point controller. Polarization modulation occurs in the next step. We use a setup proposed in [81]. First, intensity must be evenly distributed between the fast and slow axes of the phase modulator (PM). This is achieved by inserting a set of polarization controllers prior to a beam circulator. The middle port of which goes to a PM and then to a Faraday Mirror(FM). The FM ensures that whenever the PM experiences temperature dependent shifts in

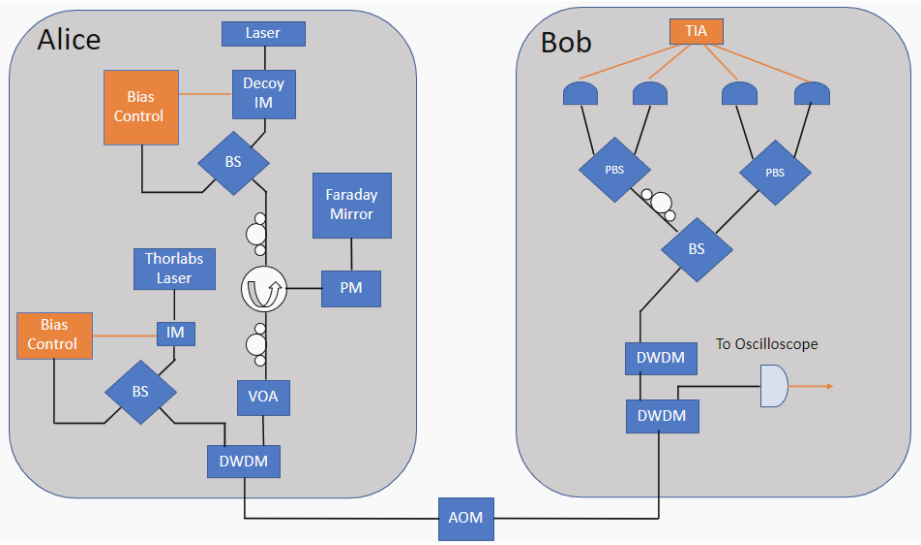


Figure 2.5: Our experimental setup for BB84 with adaptive postselection. Pulses are formed at the decoy intensity modulator (IM) and a beamsplitter (BS) supplied feedback to a null point controller. The polarizations are modulated at a phase modulator (PM) and Faraday mirror combination and the bases are aligned using polarization controller paddles (sets of circles). Pulses are attenuated to single photon level at the variable optical attenuator (VOA) and multiplexed with a higher intensity probe beam at the Dense Wavelength Division Multiplexer (DWDM). An acousto optical modulator (AOM) encodes our desired PDTC on both beams, which are demultiplexed at a second DWDM. Bob automates a random basis measurement using a BS and measures the polarizations using polarizing beam splitters (PBS). Time tags corresponding to detection events are stamped by a time interval analyzer (TIA).

birefringence, they will be experienced equally in both waveguide modes[82]. The exit port of the beam circulator feeds into another set of polarization controllers, which are used to set the bases. Various photon numbers are reached using variable optical attenuation(VOA) prior to being sent over a simulated free space channel.

In this work, turbulence was simulated on an acoustooptical modulator (AOM) which is driven by an arbitrary waveform generator(AWG). The arb that ran on the AWG was produced from lognormally distributed random transmittances between 0 and 1 with an average loss of either 13 dB, 15 dB, 17 dB, or 19 dB. The variance of the distribution was always $\sigma^2 = 0.8$, which corresponds to reasonably strong turbulence in a 3km channel.

Very importantly, the simulated atmosphere was probed so that the optical transmittance was known. Each 8 ms, a pulse was sent from another higher intensity laser at a slightly different frequency(ITU = 29 instead of 33.5 for the quantum channel). Classical pulses were multiplexed with the quantum channel using a DWDM prior to passing through the AOM and they were separated using a De-Mux DWDM. Classical pulses were then measured using a high gain detector and an oscilloscope. We used the oscilloscope's Fast Frame setting, which allowed us to measure the area of the pulse with high resolution at irregular time periods. The areas were calibrated to transmittances prior to data collection.

In the quantum channel, we isolated the quantum from classical light by passing it through two De-MUX DWDM's and using gating on the single photon avalanche detectors (SPAD). In front of the Bob's detectors, we passively selected the measurement basis using a beam splitter(BS). Then, a set of polarization controllers is used on one side to align one of the polarizing beam splitters (PBS) to the diagonal basis. The other side of the BS goes to a PBS which measures the rectilinear basis. This way, each detector is effectively assigned one polarization to measure.

Each detection was time tagged by a Time Interval Analyzer (TIA) and the data files with the time tags and detection events were analyzed by a homemade computer program.

Using the marker signals from the "SYNC" channels in the AWG's, we matched the polarizations measured as indicated by the detector number with the polarization we intended to send at a given period. Data sets were run for about 30 minutes each. The data sets were varied for the average loss, and the average loss anticipated in the decoy optimization routine. On each data set we applied the ARTS method and compared it to the PRTS method's rough prediction. Our decoy parameters are given in Table 2.1.

2.4.2 Results

The purpose of this experiment was to find a threshold using the PRTS method prior to data collection and compare it to a more brute force ARTS method which checks the whole set of transmittance cutoffs to achieve the highest secure key rate. In this way, we treat ARTS as though it will always give the highest key rate. At best, PRTS can achieve the same key rate as ARTS, but its real advantage is the fact the one does not require knowledge of the distribution to find an optimal cutoff. This experiment essentially tried to test how well PRTS could perform when we made the channel different from the conditions where the PRTS cutoff was estimated. Results are contained in Figure 2.6.

In Fig 2.6, the middle column represents an accurately predicted channel loss then the two outer columns represent a channels with 2dB loss more or less than anticipated. In other words, we tested the robustness of PRTS' cutoffs (given in Figure 2.7) to give the best result. The yellow regions, which were predicted by PRTS, include the maximum of the key rate curve in each of the plots. A range of values is used in the event that we only know the loss is between 10 and 19 dB. Thus, we showed that PRTS indeed gives a region where the optimal cutoff may be found.

Figure 2.7 also shows that the optimal cutoff is very inelastic with respect to higher or lower turbulences. Rather, the optimal cutoff is more influenced by the number of pulses sent and other experimental parameters, like dark count rate.

Table 2.1: Decoy Parameters for our experiment in [1]

Mean Loss (dB)	q_X	P_{μ_1}	P_{μ_2}	μ_1	μ_2
11	.904	.660	.215	.56	.225
13	.879	.617	.244	.56	.23
15	.844	.552	.287	.56	.23
17	.789	.46	.352	.54	.24
19	.683	.319	.439	.54	.245

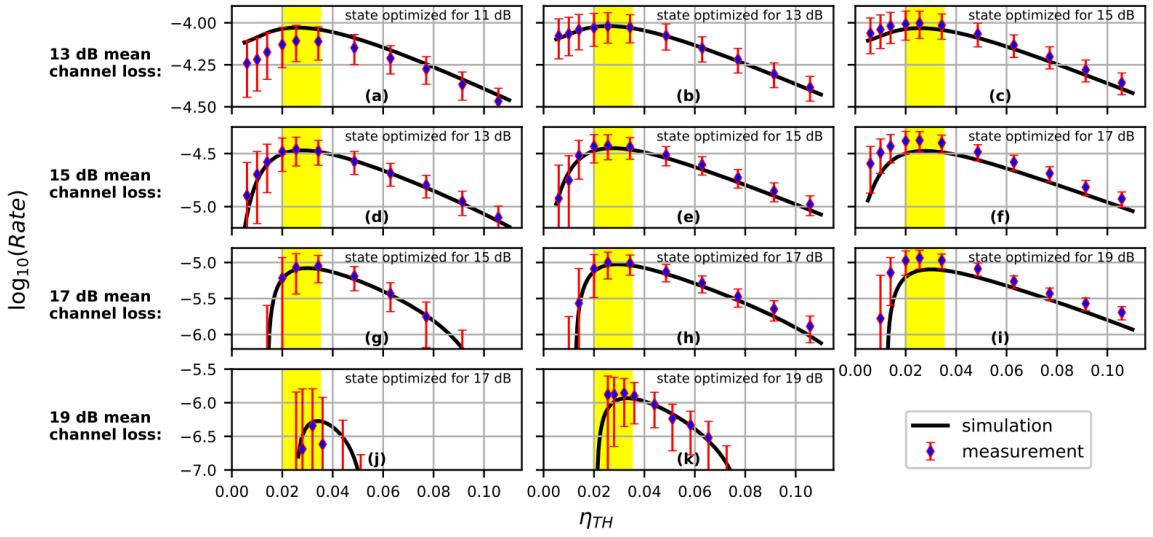


Figure 2.6: Taken from [1]. Each plot is produced in a simulated atmosphere with the same amount of turbulence, but with different losses and different amounts of anticipated loss. Continuous lines are produced using a simulation where the cutoff is determined using ARTS, while the points correspond to various cutoffs applied to a single data set with the same parameters. PRTS's predicted optimal threshold is the yellow region because we assume we only have knowledge of the channel loss to within 4 dB when optimizing our decoy parameters.

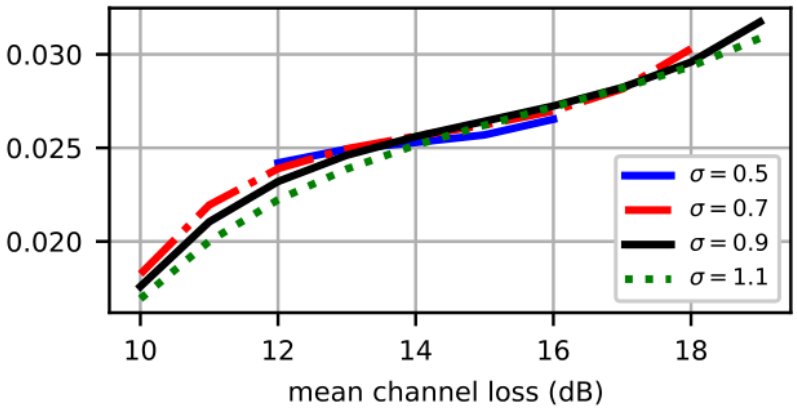


Figure 2.7: Robustness of optimal cutoff for PRTS. We see that different values of σ, or the level of turbulence, have little impact on the choice of the transmittance threshold. Also in [1]

In this work, we showed that the PRTS method provides an effective means for reducing noise in a turbulent atmospheric channel. We show that only a vague knowledge of the channel is sufficient to predict the decoy parameters, and the optimal cutoff. As the authors show in [80], like in ARTS, it can even provide a secure key where it otherwise would not be possible.

Chapter 3

Hong Ou Mandel Interference with Device Imperfections

Quantum Optics has lead to the discovery of a very useful and uniquely quantum mechanical finding called the Hong Ou Mandel (HOM) effect. Suppose two photons are incident on a beam splitter. One of four outcomes can occur, as shown in Figure 3.1

In Figure 3.1, the outcomes depend on each combination of whether the photons are reflected or transmitted. If both photons are reflected, they each pick up a phase of i so the overall phase of outcome 2 is negative. Now, if we have two identical photons, the two outcomes in the middle of 3.1 are identical, but completely out of phase. This means the amplitudes will cancel and the identical photons will exit through the same port.

To understand this more formally, we will begin with a description of the beam splitter. The input and output modes can be written in terms of creation and annihilation operators like in Figure 3.2.

Since a beam splitter does not dissipate energy, it can be represented as a unitary operator[83]. If we assume the beam splitter is 50/50, we can rewrite the annihilation operators as:

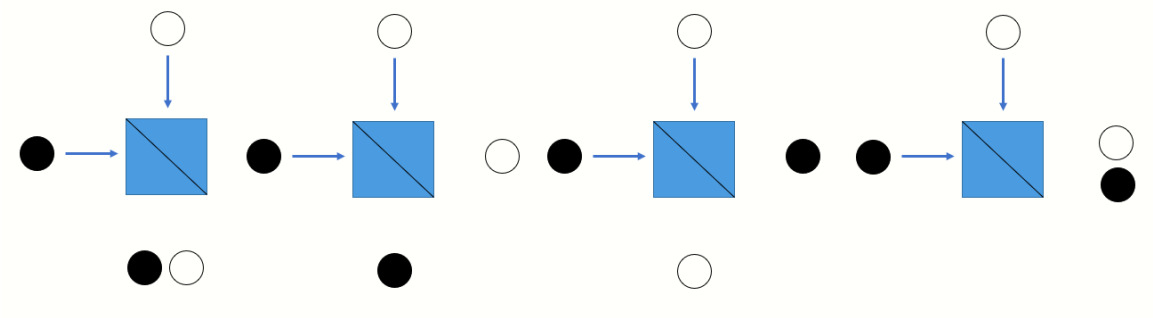


Figure 3.1: Possible outcomes for two single photons (black and white) incident on a beamsplitter. Four outcomes would be possible classically, but the Hong Ou Mandel Effect causes the second and third outcomes to destructively interfere when the photons are identical in every degree of freedom. Thus, the photons would exit the same port.

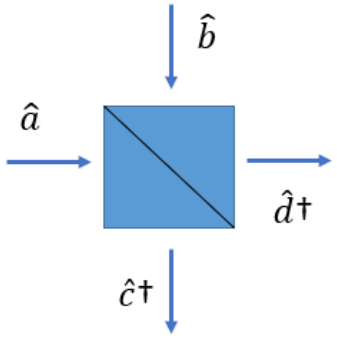


Figure 3.2: Quantum description of beamsplitter. The annihilation operators act on states incident on ports a and b, while c and d are the exit ports and are modeled as creation operators. We can also rewrite $\hat{a}$ and $\hat{b}$ in terms of $\hat{c}^\dagger$ and $\hat{d}^\dagger$.

$$\hat{a} = \frac{1}{\sqrt{2}}(\hat{c} + \hat{d}) \tag{3.1}$$

$$\hat{b} = \frac{1}{\sqrt{2}}(\hat{c} - \hat{d}) \tag{3.2}$$

Now, suppose a single vertically polarized photon is incident on port a and a horizontally polarized one on port b. We can then write the output state of the beam splitter like:

$$\hat{a}_V^\dagger \hat{b}_H^\dagger |0\rangle = \frac{1}{2}(\hat{c}_V^\dagger + \hat{d}_V^\dagger)(\hat{c}_H^\dagger - \hat{d}_H^\dagger) |0\rangle \tag{3.3}$$

$$= \frac{1}{2}(\hat{c}_V^\dagger \hat{c}_H^\dagger - \hat{c}_V^\dagger \hat{d}_H^\dagger + \hat{d}_V^\dagger \hat{c}_H^\dagger - \hat{d}_V^\dagger \hat{d}_H^\dagger) |0\rangle \tag{3.4}$$

Where we write in the Fock state or photon number basis. Each term in Equation 3.4 corresponds to a certain outcome, like in Figure 3.1. Now, suppose we make the single photons have the same polarization. We will also exploit the commutation of the creation operators on ports c and d to get:

$$\frac{1}{2}(\hat{c}^\dagger \hat{c}^\dagger - \hat{c}^\dagger \hat{d}^\dagger + \hat{d}^\dagger \hat{c}^\dagger - \hat{d}^\dagger \hat{d}^\dagger) |0\rangle = \frac{1}{2}(\hat{c}^\dagger \hat{c}^\dagger - \hat{d}^\dagger \hat{d}^\dagger) |0\rangle \tag{3.5}$$

$$= \frac{1}{\sqrt{2}}(|2\rangle_c - |2\rangle_d) \tag{3.6}$$

In Equation 3.6, the two middle terms cancel and we are left with the two terms where both photons exit through the same port. This result is profound and it has been extended beyond just photons. It has also been demonstrated with plasmons[84], phonons[85], Rubidium[86] and Helium[87] atoms, and even electrons[88](albeit behaving Fermionic statistics).

3.1 HOM Visibility in Coherent States

If we try to observe the HOM effect with lasers, we would hit a bound on the visibility. This is due to fact that coherent states can give multiple photons per pulse. We can derive a formula for the visibility of the HOM effect when using them. We will follow a derivation given in [89]. Suppose we have two coherent states $|\alpha\rangle$ and $|\beta\rangle$ incident on ports a and b, respectively. We have:

$$|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle = e^{\frac{-(\mu_A+\mu_B)}{2}} e^{\alpha a^\dagger + \beta b^\dagger} |0\rangle \tag{3.7}$$

Now, we can rewrite the creation operators as dot products of the incident photons' polarizations like:

$$a^\dagger = \hat{\epsilon_a} \cdot \hat{\epsilon_H} a_H^\dagger + \hat{\epsilon_a} \cdot \hat{\epsilon_V} a_V^\dagger \tag{3.8}$$

$$b^\dagger = \hat{\epsilon_b} \cdot \hat{\epsilon_H} b_H^\dagger + \hat{\epsilon_b} \cdot \hat{\epsilon_V} b_V^\dagger \tag{3.9}$$

At the output, the state needs to be described in terms of $c\dagger$ and $d\dagger$, depending on the whether each photon is reflected or transmitted. This gives us:

$$|\psi_{out}\rangle = e^{-\frac{\mu_A+\mu_B}{2}} \prod_{i=H,V} e^{\alpha(tc_i\dagger + rd_i\dagger)\hat{\epsilon_a}\hat{\epsilon_i}} e^{\beta(rc_i\dagger - td_i\dagger)\hat{\epsilon_a}\hat{\epsilon_i}} |0\rangle \tag{3.10}$$

After some manipulation, we can see that the output is still a product of coherent states. The probability of photons exiting each port is:

$$P_{m,n}^{out} = e^{-(\mu_A+\mu_B)} \frac{\mu_C^m \mu_D^n}{m!\, n!} \tag{3.11}$$

Here, μ_C and μ_D are the output photon numbers from ports c and d. They are:

$$\mu_C = \mu_A t^2 + \mu_B r^2 + 2tr\text{Real}(\alpha\beta^*\hat{\epsilon_a}\cdot\hat{\epsilon_b^*}) \tag{3.12}$$

$$\mu_D = \mu_A r^2 + \mu_B t^2 - 2tr\text{Real}(\alpha\beta^*\hat{\epsilon_a}\cdot\hat{\epsilon_b^*}) \tag{3.13}$$

Because the beam splitter is unitary, the sum of the input photon numbers equals the sum of the outputs.

Let us consider the properties of our detectors. We are using Indium-Gallium-Arsenide (InGaAs) detectors like in the BB84 section, hence we cannot discriminate multiphoton detections from singles. Efficiency is not perfect, so at least one photon of the multiphoton pulse must survive. Detector efficiencies will be assumed to be the same, η_D. Dark count probability can be written as $d_{c,d}$. Now, Equation 3.11 becomes:

$$P_{m,n} = P^{out}_{m,n} \times (1-(1-\eta_D)^m(1-d_c))(1-(1-\eta_D)^n(1-d_d)) \tag{3.14}$$

Where $P^{out}_{m,n}$ refers to the photon number pairs just after the beam splitter. So Equation 3.14 is interpreted as the photons we can actually count at the detector. Coincident probability is then:

$$P^{coin} = \sum_{m,n=0}^{\infty} P_{m,n} \tag{3.15}$$

$$= (1-e^{-\eta_D\mu_C}(1-d_c))(1-e^{-\eta_D\mu_D}(1-d_d)) \tag{3.16}$$

We must now consider the input states' phases. The incident coherent states can be written in density matrix notation as:

$$\rho_{in} = \int_0^{2\pi} \frac{d\theta_\alpha}{2\pi} \int_0^{2\pi} \frac{d\theta_\beta}{2\pi} |\psi_{in}\rangle \langle\psi_{in}| \tag{3.17}$$

Taking phase into account, we find:

$$P^{coin} = \int_0^{2\pi} \frac{d\theta_\alpha}{2\pi} \int_0^{2\pi} \frac{d\theta_\beta}{2\pi} P^{coin} \tag{3.18}$$

$$= 1 - \mathcal{C} I_0(2\eta_D \sqrt{\mu_A \mu_B} tr\cos(\Phi)) - \mathcal{D} I_0(2\eta_D \sqrt{\mu_A \mu_B} tr\cos(\Phi)) \tag{3.19}$$

There would be a cross term if we were not assuming equal detector efficiencies on detectors C and D. I_0 is the modified Bessel function of the first kind. $\mathcal{C}$ and $\mathcal{D}$ are:

$$\mathcal{C} = e^{\eta_D(\mu_A t^2 + \mu_B r^2)}(1 - d_C) \tag{3.20}$$

$$\mathcal{D} = e^{\eta_D(\mu_A r^2 + \mu_B t^2)}(1 - d_C) \tag{3.21}$$

In Equation 3.19, Φ represents the angle difference between the input photons' polarizations. HOM visibility is defined as:

$$V_{HOM} = 1 - \frac{P^{coin}}{P^C P^D} \tag{3.22}$$

If we assume small α and β and no dark counts, we have:

$$V_{HOM} \approx \frac{2RT\mu_A\mu_B\cos^2(\Phi)}{(T\mu_A + R\mu_B)(R\mu_A + T\mu_B)} \tag{3.23}$$

We can now use $T = R = .5$ for a 50/50 beam splitter to finally arrive at:

$$V_{HOM} \approx \frac{2\mu_A\mu_B\cos^2(\Phi)}{(\mu_A+\mu_B)^2} \tag{3.24}$$

This function gives values between [0, .5] where .5 is the case for identical input states. This is not quite as good as with single photon states where we could approach $V_{HOM} = 1$, but lasers are readily available and easier to use than single photon sources. If using lasers for communication protocols, their HOM visibility is worth considering.

3.2 Effects of Imperfections on HOM Visibility

The setup for our experiment was similar to the BB84 setup discussed previously. Taken from [89], the setup is given in Figure 3.3. Here, 2 ns pulses were carved out from CW lasers at 1550 nm. Much of the experiments were conducted at 1 MHz, except for an afterpulsing experiment which was conducted at 10 MHz. DC bias was manually controlled using a DC supply. To correct for drift, the bias was optimized prior to each run. Afterwards, polarization was modulated in the same way as the BB84 experiment; we used polarization controllers to set align the polarizations to 45 degrees with respect to the phase modulator's axes then sent them to a Faraday mirror and backwards through the phase modulator again. They exited through a beam circulator. The pulse traveled in another set of polarization controllers before being attenuated to single photon level.

We sent the single photons through short, 2m free space channels before interfering them at a beam splitter. Two InGaAs SPAD detectors were located on either side of the beam splitter. We counted detections and measured coincidences using a time interval analyzer (TIA) with a resolution of 81 ps.

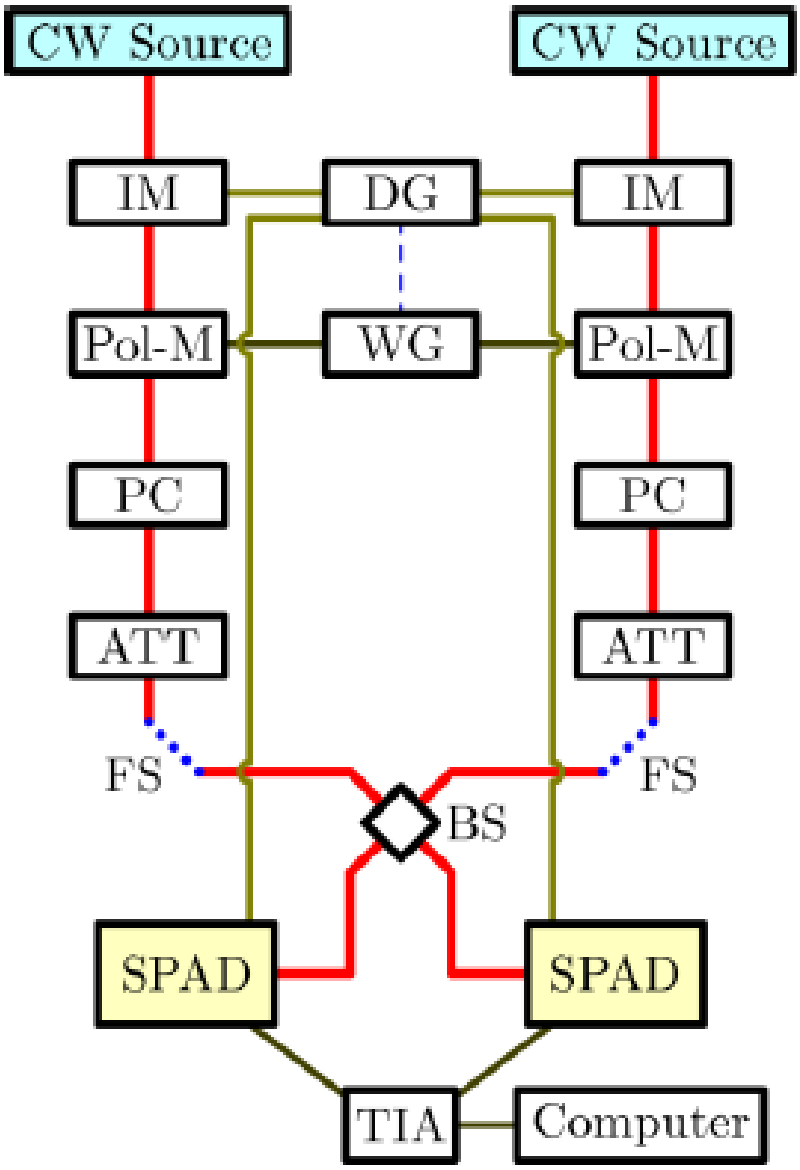


Figure 3.3: Diagram for the HOM with imperfections experiment. Continuous Wave (CW) laser sources produced light in separate arms. The light was separated into pulses by intensity modulators (IM). The polarization was modulated at (Pol-M) using a combination of polarization controllers, a phase modulator and a faraday mirror, just like in 2.5. We attenuated the light using variable optical attenuators (ATT) and sent the photons in short, 2m free space channels before interfering them at a beam splitter (BS). The outputs were monitored at single photon avalanche detectors (SPAD) and the events were time tagged by a time interval analyzer (TIA). Also in [89]

3.2.1 Detector Imperfections' Effects on HOM

When an SPAD detects a photon, it produces an avalanche of current, which in turn triggers a TIA. It takes time for the detector to reset because it cannot accurately count single photons when the current is still high. To allow the current to return to zero, there is a dead time where the detector is electrically disabled. If some of the current remains after the deadtime, it results in a false count called an afterpulse.

There are different functions to model afterpulsing and optimal models may differ even for detectors of the same model and consecutive serial number[90]. Nevertheless, we measured afterpulsing using a model described in [91, 92] for our study.

Humer *et. al.* model afterpulse probability the exponent decaying exponentially. As such, the logarithm of the detection probability is still exponentially decaying. However, poissonian sources of light, such as dark counts will follow a linear decay with respect to the log of the detection probability.

According to the study in [93], the coincident probability can be written as:

$$P_{coin,aft} = P_{coin} + [P_c - P_{coin}]P_d P_{d,totaft} + [P_d - P_{coin}]P_c P_{c,totaft} \tag{3.25}$$

where P_c and P_d are the detection probabilities according to the convention in Figure 3.2. Then, $P_{c,totaft}$ and $P_{d,totaft}$ are their afterpulse contributions. Afterpulse probability is assumed to decay exponentially with time, so $P(t) = P_0 \mathrm{e}^{-t/\tau}$ where P_0 is the initial afterpulse probability and τ is the characteristic decay time.

If we use gated mode where gates have length T_{gate} and deadtime is T_{dt} we have:

$$\begin{aligned} P_{tot,aft} &= P(T_{dT}) + P(T_{dt} + T_{gate}) + ... \\ &= P_0 \frac{\mathrm{e}^{-T_{dt}/\tau}}{1 - \mathrm{e}^{-T_{gate}/\tau}} \end{aligned} \tag{3.26}$$

The detection probabilities are then:

$$P_{c,aft} = P_c[1 + (1 - P_c)P_{c,totaft}] \tag{3.27}$$

$$P_{d,aft} = P_d[1 + (1 - P_d)P_{d,totaft}] \tag{3.28}$$

The plot of detection probablility as a function of time is given in Figure 3.4. We can extract the parameters P_0 and τ by linearly fitting the logarithms of the detection probability with respect to the time between detections. From the plot, we find $P_{0,c} = .018, \tau_c = .85\mu s$ for detector C and detector D is $P_{0,d} = .033, \tau_d = 1.41\mu s$.

Once the afterpulse probability was found, we measured the HOM visibility as a function of dead time. Alice and Bob's pulses were set to about 2ns and the gate width was 7 ns. The measurement results follow the theory well, according to Figure 3.5. We can observe that deadtime must be long enough to minimize afterpulsing in SPAD's if one wants high HOM visibility.

3.2.2 HOM and Source Imperfections

The source imperfections' impact on the HOM visibility is directly visible in Equation 3.24. In particular, polarization mismatch, total intensity, and intensity mismatch were investigated.

We can readily see the impact of polarization mismatch in Equation 3.24. To vary the polarization, we used the apparatus proposed in [82], like in our BB84 experiment discussed previously. We set the input polarization to the setup to 45 degrees with respect to the phase modulators' optical axes. The pulses were then reflected from faraday mirrors and back through the phase modulators to account for drifts in birefringence. We varied the RF voltage applied to the phase modulator to control polarization.

Bob's polarization was fixed, and Alice's was varied by changing the voltage from 0 to V_π. The results are given in Figure 3.6a. This result is useful in determining the

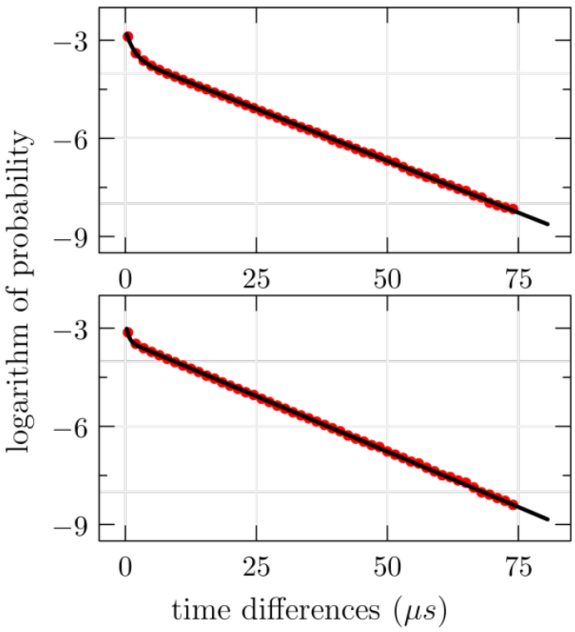


Figure 3.4: Decay of afterpulse probability after a detection. We plot the logarithm of detection probability because we model the afterpulsing as an exponential decay function. The linear fit yields the decay time τ and initial afterpulse probability P_0. Taken from [89]

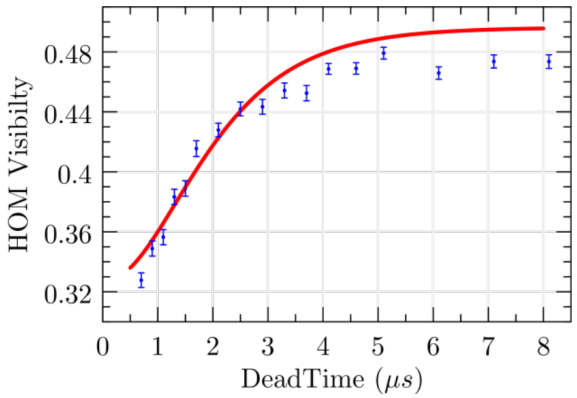
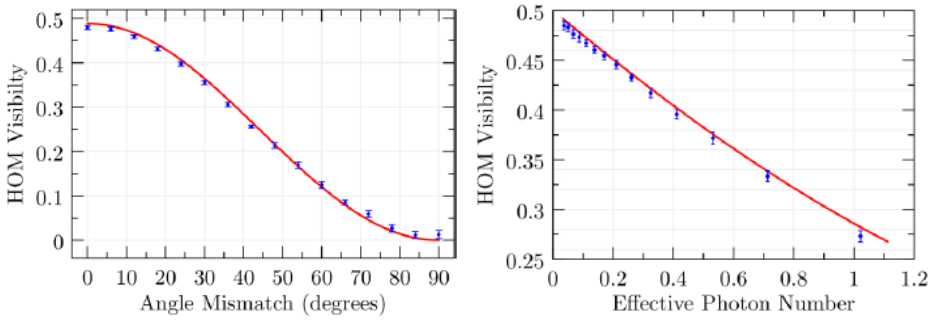


Figure 3.5: HOM visibility as a function of deadtime. Deadtime must be sufficiently long to reduce noise due to afterpulses. Extra noise increases the coincident count, thereby decreasing HOM visibility. Taken from [89]



(a) HOM visibility as a function of polarization misalignment

(b) HOM visibility as a function of average photon number

Figure 3.6: HOM visibility for source imperfections. The left panel shows the relative insensitivity of polarization mismatch when observing the HOM effect. Polarizations must be similar enough for the photons to be identical and trigger the HOM effect. The right panel shows a steep drop off with increasing photon number because any extra photons present at the beam splitter increases the coincidence probability, and thus obscures the HOM effect. Both taken from [89]

impact of misalignment in measurement device independent QKD, where the HOM effect has an important role.

In Figure 3.6b we studied the effect of the total intensity on the HOM visibility. The polarizations and intensities on Alice and Bob were both identical. At this step we should also consider how the average number of photons in a pulse is computed. Since our detectors are threshold detectors(i.e. they cannot discriminate multiphoton pulses from single), the probability of detecting a photon is given by $P = 1 - \mathrm{e}^{-\eta_D \mu}$ where η_D is again the detector efficiency and μ is the average photon number.

We can also make use of the fact that it requires a whole deadtime's worth of blanked gates plus one to get a single detection. So we can set the detection probability equal to the number of gates with photons divided by the number of available gates. We arrive at:

$$\mu_{avg} = \frac{1}{\eta_D} \frac{1 - R_{det}T_{dt} + R_{det}T_{period}}{1 - R_{det}T_{dt}} \tag{3.29}$$

Here, R_{det} is the count rate, T_{dt} is the deadtime and T_{period} is the pulse period. As shown in Figure 3.6b, the HOM effect is obscured by extra photons when the intensity is too high.

It is quite important to Measurement Device Independent (MDI) QKD to determine the proper balance of the intensity in both inputs to the beamsplitter. It can be shown from Equation 3.24 that the HOM visibility is highest when Alice and Bob's average photon numbers are equal. Experimental results are shown in Figure 3.7.

The data was taken by fixing Alice's photon number to .47 photons per pulse, as determined by the count rate in Equation 3.29 and varying Bob's. The HOM visibility drops off considerably when Alice and Bob even have a 3 dB difference. Therefore, MDI QKD will work best whenever Alice and Bob's photon numbers are similar.

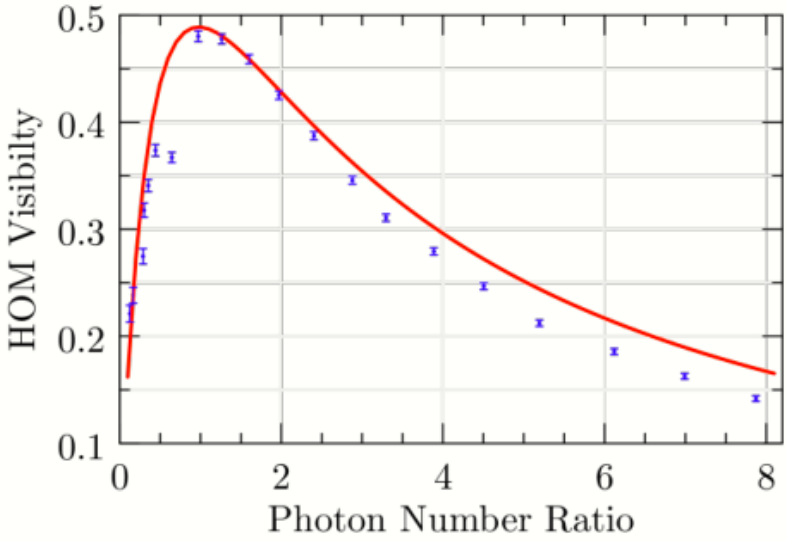


Figure 3.7: The HOM visibility with respect to the intensity mismatch. Alice and Bob's photon numbers must be matched because one side may send more "extra" (i.e. greater than 1) photons than the other, increasing the coincidence rate and decreasing HOM visibility. Taken from [89]

This experiment yielded useful observations when optimizing HOM visibility. In the next chapter, we show how to use them to improve polarization encoding MDI QKD.

Chapter 4

Measurement Device Independent QKD with Dynamic Attenuation

4.1 MDI QKD

BB84 enjoyed much success since it was conceived. The first free space experiment was completed over a distance of 32 cm in 1989[94] and the record is now a remarkable 7600 km between satellites[95]. Nevertheless, BB84 is susceptible to a number of hacking techniques such as including the detector blinding attack[96, 97], backflash attack[98], time shift attack[99], and many others (see Jain *et. al.*[59]).

Often, whenever attacks are discovered, a countermeasure is applied, increasing the complexity of the setup. As hackers continue to find holes in protocols, researchers will continue to patch them and make the real world setup increasingly more complex.

A different approach is Device Independent QKD (DI-QKD), where Alice and Bob share a photon pair from a common entanglement source. In this case, Eve's information is bounded due to the monogamy of entanglement and security can be proven using a Bell's inequality violation. Unfortunately, DI-QKD is very difficult to achieve in part because of the very high efficiency (83%) required to close the Bell State efficiency loophole[100].

Measurement-device-independent (MDI) QKD is a similar variety of countermeasure using time-reversed entanglement that removes all known and future attacks on the detectors, which are often the Achilles heel of QKD [101]. In this protocol, Alice and Bob send BB84 states to a third party, Charlie, who measures Bell States. After the experiment, Charlie publicly announces the results.

MDI QKD can be done with time-bin encoding [102, 103, 104], phase encoding [105], or polarization encoding [106, 107]. The latter is a common choice for free space[10] since the atmosphere is not very birefringent. In any case, MDI QKD involves Alice and Bob both sending pulses to a third party, Charlie, who performs Bell State measurements and announces the results. Charlie's setup in polarization encoding MDI might look like Figure 4.1.

Charlie measures Bell States whenever he counts a coincidence with orthogonal polarizations (V and H, respectively) using a set of four single-photon detectors, $\{D_{1H}, D_{1V}, D_{2H}, D_{2V}\}$, and Alice and Bob use the same encoding basis. Charlie announces the outcome $|\psi^-\rangle$ whenever coincidences occur on $D_{1V}D_{2H}$ or $D_{1H}D_{2V}$, and $|\psi^+\rangle$ if coincidences occur on $D_{1H}D_{1V}$ or $D_{2H}D_{2V}$. Other detection patterns are simply discarded. In the rectilinear basis, errors occur whenever Alice and Bob send the same polarization, and Charlie announces $|\psi^-\rangle$ or $|\psi^+\rangle$. In the diagonal basis, errors occur whenever Alice and Bob send the same polarization and Charlie announces $|\psi^-\rangle$ or Alice and Bob send orthogonal polarization states and Charlie announces $|\psi^+\rangle$.

Using the measurement results from Charlie and basis sifting, Alice and Bob can ascertain the polarization they each sent and perform the necessary bit flips to properly correlate their keys. Error correction and verification follow.

MDI QKD makes the detectors immune to attack, but not the sources. Hence, phase randomized weak coherent pulses must still be protected from photon number splitting using decoy states[52, 53, 109]. The original MDI QKD protocol used 3 different intensities [101, 110]. Zhou, *et al.*, then showed a sizeable improvement with a four-intensity method[111].

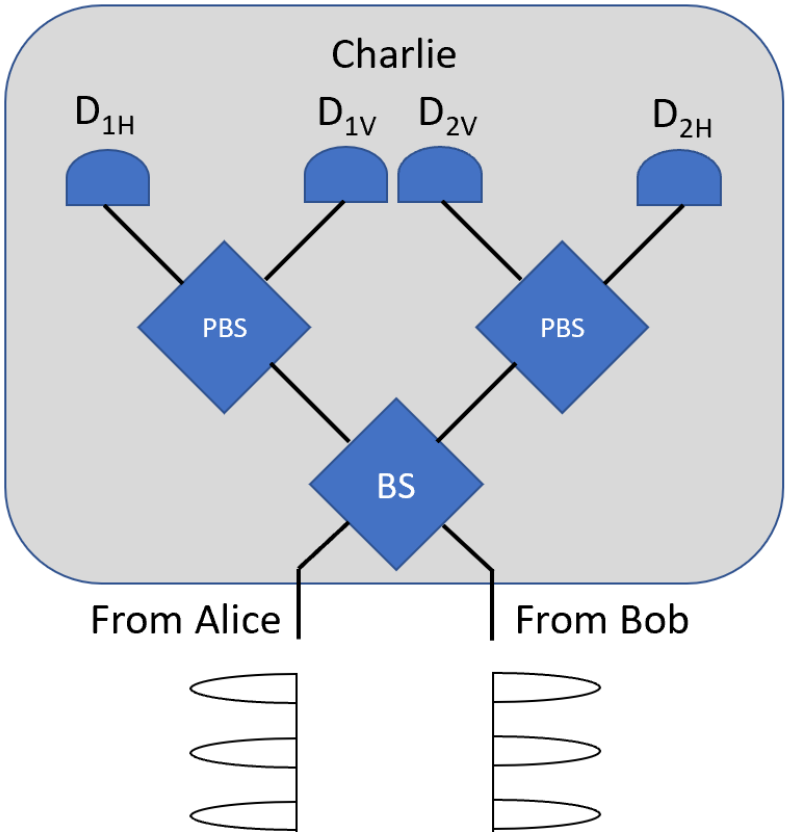


Figure 4.1: A typical measurement setup for polarization encoding MDI QKD. Here, Alice and Bob both send single photon pulses encoded in BB84 states to Charlie's Bell State Analyzer. His setup consists of a beam splitter (BS) and polarizing beam splitters (PBS) after each output. He measures coincidences between his four different detectors ($D_{1H}, D_{1V}, D_{2H}, D_{2V}$). Also in [108]

To build intuitive confidence in the protocol, it is worth considering attacks a malicious Charlie and Eve may perform. Perhaps Charlie tries to figure out who is sending which polarization. He cannot determine this after the photons interfere at the beam splitter. He cannot determine them before the beam splitter either without introducing error, just like in the intercept-resend attack in BB84. Furthermore, he cannot determine the states of Alice and Bob using his coincidence data due in part to the fact that allowed coincidences are time-reversed entangled[112, 113].

Suppose Eve tries to monitor the detectors passively using the backflash attack. In this approach, she would measure the polarizations that propagate backwards from the detectors. This technique will not earn her any information that Charlie does not already have.

Maybe Eve tries to execute the formidable detector blinding attack, where there is no general countermeasure in BB84. In this event, she will try to force Charlie's detectors to operate in "linear" mode rather than geiger mode and hide her presence from the measurement statistics. Regardless of what she does, this would interfere with Charlie's Bell State measurement, so Alice's and Bob's raw keys would contain more errors and thus reveal Eve.

4.2 Effects of Asymmetry on MDI QKD

In order to measure Bell States, MDI employs the HOM effect. Charlie lacks the ability to choose basis; he is always measuring Z. To measure the X basis, he relies on maintaining a high HOM visibility. This causes photons with identical polarizations, whose coincidences would result in errors, to bunch at the BS output and more likely land on the same detector, hence not register coincidences.

Recall from the previous chapter where high HOM visibility requires Alice's and Bob's pulses to have similar average photon numbers at the BS. The channel between Alice and Charlie will almost certainly have a different amount of loss than Bob and Charlie in a future quantum network.

In Figure 4.2, we can observe the effect mismatched channels may have on the error rates in the X and Z bases. These plots were produced using the noise model discussed in Appendix B. The Z basis is fairly robust when the transmittances are mismatched, though a balanced channel is still ideal. On the other hand, the error rate in the X basis is brittle when transmittances are different. This negatively impacts our ability to place a bound on the phase error rate in the Z basis.

When using symmetric QKD, Alice and Bob always send the same average intensities; each sends one signal state and three decoy states including possibly one vacuum. Therefore, asymmetric amounts of channel loss will result in an intensity mismatch at the beam splitter. In order to correct this problem, some groups added fiber[114] to balance the loss and control time delay.

In Wang *et. al.*, they propose using a seven intensity protocol, instead of four, to compensate for imbalances[115](also see [116]). They compare their scheme to the case of adding fiber and show that it is always better to customize intensities rather than add extra loss.

Wang's method was originally suggested for use in fiber, but it has also been successfully used in an imbalanced free space channel[117]. However, recall that free space channels have a fluctuating transmittance. If Alice and Bob customize their intensities for their expected amount of average loss, the fluctuations will ensure that they are never working in the channels used for optimization.

It has been suggested to use postselection[118, 119], like the technique used for BB84. This would operate similarly as well. A multiplexed, high intensity probe beam would be send along the same path as the single photon pulses and its intensity would be measured by a classical detector, or power meter. Time periods where Alice and Bob both have low transmittance and likely high error rates can then be discarded to improve the overall key rate.

In [108] we propose a scheme where instead of discarding time periods, we attempt to "salvage" them. This would mean we do not actively shrink the data size,

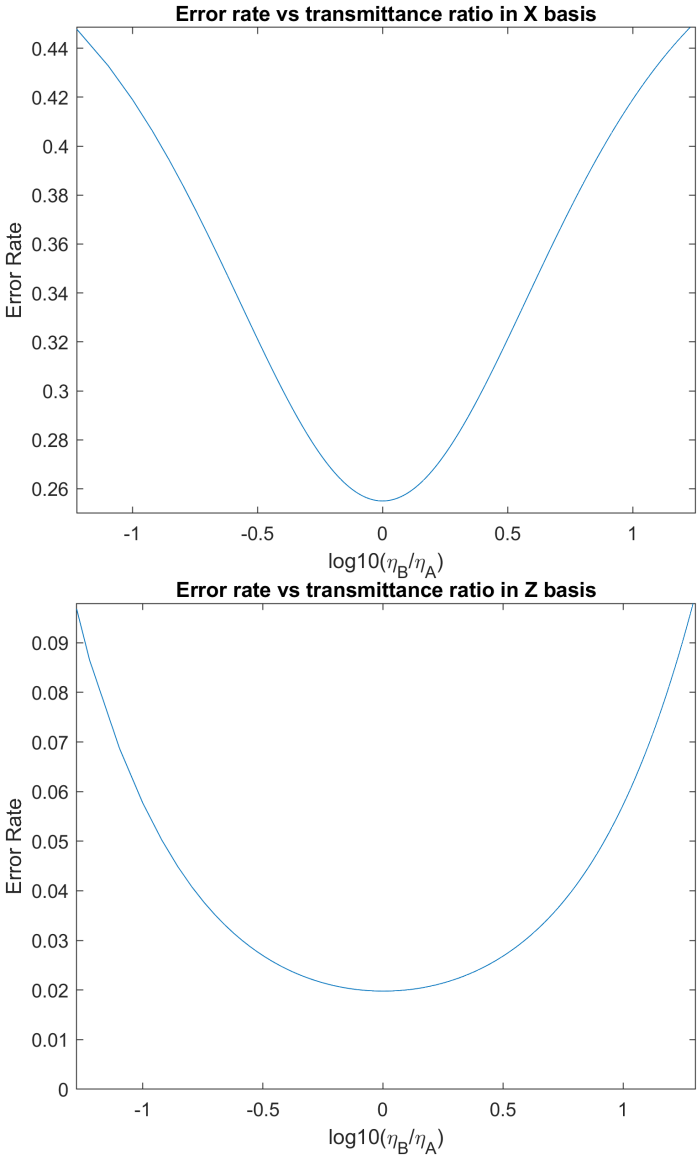


Figure 4.2: Transmittance mismatch's effects on error in each basis. The rectilinear basis is mostly robust in turbulence, but because the diagonal basis relies on the HOM effect, the error rate increases significantly for even slight (even 3 dB) transmittance mismatch.

but we monitor the probes for imbalance and then adaptively apply attenuation to make the higher intensity channel closer to the side with lower transmittance.

4.3 Dynamic Attenuation Background

To implement our Dynamic Attenuation(DA) scheme, we propose to add some sort of variable optical attenuator (VOA) between the dense wavelength division multiplexer (DWDM), which separates the probe from the quantum light, and the beam splitter (BS) where Alice and Bob's pulses interfere. A possible setup is shown in Figure 4.3.

If we assume Alice's and Bob's channels are independent, the joint probability distribution is simply:

$$P(\eta_A, \eta_B) = P(\eta_A)P(\eta_B), \tag{4.1}$$

where $P(\eta)$ is defined in Section 1.3.

Since the secret key rate is a function of transmittance, one can compute the average key rate using the following integral, given an infinite key length:

$$R_{ave} = \int_0^1 \int_0^1 R(\eta_A, \eta_B)P(\eta_A)P(\eta_B)d\eta_A d\eta_B, \tag{4.2}$$

where we can substitute the joint PDTC for $P(\eta_A)P(\eta_B)$. $R(\eta_A, \eta_B)$ is the key rate given by[101]:

$$R \geq P_Z^{1,1}Y_Z^{1,1}[1 - H_2(e_X^{1,1})] - Q_Z f_{EC}(E_Z)H_2(E_Z) \tag{4.3}$$

Here, $P_Z^{1,1}$ is the probability of sending singe-photon pair in the Z basis, $Y_Z^{1,1}$ is the yield of single-photon pair in the Z basis, and Q_Z and E_Z are the gain and error rates, respectively. $e_X^{1,1}$ is the error rate of single-photon in the X basis, $f_E C$ is the error correcting efficiency, and $H_2(x)$ is Shannon binary entropy function.

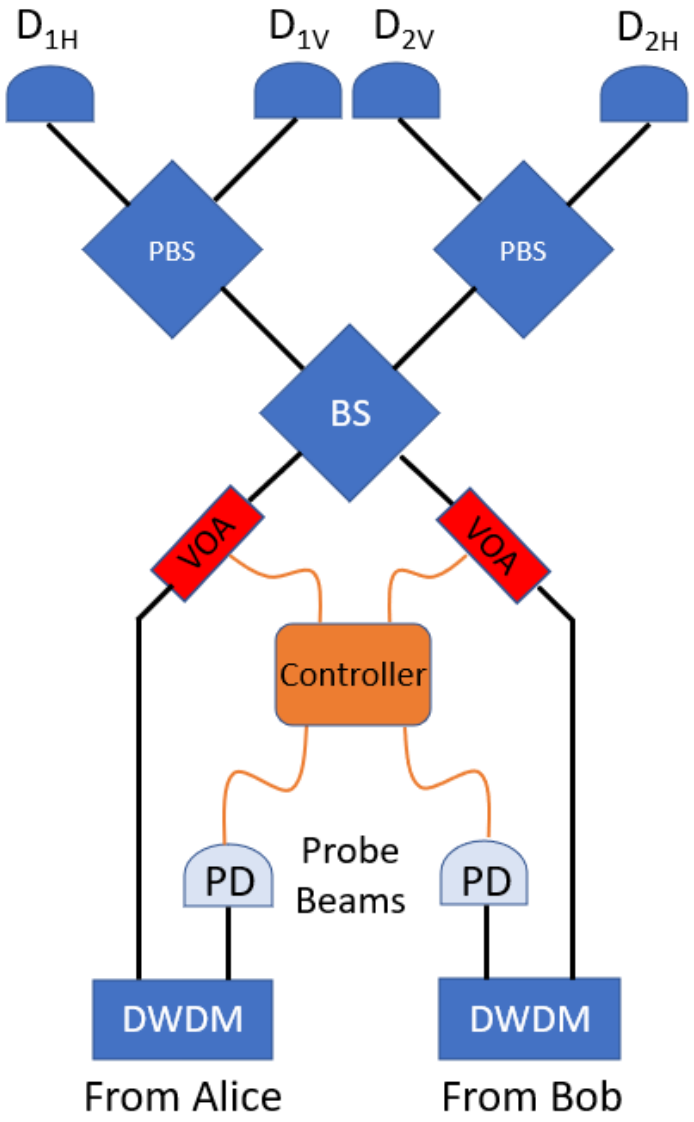


Figure 4.3: Implementing dynamic attenuation in Polarization Encoding MDI QKD. Here, Alice and Bob would each send probe pulses multiplexed in the same spatial channel as their single photon pulses. Charlie would separate the probe pulses using DWDM's and measure their intensities using classical light detectors with a generic controller. Depending on those measurements, he applies an optimal amount of attenuation using VOA's to the stronger channel. Also in [108]

When using dynamic attenuation, the joint PDTC is transformed according to

$$P(\eta_A\prime, \eta_B\prime) = \int\int K(\eta_A\prime, \eta_B\prime, \eta_A, \eta_B) P(\eta_A, \eta_B) d\eta_A d\eta_B, \tag{4.4}$$

where $K(\eta_A\prime, \eta_B\prime, \eta_A, \eta_B)$ represents the kernel relating the new joint PDTC with the original one. Because we cannot achieve infinite resolution, a lookup table is used instead of the kernel.

If we use the lookup table to transform the joint probability distribution, the asymptotic key rate after dynamic attenuation is found from equation 4.2. We have:

$$R'_{ave} = \int_0^1 \int_0^1 R(\eta_A\prime, \eta_B\prime) P(\eta_A\prime, \eta_B\prime) d\eta_A\prime d\eta_B\prime \tag{4.5}$$

Because we only approximated the kernel by using a lookup table, we will have to evaluate the integral numerically.

Furthermore, because we have introduced loss, we have to further modify Equation 4.5 due to the finite key effect. Now, we have to integrate against the noise model and find $\{n_Z, n_X, m_Z, m_X\}$ and then apply the finite version of Equation 4.3 afterward. So we individually find:

$$n^{i,j}_{X,Z} = \int_0^1 \int_0^1 n^{i,j}_{X,Z}(\eta_A, \eta_B) P(\eta_A\prime, \eta_B\prime) d\eta_A\prime d\eta_B\prime \tag{4.6}$$

$$m^{i,j}_{X,Z} = \int_0^1 \int_0^1 m^{i,j}_{X,Z}(\eta_A, \eta_B) P(\eta_A\prime, \eta_B\prime) d\eta_A\prime d\eta_B\prime \tag{4.7}$$

Where $n^{i,j}_{X,Z}$ and $m^{i,j}_{X,Z}$ represent the number of sifted bits and errors, respectively, in the X and Z bases and for i, j states (signal, or one of the decoy states) from Alice and Bob. Once the sifted bits and errors have been found, we compute the full secure key length using our sifted bits/errors and QKD system parameters. A detailed description of the key calculation can be found in Appendix B

4.4 Using Dynamic Attenuation

In the optimization and lookup table generation step, we compute the finite secure key rate using:

$$R = P_s^2(s^2 \mathrm{e}^{-2s} Y_{X,min}^{1,1}[1 - H_2(e_X^{1,1,max})] - Q_Z f_{EC}(E_Z) H_2(E_Z)) \tag{4.8}$$

where P_s is the probability of sending a signal state, s is the average photon number of the signal state, $Y_{X,min}^{1,1}$ is the lower bound of a single-photon pair yield in the X basis, and Q_Z and E_Z are the Z-basis (signal) gain and error rates, respectively. $e_{X,max}^{1,1}$ is the upper bound of single-photon pair error rate in the X basis, f_{EC} is the error correcting efficiency, and $H_2(x)$ is the Shannon binary entropy function. A detailed calculation can be found in Appendix B.2.

Just as when using decoy states in BB84, it is essential to optimize the photon numbers and probability of sending each intensity. In this work, we assume identical statistical distributions so we use symmetric MDI. Consequently we optimize six parameters: $\{s, \mu, \nu, P_s, P_\mu, P_\nu\}$. Due to the difficulty in guessing initial points for optimization, as well as the potential presence of nonsmoothness, I used the MATLAB's genetic algorithm.

Although Nelder-Mead optimization was used in [1], it does not perform well for large numbers of parameters, as might be encountered in asymmetric MDI. Additionally, it requires an initial starting point, which is often difficult to guess when using large numbers of decoy states. On the other hand, the genetic algorithm starts with a population of random points in the parameter space and a "fitness function" defines the ability of points to "reproduce" successfully. After many generations, it heuristically finds a minimum and since it is derivative free, it can be used for nonsmooth functions[120].

Understandably, many groups that may be interested in dynamic attenuation will be using an asymmetric protocol. Our method is also applicable to asymmetric, but the optimization step will include a formidable set of 12 parameters instead of our 6.

In this case, it was suggested in an appendix of [115] to switch to polar coordinates and exploit the theorem:

$$\frac{\mu_A^{opt}}{\mu_B^{opt}} = \frac{\nu_A^{opt}}{\nu_B^{opt}} \tag{4.9}$$

Then the optimization problem is simplified by jointly optimizing $\mu_{A,B}$ and $\nu_{A,B}$ through the transformation:

$$r_\mu = \sqrt{\mu_A^2 + \mu_B^2} \tag{4.10}$$

$$r_\nu = \sqrt{\nu_A^2 + \nu_B^2} \tag{4.11}$$

$$\theta_{\mu\nu} = \arctan(\frac{\mu_A}{\mu_B}) \tag{4.12}$$

Then a user would optimize just five intensities $[s_A, s_B, r_\mu, r_\nu, \theta_{\mu\nu}]$ where the optimization routine is constrained to search along the ridge obeying Equation 4.9. I obtained the best results when assuming probabilities of $\{.3, .3, .3\}$ when optimizing the intensities, then I separately optimized the probabilities afterward. Optimal decoy parameters are given in Table 4.1.

Dynamic Attenuation requires the users to produce a lookup table of optimum attenuations for the stronger channel prior to conducting an experiment. This is produced through the use of nested loops where Alice's and Bob's transmittances are varied in the ranges from $0 < \eta < 1$. For each pair of transmittances, we assume a static channel and compute the secure key rate using Equation 4.8. We attenuate the stronger transmittance in .1 dB increments and use the optimal attenuation for the lookup table.

The lookup table generation is nicely illustrated in Figure 4.4. Here, every point represents a test of the secure key rate and an actual iteration of the loop. The two

Table 4.1: Decoy parameters for dynamic attenuation simulations.

N	dB	s	μ	ν	P_s	P_μ	P_ν
10^{12}	28	0.353	0.229	0.051	0.527	0.055	0.285
10^{13}	34	0.450	0.200	0.037	0.573	0.066	0.219
10^{14}	40	0.499	0.198	0.026	0.466	0.123	0.295

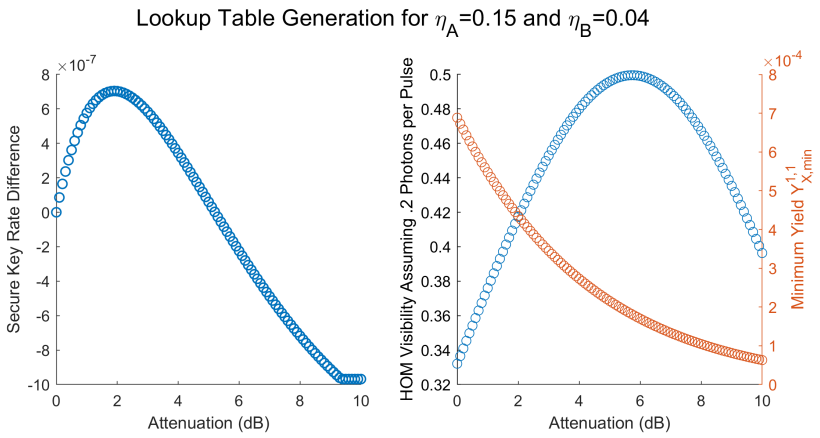


Figure 4.4: Effect of attenuating an overly strong channel. This case represents the procedure needed to produce a single point in the final lookup table. In this example, we select transmittances of $\eta_A = 0.15$ and $\eta_B = .04$ and we apply an incremental attenuation of .1 dB to Alice's side to bring hers closer to Bob's. Each point represents .1 dB of additional attenuation for Alice since her channel has higher transmittance. The left panel shows the improvement in secure key rate as we attenuate Alice's (stronger) side. Notice in the right panel, as we attenuate Alice, we see improved HOM visibility at the expense of single photon yield. We balance these two effects by evaluating Equation 4.8 for each point, where we assume an entire experiment with data size N was conducted with new transmittance, t_A. We observe the maximum improvement to key rate at about 2 dB of attenuation, which we record in the lookup table for these two transmittances. Also in [108]

.

transmittances shown were chosen because they show a decent improvement and when too much attenuation is applied the key rate worsens.

Figure 4.4 also shows the effects of dynamic attenuation inside the key rate calculation. The yield is related to the detection rate and decreases when more loss is applied. On the other hand, the HOM visibility increases, thereby improving our estimate of the phase error rate.

It should be noticed that adding enough attenuation to make the channels identical is often undesirable. In the same figure, even though the HOM visibility is maximized at around 6 dB of attenuation, the extra loss has a deleterious effect on the raw key. For this reason, the optimum is around 2 dB instead.

After iterating over $0 < \eta_A < 1$ and $0 < \eta_B < 1$, we get a lookup table and resulting key rates that resemble Figure 4.5. Here, we observe that the we should optimally apply zero attenuation, except when Alice's and Bob's channels are very imbalanced. However, the channels' fluctuations will be greatest and transmittances most different when the atmospheric turbulence is strong. If we apply the optimal attenuation, the impact on the secret key rate, as shown in the right plot, increases precipitously as the imbalance goes up.

4.5 Results of Applying Dynamic Attenuation to Statistically Identical, Independent Channels

Now that we have a lookup table, we are ready to simulate an experiment. We prepare two different lognormal distributions using the same PDTC from earlier:

$$P(\eta_{A,B}) = \frac{1}{\sqrt{2\pi}\sigma\eta_{A,B}} \mathrm{e}^{\frac{-(\ln(\frac{\eta_{A,B}}{\eta_0})+\frac{\sigma^2}{2})^2}{2\sigma^2}} \tag{4.13}$$

Because we are only approximating the true kernel with a lookup table, we must evaluate the integral in Equation 4.7 numerically. We set up nested loops where

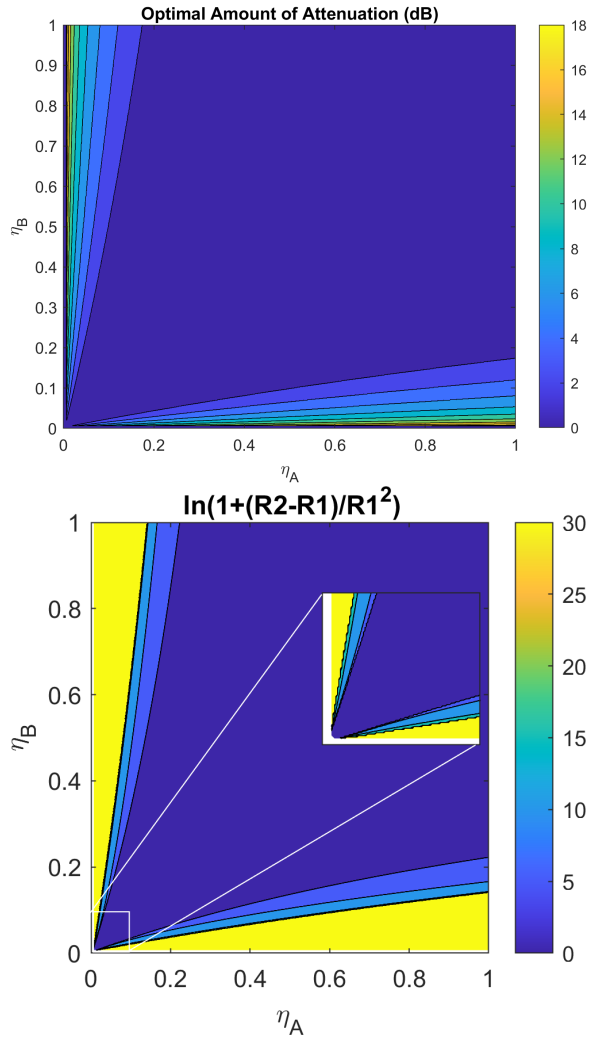


Figure 4.5: Appearance of the lookup table and effects on key rate. The top panel shows the amount the stronger channel should be attenuated to optimize the secure key rate. Assuming this is applied, the improvement is shown in the bottom panel. The function is chosen in order to better show the steep drop in the key rate without dynamic attenuation, R1. R2 is the key rate with dynamic attenuation. Also see [108]

$0 < \eta_A < 1$ and $0 < \eta_B < 1$. For each pair of transmittances, we calculate the number of sifted bits using the noise model. Separately, we also calculate them when applying the optimal amount of attenuation to the stronger channel. Afterward, we compute the secure key rate using Equation 4.8.

We perform this integral for values of σ^2 from .01 for weak turbulence to 1.2 for moderately strong turbulence, after which the lognormal model loses validity. The results are plotted in Figure 4.6. Here, we see an improvement that grows with increasing σ^2 and in many scenarios, we can only achieve a secure key at high turbulence if we use dynamic attenuation.

It should be noted, however, that since much of the lookup table has an optimal attenuation of 0 dB, typical variable optical attenuators with minimum insertion losses of 2-3 dB could harm the secure key rate. We plot this case in Figure 4.7. Here, we see that despite a loss at lower levels of turbulence, we still see an improvement when turbulence is higher.

Given this insight, experimentalists may have to alter their setup depending on the level of turbulence and, if turbulence is high, finish sending data quickly to avoid the deleterious effects of the minimum insertion loss at low turbulence. Given a 1 GHz repetition rate like [121], it only takes 15-20 min to send $N = 1 \times 10^{12}$. Based on diurnal data on C_n^2 in [39, 38, 40], the turbulence should not change significantly in this time frame.

In this work, we proposed a scheme which allows MDI QKD to work in higher turbulence. We show that even when a nonzero minimum loss is added, the key rate can be improved in certain circumstances. Thus, we have shown the seemingly paradoxical conclusion where we can add loss and improve secure key rate.

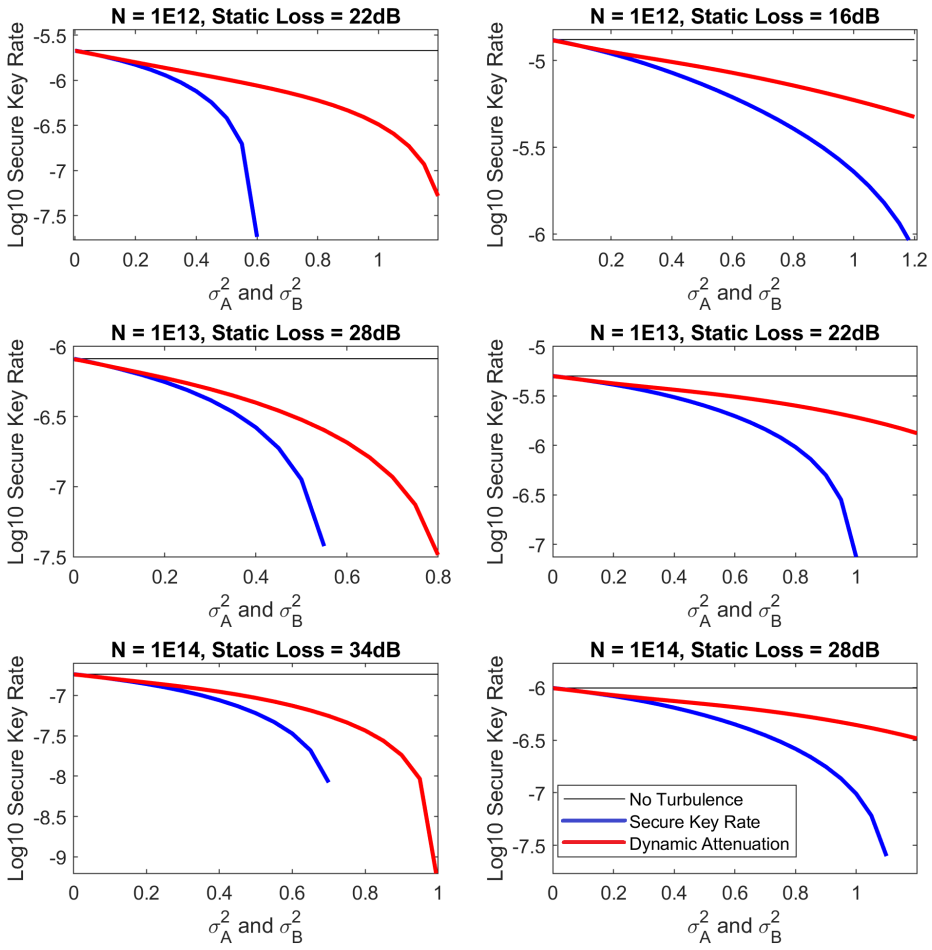


Figure 4.6: Dynamic attenuation applied to independent, statistically symmetric channels. Blue curves correspond to the case of no dynamic attenuation while it is applied for the red curves. We optimize parameters and generate the lookup table once for each data size chosen. We see a significant increase in the robustness in turbulence for each case. Also in [108]

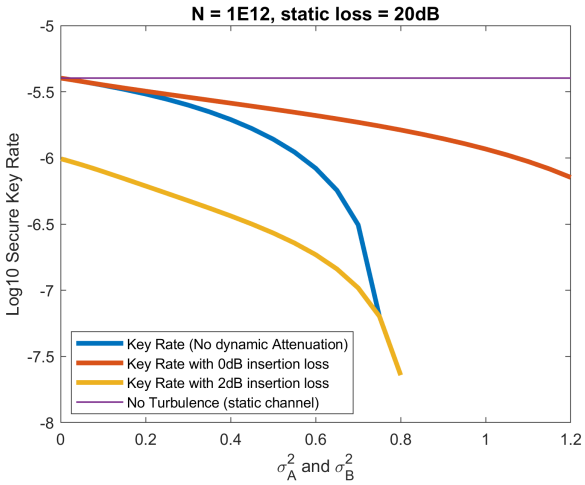


Figure 4.7: Dynamic Attenuation with Nonzero Minimum Loss. We assume N=1E12, the case where dynamic attenuation gave the greatest improvement in Figure 4.6 and generate a new lookup table where the minimum loss is 2 dB instead of 0. We still see an improvement, albeit only at high turbulence. Also in [108]

Chapter 5

Future Work

5.1 Thoughts on Implementing Dynamic Attenuation with Nonzero Insertion Loss

In this dissertation and in [108], we suggest using Lithium Niobate based intensity modulators to attenuate the input pulses at Charlie's side to compensate for transmittance mismatched channels. Of course, a real intensity modulator will introduce loss of at least 2 dB. Another, perhaps more difficult idea would be to use a free space attenuator. This would have have much smaller minimum loss and thus, dynamic attenuation would be beneficial for a wider range of turbulence levels. However, an experimentalist would need to find a way to move a wheel or bar at extremely high speeds to account for the millisecond, or likely smaller, scale at which transmittance changes.

Another idea may insert a mirror which directs the input light to a detector. This mirror could be slightly tilted piezoelectrically to control the input light. Another, more feasible, version of this idea would be to incorporate dynamic attenuation into setups like[117], which use a deformable mirror to correct the turbulence-induced corruption of the wavefront. Perhaps such a setup could be retrofitted to perform dynamic attenuation since they modulate transmittance anyway.

5.2 Combining Postselection with Dynamic Attenuation in MDI QKD

In many earlier schemes of dealing with turbulence, QKD used postselection, which discards detections when the measured intensity of a probe beam is below a threshold. On the other hand, dynamic attenuation salvages time bins where transmittances are mismatched, possibly eliminating the need to delete them. Interesting work may try to compare the performance of the two schemes and attempt to combine them.

Bibliography

[1] Eleftherios Moschandreou, Brian J. Rollick, Bing Qi, and George Siopsis. Experimental decoy-state bennett-brassard 1984 quantum key distribution through a turbulent channel. *Physical Review A*, 103:032614, 2021. ix, 26, 33, 39, 40, 66, 92, 93, 99

[2] G.S. Vernam. Cipher printing telegraph systems. *Journal of the American Institute of Electrical Engineers*, 55:109–115, 1926. 1

[3] Claude E Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949. 1

[4] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999. 2

[5] Daniel J Bernstein, Jean-François Biasse, and Michele Mosca. A low-resource quantum factoring algorithm. In *International Workshop on Post-Quantum Cryptography*, pages 330–346. Springer, 2017. 2

[6] Adrian Cho. Google claims quantum computing milestone, 2019. 2

[7] Leslie Lamport. Constructing digital signatures from a one way function, 1979. 2

[8] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Annual cryptology conference*, pages 361–379. Springer, 2013. 2

[9] Daniel J Bernstein, Nadia Heninger, Paul Lou, and Luke Valenta. Post-quantum rsa. In *International Workshop on Post-Quantum Cryptography*, pages 311–329. Springer, 2017. 2

[10] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002, 2020. 2, 28, 58

[11] Ward Beullens. Breaking rainbow takes a weekend on a laptop. *Cryptology ePrint Archive*, 2022. 3

[12] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983. 3

[13] H Bennett Ch and G Brassard. Quantum cryptography: public key distribution and coin tossing int. In *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, pages 175–9, 1984. 3, 18

[14] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985. 3

[15] Damien Stucki, Sylvain Fasel, Nicolas Gisin, Yann Thoma, and Hugo Zbinden. Coherent one-way quantum key distribution. In *Photon Counting Applications, Quantum Optics, and Quantum Cryptography*, volume 6583, pages 194–197. SPIE, 2007. 3

[16] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018. 3

[17] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982. 3, 18

[18] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145, 2002. 4

[19] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006. 5

[20] Yu-Yang Ding, Hua Chen, Shuang Wang, De-Yong He, Zhen-Qiang Yin, Wei Chen, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. Polarization variations in installed fibers and their influence on quantum key distribution systems. *Optics Express*, 25(22):27923–27936, 2017. 7

[21] Jacek Wojtanowski, Marek Zygmunt, Mirosława Kaszczuk, Z Mierczyk, and Michal Muzal. Comparison of 905 nm and 1550 nm semiconductor laser rangefinders' performance deterioration due to adverse environmental conditions. *Opto-Electronics Review*, 22(3):183–190, 2014. 7

[22] Zabih Ghassemlooy, Wasiu Popoola, and Sujan Rajbhandari. *Optical wireless communications: system and channel modelling with Matlab®*. CRC press, 2012. 7, 9, 10, 11

[23] Scott Bloom, Eric Korevaar, John Schuster, and Heinz Willebrand. Understanding the performance of free-space optics. *Journal of Optical Networking*, 2(6):178–200, 2003. 7

[24] Thomas W Schlatter. Atmospheric composition and vertical structure. *Environmental Impact and Manufacturing*, 6:1–54, 2009. 7, 8

[25] United States Air Force National Oceanic & Atmospheric Administration. *US Standard Atmosphere*. National Oceanic and Atmospheric Administration, 1976. 9

[26] RW Fenn, SA Clough, WO Gallery, RE Good, FX Kneizys, JD Mill, LS Rothman, EP Shettle, and FE Volz. Optical and infrared properties of

the atmosphere. *Handbook of geophysics and the space environment*, 18, 1985. 9, 10

[27] Frederic E Volz. Infrared refractive index of atmospheric aerosol substances. *Applied Optics*, 11(4):755–759, 1972. 9

[28] M. Ijaz, Z. Ghassemlooy, J. Pesek, O. Fiser, H. Le Minh, and E. Bentley. Modeling of fog and smoke attenuation in free space optical communications link under controlled laboratory conditions. *Journal of Lightwave Technology*, 31:1720–1726, 2013. 10, 11

[29] HC van de Hulst. *Light scattering by small particles*. Dover Publications, 1981. 10

[30] Isaac I Kim, Bruce McArthur, and Eric J Korevaar. Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. In *Optical wireless communications III*, volume 4214, pages 26–37. International Society for Optics and Photonics, 2001. 10, 11

[31] Paul W Kruse, Laurence D McGlauchlin, and Richmond B McQuistan. *Elements of infrared technology: Generation, transmission and detection*. Wiley, New York, 1962. 10

[32] Alexander Berk, Lawrence S Bernstein, and David C Robertson. Modtran: A moderate resolution model for lowtran. Technical Report SSI-TR-124, Spectral Sciences Inc., Burlington MA, Burlington, MA, 1987. 12, 35

[33] HJP Smith, DJ Dube, ME Gardner, SA Clough, and FX Kneizys. Fascode-fast atmospheric signature code (spectral transmittance and radiance). Technical report, VISIDYNE INC BURLINGTON MA, 1978. 12, 35

[34] Eugene; A. Zajac Hecht. *Optics*. Addison-Wesley Publishing Co, 1974. 12

[35] SF Clifford. The classical theory of wave propagation in a turbulent medium. In *Laser Beam Propagation in the Atmosphere*, pages 9–43. Springer, 1978. 12

[36] Joseph W Goodman. *Statistical optics*. John Wiley & Sons, 1985. 12, 14, 15, 35

[37] A. Kolmogorov. *Turbulence*. Wiley-Interscience, New York, 1961. 14

[38] Hongxing Wang, Bifeng Li, Xiaojun Wu, Chuanhui Liu, Zhihui Hu, and Pengfei Xu. Prediction model of atmospheric refractive index structure parameter in coastal area. *Optik - International Journal for Light and Electron Optics*, 126:2726–2730, October 2015. 15, 71

[39] D. Sprung, E. Sucher, A. Ramkilowan, and D. J. Griffith. Investigation of optical turbulence in the atmospheric surface layer using scintillometer measurements along a slant path and comparison to ultrasonic anemometer measurements. In Adolfo Comern, Karin Stein, Evgueni I. Kassianov, John D. Gonglewski, and Klaus Schfer, editors, *Remote Sensing of Clouds and the Atmosphere XIX; and Optics in Atmospheric Propagation and Adaptive Systems XVII*, volume 9242 of *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, page 92421I, October 2014. 15, 71

[40] Chun Qing, Xiaoqing Wu, Xuebin Li, Qiguo Tian, Dong Liu, Ruizhong Rao, and Wenyue Zhu. Simulating the refractive index structure constant (C_n^2) in the surface layer at antarctica with a mesoscale model. *The Astronomical Journal*, 155:37, 2018. 15, 71

[41] Larry C Andrews, Ronald L Phillips, and Cynthia Y Hopen. *Laser beam scintillation with applications*, volume 99. SPIE press, 2001. 15

[42] Sherman Karp, Robert M. Gagliardi, Steven E. Moran, and Larry B. Stotts. The turbulence channel. In *Optical Channels*. Springer, January 1988. 16

[43] Valerian Ilich Tatarski. *Wave propagation in a turbulent medium*. Courier Dover Publications, 2016. 16

[44] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman. Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes. *Physical Review A*, 45:8185–8189, 1992. 18

[45] Nuno A Silva and Armando N Pinto. Heralded single-photon source from spontaneous four-wave mixing process in lossy waveguides. In *Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, volume 9648, page 964814. International Society for Optics and Photonics, 2015. 18

[46] Brian P Williams, Ronald J Sadlier, and Travis S Humble. Superdense coding over optical fiber links with complete bell-state measurements. *Physical Review Letters*, 118(5):050501, 2017. 19

[47] Marcos Curty, Xiongfeng Ma, Bing Qi, and Tobias Moroder. Passive decoy-state quantum key distribution with practical light sources. *Physical Review A*, 81(2):022310, 2010. 19

[48] Adam Walton, Anne Ghesquière, George Brumpton, David Jennings, and Ben Varcoe. Thermal state quantum key distribution. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 54(18):185501, 2021. 19

[49] Elizabeth Newton, Anne Ghesquière, Freya L Wilson, Benjamin TH Varcoe, and Martin Moseley. Quantum secrecy in thermal states. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 52(12):125501, 2019. 19

[50] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44–44, jul 2002. 19

[51] Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Physical Review Letters*, 92:057901, 2002. 19

[52] W. Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters 91, 057901*, November 2003. 19, 58

[53] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94:230504, Jun 2005. 19, 24, 25, 58

[54] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72:012326, Jul 2005. 19, 21, 93

[55] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters*, 84(19):3762–3764, 2004. 24, 25

[56] Yi Zhao, Bing Qi, and Hoi-Kwong Lo. Experimental quantum key distribution with active phase randomization. *Applied Physics Letters*, 90(4):044106, 2007. 24

[57] Hoi-Kwong Lo and John Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases. *arXiv preprint quant-ph/0610203*, 2006. 24

[58] Xiao-Ming Chen, Lei Chen, and Ya-Long Yan. The rationality about the assumption that the signal and decoy states are indistinguishable in decoy-state quantum key distribution. *arXiv preprint arXiv:2110.08504*, October 2021. 24

[59] Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt, and Gerd Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, 57(3):366–387, 2016. 24, 57

[60] Siddhartha Das and George Siopsis. Practically secure quantum position verification. *arXiv preprint arXiv:1711.03392v1*, 2017. 27

[61] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau. Practical issues in quantum-key-distribution postprocessing. *Physical Review A*, 81(012318), 2010. 26, 27

[62] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 410–423, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg. 27

[63] Robert G. Gallager. Low-density parity-check codes, 1963. 27

[64] Jung Hyun Bae, Ahmed Abotabl, Hsien-Ping Lin, Kee-Bong Song, and Jungwon Lee. An overview of channel coding for 5g nr cellular communications. *APSIPA Transactions on Signal and Information Processing*, 8, 2019. 27

[65] Hoi-Kwong Lo and H. F. Chau. Security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999. 27

[66] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004. 25, 28, 33

[67] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441, 2000. 28

[68] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Physical Review A*, 89:022307, Feb 2014. 28, 92, 93

[69] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, January 2012. 29

[70] Peter W Milonni, John H Carter, Charles G Peterson, and Richard J Hughes. Effects of propagation through atmospheric turbulence on photon statistics. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(8):S742, 2004. 29

[71] Paul Diament and M. C. Teich. Photodetection of low-level radiation through the turbulent atmosphere∗. *Journal of The Optical Society of America*, 60(11):1489–1494, Nov 1970. 29

[72] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi. Impact of turbulence in long range quantum and classical communications. *Physical Review Letters*, 109(200502), 2012. 29

[73] D. Vasylyev, A. A. Semenov, and W. Vogel. Atmospheric quantum channels with weak and strong turbulence. *Physical Review Letters*, 117:090501, Aug 2016. 29

[74] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and Ch. Marquardt. Free-space quantum links under diverse weather conditions. *Physical Review A*, 96:043856, Oct 2017. 29

[75] A. A. Semenov and W. Vogel. Quantum light in the turbulent atmosphere. *Physical Review A*, 80(2):021802, August 2009. 29

[76] A. A. Semenov and W. Vogel. Entanglement transfer through the turbulent atmosphere. *Phys. Rev. A*, 81(2):023835, February 2010. 29

[77] Gregory R Osche. *Optical detection theory for laser applications*. John Wiley and Sons Inc., 2002. 29

[78] C Erven, B Heim, E Meyer-Scott, J P Bourgoin, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, dec 2012. 29

[79] Giuseppe Vallone, Davide G. Marangon, Matteo Canale, Ilaria Savorgnan, Davide Bacco, Mauro Barbieri, Simon Calimani, Cesare Barbieri, Nicola Laurenti, and Paolo Villoresi. Adaptive real time selection for quantum key

distribution in lossy and turbulent free-space channels. *Physical Review A*, 91:042320, Apr 2015. 29, 31

[80] Wenyuan Wang, Feihu Xu, and Hoi-Kwong Lo. Prefixed-threshold real-time selection method in free-space quantum key distribution. *Physical Review A*, 97:032337, Mar 2018. 30, 34, 41

[81] Zhiyuan Tang, Kejin Wei, Olinka Bedroya, Li Qian, and Hoi-Kwong Lo. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Physical Review A*, 93(4):042308, April 2016. 35

[82] I Lucio-Martinez, P Chan, X Mo, S Hosier, and W Tittel. Proof-of-concept of real-world quantum key distribution with quantum frames. *New Journal of Physics*, 11(9):95001, 2009. 37, 51

[83] Sudhakar Prasad, Marlan O. Scully, and Werner Martienssen. A quantum description of the beam splitter. *Optics Communications*, 62:139–145, 1987. 42

[84] Reinier W. Heeres, Leo P. Kouwenhoven, and Valery Zwiller. Quantum interference in plasmonic circuits. *Nature Nanotechnology*, 8:719–722, 2013. 44

[85] Kenji Toyoda, Ryoto Hiji, Atsushi Noguchi, and Shinji Urabe. Hong–ou–mandel interference of two phonons in trapped ions. *Nature*, 527:74–77, 2015. 44

[86] A. M. Kaufman, B. J. Lester, C. M. Reynolds, M. L. Wall, M. Foss-Feig, K. R. A. Hazzard, A. M. Rey, and C. A. Regal. Two-particle quantum interference in tunnel-coupled optical tweezers. *Science*, 345:306–309, 2014. 44

[87] R. Lopes, A. Imanaliev, A. Aspect, M. Cheneau, D. Boiron, and C. I. Westbrook. Atomic hong–ou–mandel experiment. *Nature*, 520:66–68, 2015. 44

[88] R. C. Liu, B. Odom, Y. Yamamoto, and S. Tarucha. Quantum interference in electron collision. *Nature*, 391:263–265, 1998. 44

[89] E. Moschandreou, J. I. Garcia, B. J. Rollick, B. Qi, R. Pooser, and G. Siopsis. Experimental study of hong–ou–mandel interference using independent phase randomized weak coherent states. *Journal of Lightwave Technology*, 36(17):3752–3759, September 2018. 45, 48, 49, 52, 53, 55, 99

[90] Abdul Waris Ziarkash, Siddarth Koduru Joshi, Mario Stipčević, and Rupert Ursin. Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors. *Sci Rep*, 8:5076, 2018. 50

[91] Gerhard Humer, Momtchil Peev, Christoph Schaeff, Sven Ramelow, Mario Stipcevic, and Rupert Ursin. A simple and robust method for estimating afterpulsing in single photon detectors. *Journal of Lightwave Technology*, 33:3098–3107, 2015. 50

[92] Thiago Ferreira da Silva, Guilherme B. Xavier, and Jean Pierre von der Weid. Real-time characterization of gated-mode single-photon detectors. *Journal of Lightwave Technology*, 47:1251–1256, 2011. 50

[93] C. Wang, F. Wang, H. Chen, S. Wang, W. Chen, Z. Yin, D. He, G. Guo, and Z. Han. Realistic device imperfections affect the performance of hong-ou-mandel interference with weak coherent states. *Journal of Lightwave Technology*, 35(23):4996–5002, December 2017. 50

[94] C. H. Bennett and G. Brassard. Experimental quantum cryptography: The dawn of a new era for quantum cryptography: The experimental prototype is working]. *SIGACT News*, 20(4):78–80, nov 1989. 57

[95] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, Wei Chen, Yun-Hong Gong, Yang Li, Ze-Hong Lin, Ge-Sheng Pan, Jason S. Pelc, M. M. Fejer, Wen-Zhuo Zhang, Wei-Yue Liu, Juan Yin, Ji-Gang Ren, Xiang-Bin Wang, Qiang Zhang, Cheng-Zhi Peng, and Jian-Wei Pan. Long-distance free-space

quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509–513, Aug 2017. 57

[96] V Makarov. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, 11(6):65003, 2009. 57

[97] Lars Lydersen, Mohsen Akhlaghi, A Majedi, Johannes Skaar, and Vadim Makarov. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New Journal of Physics*, 13(11):113042, 2011. 57

[98] Paulo Pinheiro, Poompong Pereira, Shihan Chaiwongkhot, Rolf Sajeed, Jean-Philippe Horn, Thomas Bourgoin, Norbert Jennewein, Vadim Lütkenhaus, and Makarov. Eavesdropping and countermeasures for backflash side channel in quantum cryptography. *Optics express*, 26(16):21020–21032, 2018. 57

[99] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Info. Comput.*, 7(1):73–82, Jan 2007. 57

[100] Anupam Garg and N. D. Mermin. Detector inefficiencies in the einstein-podolsky-rosen experiment. *Physical Review D*, 35:3831–3835, 1987. 57

[101] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13):130503, mar 2012. 58, 63

[102] Xiongfeng Ma, Chi-Hang Fred Fung, and Mohsen Razavi. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Physical Review A*, 86(052305), October 2012. 58

[103] Fumihiro Kaneda, Feihu Xu, Joseph Chapman, and Paul G Kwiat. Quantum-memory-assisted multi-photon generation for efficient quantum information processing. *Optica*, 4(9):1034–1037, 2017. 58

[104] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, et al. Experimental measurement-device-independent quantum key distribution. *Physical Review Letters*, 111(13):130502, 2013. 58

[105] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L Braunstein, Seth Lloyd, Tobias Gehring, Christian S Jacobsen, and Ulrik L Andersen. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 9(6):397–402, 2015. 58

[106] T Ferreira Da Silva, D Vitoreti, GB Xavier, GC Do Amaral, GP Temporão, and JP Von Der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A*, 88(5):052303, 2013. 58

[107] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical Review Letters*, 112:190503, May 2014. 58

[108] Brian J. Rollick, George Siopsis, and Bing Qi. Dynamic attenuation scheme in measurement-device-independent quantum key distribution over turbulent channels, 2022. 59, 61, 64, 68, 70, 72, 73, 74, 99

[109] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94:230503, Jun 2005. 58

[110] Zong-Wen Yu, Yi-Heng Zhou, and Xiang-Bin Wang. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Physical Review A*, 91(3):032318, 2015. 58

[111] Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A*, 93:42324, 2016. 58

[112] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Physical Review A*, 54(4):2651, 1996. 60

[113] Hitoshi Inamori. Security of practical time-reversed epr quantum key distribution. *Algorithmica*, 34(4):340–365, 2002. 60

[114] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Physical Review Letters*, 111:130501, September 2013. 61

[115] Wenyuan Wang, Feihu Xu, and Hoi-Kwong Lo. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks. *Physical Review X*, 9:41012, 2019. 61, 67, 94, 96

[116] Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo. Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics*, 15:113007, 2013. 61

[117] Yuan Cao. Long-distance free-space measurement-device-independent quantum key distribution. *Physical Review Letters*, 125:260503, 2020. 61, 74

[118] Wenyuan Wang, Feihu Xu, and Hoi-Kwong Lo. Prefixed-threshold real-time selection for free-space measurement-device-independent quantum key distribution. *arXiv preprint arXiv:1910.10137*, 2019. 61

[119] Zhuo-Dan Zhu, Dong Chen, Shang-Hong Zhao, Qin-Hui Zhang, and Jun-Hua Xi. Real-time selection for free-space measurement device independent quantum key distribution. *Quantum Information Processing*, 18(1):33, Dec 2018. 61

[120] Lin Li, Alfredo Alan Flores Saldivar, Yun Bai, Yi Chen, Qunfeng Liu, and Yun Li. Benchmarks for evaluating optimization algorithms and benchmarking matlab derivative-free optimizers for practitioners' rapid access. *IEEE Access*, 7:79657–79670, 2019. 66

[121] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics*, 10:312–315, 2016. 71

Appendices

Appendix A

BB84 Key Calculation

We assume that Alice has full knowledge of Bob's detection setup parameters such as efficiency, etc. We will follow the steps from Lim *et al.* [68] and also repeated in [1]. In these conventions, X denotes the rectilinear (computational) basis and Z the diagonal basis. Alice optimizes her parameters : $\{q_X, P_{\mu_1}, P_{\mu_2}, \mu_1, \mu_2\}$ where q_X is the proportion of the bits encoded in the X-basis, P_{μ_1} and P_{μ_2} are the proportions of the signal and weak decoy states, respectively. μ_1 and μ_2 are the average numbers of photons per pulse for the signal and weak decoy states, respectively. For the vacuum decoy state we fixed $\mu_3 = 0.001$ and $P_{\mu_3} = 1 - P_{\mu_1} - P_{\mu_2}$.

Following Lim's paper, we use:

$$\tau_n = \sum_k \frac{\mathrm{e}^{-k} k^n p_k}{n!} \tag{A.1}$$

$$n^{\pm}_{X,k} := \frac{\mathrm{e}^k}{p_{\mu_k}} [n_{X,k} \pm \sqrt{\frac{n_X}{2} \ln \frac{21}{\epsilon_{sec}}}] \tag{A.2}$$

Then n_Z can be calculated similarly. Now, we calculate:

$$s_{X,0} \geq \tau_0 \frac{\mu_2 n^-_{X,\mu_3} - \mu_3 n^+_{X,\mu_2}}{\mu_2 - \mu_3} \tag{A.3}$$

And

$$s_{X,1} \geq \frac{\tau_1 \mu_1 [n^-_{X,\mu_2} - n^+_{X,\mu_3} - \frac{\mu_2^2 - \mu_3^2}{\mu_3^2}(n^+_{X,\mu_1} - \frac{s_{X,0}}{\tau_0})]}{\mu_1(\mu_2 - \mu_3) - \mu_2^2 + \mu_3^2} \tag{A.4}$$

It's also important that we upper bound the phase error rate for each intensity. We have:

$$\phi_X \leq \frac{v_{Z,1}}{s_{Z,1}} + \gamma(\epsilon_{sec}, \frac{v_{Z,1}}{s_{Z,1}}, s_{Z,1}, s_{X,1}) \tag{A.5}$$

and the uncertainty gamma is:

$$\gamma(a,b,c,d) := \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log_2(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}} \tag{A.6}$$

Applying the finite-size key distillation method from [68], we calculate the secure key Rate $R = \frac{\ell}{N}$, where ℓ the number of distilled bits,

$$\ell = \left\lfloor s_{X,0} + s_{X,1}\left(1 - h(\phi_X)\right) - n_X \cdot f_{EC} \cdot h(m_X/n_X) - 6\log_2\frac{21}{\varepsilon_{sec}} - \log_2\frac{2}{\varepsilon_{cor}} \right\rfloor \tag{A.7}$$

where $s_{X,0}$ and $s_{X,1}$ are the contributions to the key rate from vacuum and single photon pulses and ϕ_X the phase error contributed by single photon events. Their expressions stem from the three decoy state method [54] extended to include finite-size effects and are taken directly from [68]. In [1], we assumed Lim's values so the error correction efficiency was set as $f_{EC} = 1.16$, the secrecy $\varepsilon_{sec} = 10^{-10}$ and the correctness $\varepsilon_{cor} = 10^{-15}$.

Appendix B

Noise Model and Finite Key Calculation in MDI QKD

We first describe the model needed to predict the sifted key and error quantities, then proceed to compute finite secure key length using a method described in an appendix of [115]. We shall follow conventions given in the relevant chapter where $[s_{A,B}, \mu_{A,B}, \nu_{A,B}, \omega = 0]$ where $s_{A,B}$ are the signal state intensities, μ and ν are the decoy intensities and ω is the vacuum state assuming perfect intensity modulators. η_D is the detector efficiency for all detectors and $\eta_{A,B}$ are the channel transmittances excluding the detector.

B.1 Noise Model

B.1.1 Z Basis

The probability of coincidence when Alice and Bob send opposite polarizations is:

$$n_{z1} = \frac{1}{2}(1 - 2e_{d,Z})(1 - \mathrm{e}^{-\eta_A \eta_D s_A})(1 - \mathrm{e}^{-\eta_B \eta_D s_B}) \tag{B.1}$$

Where dark counts are neglected as well as cases of Alice and Bob both being misaligned. $P_{s_{A,B}}$ and N are suppressed in this step because they are cancelled in the secure key calculation.

Whenever Alice and Bob send the same polarization the coincident probability is:

$$n_{z2} = \frac{1}{2}(1 - \mathrm{e}^{-(1-e_{d,Z})\eta_A\eta_D s_A}\mathrm{e}^{-(1-e_{d,Z})\eta_B\eta_D s_B})(e_{d,Z}\eta_A\eta_D s_A + e_{d,Z}\eta_B\eta_D s_B + 2Y_0) \tag{B.2}$$

Now, $n_Z = n_{z1} + n_{z2}$ and $m_X = n_{z2}$.

B.1.2 X Basis

We will refer to each intensity as k_i, where 2, 3 are the decoy states, and 4 is the vacuum. The only coincidences that survive sifting will have the same intensity state.

First consider when Alice and Bob send opposite polarizations. Whenever only 1 photon is incident at the beam splitter, the only coincidences that are possible are due to dark counts. We have:

$$P_{coin} = \eta_A\eta_D k_{i,A}\mathrm{e}^{-\eta_A\eta_D k_{i,A}}Y_0 + \eta_B\eta_D k_{j,B}\mathrm{e}^{-\eta_B\eta_D k_{j,B}}Y_0 \tag{B.3}$$

When Alice and Bob each send 1 photon, we have:

$$P_{coin} = \eta_A\eta_B\eta_D^2 k_{i,A}k_{j,B}\mathrm{e}^{-\eta_A\eta_D k_{i,A}-\eta_B\eta_D k_{j,B}} \tag{B.4}$$

Then cases where Alice or Bob sends 2 photons and the other sends none:

$$\eta_A\eta_B\eta_D^2\mathrm{e}^{-\eta_A\eta_D k_{i,A}-\eta_B\eta_D k_{j,B}}\frac{k_{i,A}^2 + k_{j,B}^2}{2} \tag{B.5}$$

3 photon events are not considered so the model loses accuracy at lower losses and high photon numbers.

The number of $|\phi^-\rangle$ events is:

$$\begin{aligned} n_{c1} = \frac{1}{2}((\eta_A\eta_D k_{i,A} \mathrm{e}^{-\eta_A\eta_D k_{i,A}} Y_0 + \eta_B\eta_D k_{j,B} \mathrm{e}^{-\eta_B\eta_D k_{j,B}} Y_0) + .5 \\ * (\eta_A\eta_B\eta_D^2 k_{i,A} k_{j,B} \mathrm{e}^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}})(1 - 2e_{d,X}) + .25 \\ * (\eta_A\eta_B\eta_D^2 \mathrm{e}^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}} \frac{k_{i,A}^2 + k_{j,B}^2}{2})) \end{aligned} \tag{B.6}$$

Then the number of $|\phi^+\rangle$ events is:

$$\begin{aligned} n_{w1} = \frac{1}{2}((\eta_A\eta_D k_{i,A} \mathrm{e}^{-\eta_A\eta_D k_{i,A}} Y_0 + \eta_B\eta_D k_{j,B} \mathrm{e}^{-\eta_B\eta_D k_{j,B}} Y_0) \\ + (\eta_A\eta_B\eta_D^2 k_{i,A} k_{j,B} \mathrm{e}^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}}) e_{d,X} + .25 \\ * (\eta_A\eta_B\eta_D^2 \mathrm{e}^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}} \frac{k_{i,A}^2 + k_{j,B}^2}{2})) \end{aligned} \tag{B.7}$$

When Alice and Bob send the same polarization state, the analysis is similar, except with the roles of $|\phi^+\rangle$ and $|\phi^-\rangle$ exchanged. Therefore, $n_{c2} = n_{c1}$ and $n_{w2} = n_{w1}$. Finally, we have:

$$n_X^{i,j} = 2(n_{c1} + n_{w1}) \tag{B.8}$$

$$m_X^{i,j} = 2n_{w1} \tag{B.9}$$

B.2 Secure Key Calculation

We are ready to take our $[n_Z, n_X, m_Z, m_X]$ from the previous subsection and use them to calculate our secure key rate. We mostly follow steps in the appendix of [115]. Because we suppressed $N, P_{k_{i,j}}$ before, the gains are given by:

$$Q_X^{i,j} = n_X^{i,j} \tag{B.10}$$

$$T_X^{i,j} = m_X^{i,j} \tag{B.11}$$

Where $n_X^{i,j}$ applies to all decoy intensities $i \in [2,3,4]$. Now, we apply bounds according to $\gamma = 5.3$. This value is the number of standard deviations within our confidence interval for a failure probability of 10^{-7}. We have:

$$\overline{Q_X^{i,j}} = Q_X^{i,j} + \gamma\sqrt{\frac{Q_X^{i,j}}{NP_{k_i}P_{k_j}}}$$
$$\underline{Q_X^{i,j}} = Q_X^{i,j} - \gamma\sqrt{\frac{Q_X^{i,j}}{NP_{k_i}P_{k_j}}}$$
$$\overline{T_X^{i,j}} = T_X^{i,j} + \gamma\sqrt{\frac{T_X^{i,j}}{NP_{k_i}P_{k_j}}}$$
$$\underline{T_X^{i,j}} = T_X^{i,j} - \gamma\sqrt{\frac{T_X^{i,j}}{NP_{k_i}P_{k_j}}}$$

Then, we can define:

$$\underline{Q_{M1}^{\nu\nu}} = \mathrm{e}^{\nu_A+\nu_B}\underline{Q_X^{\nu\nu}} - \mathrm{e}^{\nu_A}\overline{Q_X^{\nu\omega}} - \mathrm{e}^{\nu_B}\overline{Q_X^{\omega\nu}} + \underline{Q_X^{\omega\omega}} \tag{B.12}$$
$$\overline{Q_{M2}^{\mu\mu}} = \mathrm{e}^{\mu_A+\mu_B}\overline{Q_X^{\mu\mu}} - \mathrm{e}^{\mu_A}\underline{Q_X^{\mu\omega}} - \mathrm{e}^{\mu_B}\underline{Q_X^{\omega\mu}} + \underline{Q_X^{\omega\omega}} \tag{B.13}$$

Then we can place lower and upper bounds on yield and error, respectively:

$$Y_{X,min}^{1,1} = \frac{1}{\mu_A - \nu_A}\left(\frac{\mu_A}{\nu_A\nu_B}\underline{Q_{M1}^{\nu\nu}} - \frac{\nu_A}{\mu_A\mu_B}\overline{Q_{M2}^{\mu\mu}}\right) \tag{B.14}$$
$$e_{X,max}^{1,1} = \frac{1}{\nu_A\nu_B Y_{X,min}^{1,1}}(\mathrm{e}^{\nu_A+\nu_B}\overline{T_{\nu\nu}} - \mathrm{e}^{\nu_A}\underline{T_{\nu\omega}} - \mathrm{e}^{\nu_B}\underline{T_{\omega\nu}} + \overline{T_{\omega\omega}}) \tag{B.15}$$

Finally, we shall define E_z as the error rate in the Z basis. Now our secure key rate is:

$$R = P_{s_A}P_{s_B}(s_A s_B \mathrm{e}^{-(s_A+s_B)}Y_{X,min}^{1,1}[1 - h_2(e_{X,max}^{1,1})] - f_{EC}Q_Z^{1,1}h_2(E_z)) \tag{B.16}$$

Where f_{EC} is the error correcting efficiency which we set to 1.16 and h_2 is the binary Shannon entropy.

Vita

Brian Rollick got his B.S. in Physics with an Economics minor in 2016 from Allegheny College. There, he briefly studied cold molecular clouds in the interstellar medium under Daniel Willey. After joining the University of Tennessee's Ph.D. program, he switched to quantum information. He mainly studies quantum optics and QKD. The main chapters in this work are based on his papers: [1], [89] and [108], respectively.