Measurement-Device-Independent Quantum Key Distribution

MS Thesis

Submitted in partial fulfillment of the requirements for the award of the degree of

MASTER OF SCIENCE

IN

PHYSICS

Abdul Basit Alam Khan

00000278371

Supervised by

Dr. Aeysha Khalique

Department of Physics, School of Natural Sciences

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

March 2022

FORM TH-4

National University of Sciences & Technology

MS THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: Abdul Basit Alam Khan, Regn No. 00000278371 Titled: Measurement Device Independent Quantum Key Distribution be Accepted in partial fulfillment of the requirements for the award of **MS** degree.

Examination Committee Members

1. Name: DR. M. ALI PARACHA Signature:

2. Name: DR. SAADI ISHAQ Signature:

Supervisor's Name DR. AEYSHA KHALIQUE Signature:

Head of Department

20-07-2022
Date

COUNTERSINGED

Date: 22.07.2022

Dean/Principal

Abstract

Quantum Key Distribution (QKD) has come a long way since the advent of the BB84 protocol and an integral step in this development has been that of Measurement Device Independence (MDI). As such I have attempted to track this development in Discrete Variable-Quantum Key Distribution (DV-QKD) by studying theoretically the important aspects that make up a QKD type setup. I then move on to explain one of the more recently developed protocols in light of the physics involved that transmits and generates the signal state as well as how it is interpreted for it to be considered as one of the Bell States, a necessity for MDI type protocols.

Contents

Chapter 1

Thesis Outline

Chapter 2 In this chapter, I give a brief history and development of cryptography in general. Then moving on to describing the need for the relatively recent, with respect to the history of cryptography, quantum cryptography. Described concepts include Cryptography through history, One-Time Pad, breaking of classical encryption protocols and the development of quantum protocols to maintain secure communication.

Chapter 3 In this chapter I have introduced some of the key concepts that one will come across throughout the literature of quantum key distribution (QKD) protocols. These include but are not limited to, the Shannon Entropy, BB84 protocol and the modification of the BB84 protocol using decoy states. Of course a cyrptographic setup is only as good as the security it provides, security against malicious actors, hence we also introduce some of the most common techniques an eavesdropper might use.

Chapter 4 Finally in the last chapter I have discussed a relatively new approach to the problem of insecure quantum key distribution, which was device independent quantum key distribution. Going on to give the modified measurement device independent (MDI) protocol and finally a very recent variant of an MDI type setup introduced in a 2020 paper. Described in the chapter is the physics behind the protocols and how it ties into the security aspect of a general MDI-QKD protocol.

Chapter 2

Introduction

As the world heads into a new quantum revolution, where we see quantum technologies used especially in telecommunications, the concept of quantum information is one that lies at it's heart. The ability to effectively transfer information from one place to another, it can be reasoned, has been one of the most important aspects of human development. Of course as humanity develops, more efficient ways of communication get developed. The need for newer methods of information transfer can be simplified, somewhat, down to two key reasons, speed and security. Where speed is concerned, we have seen development from the stone ages up until the advent of modern communications using the electromagnetic spectrum. Starting from relaying information on foot by word of mouth in prehistoric times. Then developing to using animals to quicken the pace whether it be riders on horses or various birds trained to relay information. Further development in pace took place only relatively recently in human history with electricity being used through long wires laid down over large distances. While currently we have reached a sort of limit on speed when humans started using the electromagnetic spectrum, from radio waves (FM, AM, etc) to light (in optical fibers), to communicate.

This is so because of the universal speed limit on light or any sort of information moving through space-time.

Now let us take a look at the security aspect of it all. Of course one can understand why secure information transfer is necessary. Conflict is natural, and as such one can always assume malicious third parties looking to use our information for their benefit. Hence it is paramount to have the information safeguarded against any attempts to steal it. To track the development of secure communication we shall look at only some key developments through history that would help us develop the understanding for this thesis. It is necessary to understand a thing or two about encryption. Firstly, what is encryption? It is the coding of information via some kind of scheme or system that should render the information incomprehensible to anyone else. The only way to decode the information is then to use a secret key.

Encryption has been around for a long time, dating back to a few hundred years BC presently known, when the Spartans had used cryptography to relay information between commanders. There had been various encryption methods in those times, these methods relied on both parties having an understanding of the encryption scheme used in order to be able to decode the message, they must possess the same key that was used to encrypt the information. This does of course rely on the fact that the third party either never finds out about the encryption scheme or one of the two parties never leak the scheme. In either case, if the encryption key is known then no message would be secure after that point and they would have to come up with a totally new key. This method of using a common fixed key to be used for encryption is known as the symmetric key.

The other more secure method of encryption is by using the asymmetric key. This concept is relatively modern, first introduced in 1976 by Diffie and Hell-

man [5]. In this method there is a public key that is, as the name suggests, available to the public so that anyone can use it to encrypt their message to send. While the private key that is held by the receiver only is used to decode that message. Whereas if the person with the private key encrypts the message, the public will be able to decrypt that message using the public key. There are more benefits to this procedure than just its security. It provides authentication to the message as well as does not warrant key distribution as the private key is always with the receiver while the public key is always available. Such a process is however slow and if a third party has access to the private key then the whole process is rendered useless.
After having briefly discussed symmetric and asymmetric keys, we look towards a method that we follow to develop the keys discussed in this thesis. The One-Time Pad(OTP); the One-Time Pad is an encryption scheme that makes use of the symmetric key. It is claimed to be unbreakable, if certain conditions are fulfilled. The conditions for the success of the One-Time Pad are:

- Key should be completely random

- Key should be as long as the message

- As per the name, one key for one message only, never to be reused in any shape or form

- The key should be kept secret by both the parties

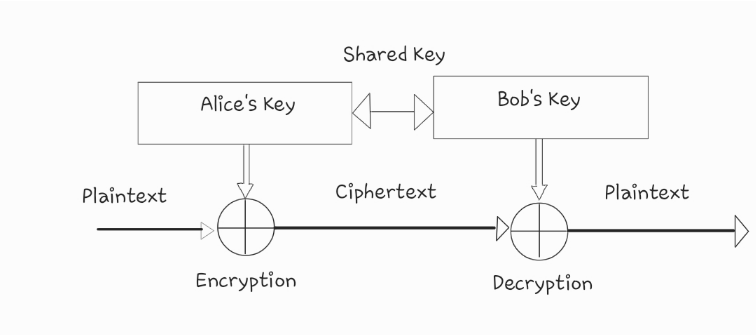

Figure 2.1: One-Time Pad

The way this works can be illustrated in 2.1. It shows how Alice and Bob can exchange messages, labeled as *Plaintext* by firstly having a shared key. Then the sender, Alice in this case, encrypts her message using the shared secret key. That message is then transmitted via a public channel where it is able to be targeted by malicious actors like Eve. However, due to the key being secret Eve cannot decrypt the message. When fulfilling these requirements, OTP has a quality known as *perfect secrecy* [19] which can be seen since firstly the key is random and hence completely secure, only the two communicating parties know of it, and never use the same key again. So the encoded message, known as the ciphertext, reveals nothing about the real message, the plaintext. From this point on the task is to find suitable ways to fulfill these requirements.

OTP was classically, not using quantum methods, used during the World War era where communications had to mostly be sent to the front-lines or to headquarters. Information that was one way and hence could utilize one key for one message, which would then obviously be discarded, could be sent through the OTP method while also being very secure. So long as both parties maintain a certain amount of keys to encode their messages, information transfer is possible, while if they run out of keys the problem that arises is how to transmit more keys securely and without enemy interference. Clearly we have a problem now when we enter the modern age of information, where both speed and secrecy are of great value, the OTP method of encryption runs into problems. What do the users do once they run out of their random keys? Communication is secure so long as they have random keys left to encode their messages, but once out, do they wait for new keys and hence compromise on the speed or do they reuse some of their previous keys. No choice is without consequence. Clearly the choice to reuse keys violates one of the key requirements of the OTP, that of using the key once. While waiting for a new set of keys requires the parties to somehow exchange keys securely, which would in itself require some other method of transmitting keys that will not be as secure as the OTP, hence vulnerable to attack, hence compromising the security of the OTP itself. It is because of these kinds of problems with the OTP that we do not see it being used in classical information transfer anymore.

Since there are more effective classical encryption protocols than the OTP, it begs the question as to why there is a need for any sort of quantum protocol in the first place. In short, classical encryption schemes were proven to be weak against hacking by a quantum computer [15]. Which then necessitates some other way to securely communicate and exchange information, lest we wish to forfeit information security to quantum computers. Hence, with the advent of Quantum Information, there came protocols for transmitting information that were secure against attacks by third parties due to the laws of physics themselves rather than elaborate encryption schemes. Enter, Quantum Key Distribution (QKD), as the name suggests, it is a method through which we can transmit keys using quantum mechanics rather than classical information transfer protocols. To have a secret key is the foundation of the

OTP, and having protocols that are guaranteed security from physical laws gives a secure method to transmit those keys amongst users. Owing to this fact, the OTP has seen a resurgence in recent times. Now it is important to always remember that these quantum protocols will be used to only transmit the keys and not the messages themselves. The messages can be sent much more easily, at present, through classical channels using the OTP with the keys that were transferred by quantum means. Using quantum channels, we make use of not the classical bits which were the on and off states of a transistor. But rather a quantum bit (qubit) state, which in addition to being in the state $|0\rangle$ and $|1\rangle$ can also be in a linear superposition of the two states, represented by the following:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\Phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.1}$$

In the quantum description, we have to also look at how we are going to measure our qubits as measurement plays an important role. Since the act of the measurement destroys the state, we have to be careful where in the protocol the measurement device is placed, they are usually placed at the end of the signal where we want to record the information contained within the signal. The devices used are detectors, and specific arrangements of detectors and other devices allow us to measure different kinds properties of the signals, depending on how they were encoded.

We now establish the need to better develop quantum protocols. It just so happens that mostly all of the QKD protocol implementations encounter device imperfections and other short comings existing in the physical realm. These imperfections introduce errors in the protocol and compromise the security of our key [17]. These points of information leakage are known as *side-channels* which can be exploited by malicious third parties, also known as the eavesdropper (Eve). Hence new protocols are required to overcome Eve's ability to siphon off information from our system, this counts as a major driving factor in the development of more secure QKD protocols.

Now the first viable QKD protocol dates back to 1984, known as BB84 [3]. BB84 does itself run into some practical problems when it comes to implementation as well as risks data leak via different kinds of attacks that Eve can execute on the protocol. The decoy state protocol was introduced to deal with some of Eve's attacks, to give a better key generation rate. This decoy state protocol can alert the users, commonly called Alice and Bob, to Eve's presence as well as help them estimate the error she introduces. There have been various offshoots of the BB84 protocol such as the E91 [6], Six State Protocol [4] and more. Each protocol wants to maximize security and fend off Eve's attacks, which for the most part goes hand in hand. Quickly however, all these QKD protocols ran into problems occurring due to the devices. Hence Device Independent (DI) QKD was introduced to minimize the side-channels occuring due to the devices, be they at Alice or Bob's end. Further development led to Measurement Device Independent (MDI) QKD which claims to be rid of all side-channels related to the measurement device by virtue of the setup itself. This type of QKD protocol introduces a third party that does the measurement for us and announces their result. The setup allows for security despite the measurement result being public.

The field of QKD is still rapidly developing to safeguard against all kinds of attacks that Eve can come up with. Of course Eve's attacks themselves are also of special interest so as to understand the weaknesses of protocols and not be caught off guard by an actual malicious eavesdropper. In the thesis below, we link the development and understanding of a few key concepts with a recent paper on MDI-QKD. The thesis organized by firstly taking a look at some important mathematical concepts required to understand the protocols. Leading on to the BB84 protocol, which is the basis of the following chapter on MDI-QKD. Lastly, we link up to one of the more recently developed MDI-QKD protocol.

Chapter 3

Basic Quantum Key Distribution Protocols

Here I start off by reviewing the most basic of QKD protocols and then move on to discussing a vital modification to improve security. This is needed to understand how certain modifications are helpful in dealing with attacks made by the eavesdropper. However, first we must discuss how we quantify information by making use of Shanon Entropy.

3.1 Shannon Entropy

A concept which is very fundamental to QKD and indeed any field within Quantum Information, is the way in which we understand information. The task, of course, is not easy to have a set definition of information that can then be used to evaluate how much of it is contained within messages or codes. However, we start by giving a verbal explanation of information. In any scenario we say that the information contained within (about) a particular object (variable) is only as much as what we do not already know about it, also called the apriori information. Of course if everything is known about, say, the variable X, then no one stands to gain any new 'information' about X. It is hence that we modify our discussion slightly to discuss not the information contained but our ignorance about the object. So say we knew X to be the result of the throw of a fair 6 sided die. From this we could say that the probability of any number X would be $\frac{1}{6}$. The information that we gain by learning the value of X is what we need to define. The information contained in a variable is defined as

$$S(p(x)) \;=\; -\sum_x \, p(x)\; \log_2 p(x) \tag{3.1}$$

Since S is a log function of probability we see that due to the negative sign it will always remain positive since probabilities are always less than 1. For much the same reason, the function S is known as an entropy. Of course, if for a variable X we have its value known, say $X = 7$, then $p(7) = 1$ and we see that $S = 0$. Now as for the case of the fair die, we have that $p(x) = \frac{1}{6}$ for all X and so $S = -(\log_2 \frac{1}{6})$ $S \approx 2.58$ which we know to be the maximum value of S for this case. It is seen that for N values of X, the value of S is maximized when the probabilities of X are uniformly distributed. Which is to say that in such a scenario we will gain maximum information if the probabilities are all uniform for all values of X. This Entropy function is known as the Shannon Entropy. For the case when X can take only two values $X \in \{a, b\}$, we have a binary entropy function where if $p(a) = p$ then $p(b) = 1 - p$ and the function becomes

$$H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p) \tag{3.2}$$

The Shannon Entropy is written with the symbol H rather than S, which will be seen throughout this document. As for the binary entropy function, we have that $0 \leq H(p) \leq 1$

3.2 The BB84 Protocol

The BB84 protocol [3], named after its two developers Charles Bennett and Gilles Brassard who released the paper in 1984, is perhaps the most famous and among the first proposed protocols for quantum key distribution (QKD).This experiment is based around an ideal scenario where there will be no physical imperfections in their devices or channels, and hence, no errors induced in the quantum states that they send (this assumption will hold throughout this section). To realize the protocol the two users, Alice (A) and Bob (B) have available to them the following 4 states, or qubits, in their respective basis. In the **Z** basis we have $\{|0\rangle, |1\rangle\}$ and in the **X** basis they have $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The states $(|0\rangle, |+\rangle)$ both correspond to a binary bit value of 0 while the other two states $(|1\rangle, |-\rangle)$ represent the binary bit value 1. They proceed by having either Alice being the sender and Bob the receiver or vice versa, both situations are equivalent. Alice sends her bits to Bob over the quantum channel. The probability of selecting between the **X** and **Z** basis is $\frac{1}{2}$ while the choice of state to send in each basis is also $\frac{1}{2}$. Theoretically, if Bob were to measure the bits that Alice sent in the same basis that Alice prepared them in, then their bit values should be the same. On the other hand however, if Bob uses a different basis for measurement than Alice, his results will differ. Table 1 will outline their outcomes for this scenario.

Knowing now all possible measurement outcomes, we can continue to setup

Table 3.1: Alice and Bob's state results

Basis (A)	State (A)	Basis (B)	Output (B)	Binary States
Z	$\|0\rangle$	Z	$\|0\rangle$	0
		X	$\|+\rangle$	0
			$\|-\rangle$	1
	$\|1\rangle$	Z	$\|1\rangle$	1
		X	$\|+\rangle$	0
			$\|-\rangle$	1
X	$\|+\rangle$	X	$\|+\rangle$	0
		Z	$\|0\rangle$	0
			$\|1\rangle$	1
	$\|-\rangle$	X	$\|-\rangle$	1
		Z	$\|0\rangle$	0
			$\|1\rangle$	1

the protocol for information transfer. Alice sends her bits by randomly selecting either the **X** or **Z** basis and then randomly selecting among the states. Bob then measures the received bit by randomly selecting a measurement basis. Alice and Bob's results will be correlated when both use the same basis for preparation and measurement. To check for these correlated outputs, Alice announces her choice of basis for each state sent, not the particular choice of state, over an insecure classical channel. For example, if Alice made the following choices for the first ten qubits Basis: **X Z Z X X X Z X Z Z** and the States: $|0_x\rangle$ $|0\rangle$ $|1\rangle$ $|1_x\rangle$ $|0_x\rangle$ $|0_x\rangle$ $|1\rangle$ $|0_x\rangle$ $|1\rangle$ $|1\rangle$, then she will announce only the string of Basis. Bob checks his results, by choosing the states where they both used the same basis, against the announcement made by Alice and obtains a correlation between their bits. (We shall see later how the presence of an eavesdropper, Eve, introduces errors in the correlated bits.) These correlated bits are known as the sifted key, which can then be used to establish secure communication.

In a slightly more realistic scenario, we have to consider the possibility of there being an eavesdropper in our quantum communication. The benefit of QKD however comes through with the ability to detect Eve due to the errors that she will inevitably induce when she disturbs Alice and Bob's quantum states. A straightforward attack that Eve can carry out is known as the *intercept and resend* attack. Eve will simply measure the output states of Alice by randomly selecting one of the two measurement basis. If she selects the same basis as Alice, she gets the state that Alice had intended to send and then prepares the qubit in the same state to send on to Bob. On the other hand, if she measures the qubit in the wrong basis, there is a 50% that she does not get the state Alice intended to send, as can be seen from the table. 3.1 In order to avoid being detected, Eve does have to send on the state she measured, from Alice, to Bob. Herein lies the error that she can introduce in the setup. When Eve disturbs the measurement and sends on the qubit she measured, there is a 50% chance she used the same basis as Alice. Whereas if she prepared the qubit in the wrong basis, there is a 50% chance that Bob will measure it in the same basis as both Alice and Eve. Since Alice and Bob will both discard the bits that do not correlate in the sifting process, i.e. the bits sent for which their basis choice do not match, the discarded bits do not benefit Eve since they do not make up part of the final key. While during the instances when A & B agree for their basis choice, their bit values may differ due to the presence of Eve, which necessitates that they further discard some bits in order to ensure that Eve gets minimum information. In order to hide her presence better, Eve can then be tempted to try some more sophisticated attacks on A & B's quantum communication. Such attacks are discussed in section 3.4

In 3.2 we have the full extent of the BB84 protocol in outlined in a very basic scenario with 10 bits.

Table 3.2: BB84 With Eve

Alice's State	0	1	0	0	1	1	1	0	0	1
Alice's Basis	Z	Z	Z	X	X	Z	Z	Z	X	Z
Polarization State Sent	0	1	0	+	-	1	1	0	+	1
Eve's Random Basis	X	X	Z	X	Z	Z	Z	X	Z	X
Eve's State (measured and sent)	-	-	0	+	0	1	1	+	1	-
Bob's Basis	Z	X	Z	X	X	Z	Z	Z	Z	X
Bob's State	0	-	0	+	-	1	1	0	1	-
Public Channel discussion										
Shared Secret Key	0		0	0	1	1	1	0		
Errors Introduced	No		No	No	No	No	No	No		

In this whole process, the quantum channel is used only for the communication of qubits. All other types of information exchanges take place through classical insecure channels, where the assumption is that Eve is always listening. After having done the initial communication about their basis choice, the post processing is also done over this insecure channel. Post processing events include error correction and privacy amplification.

3.3 Decoy State Protocol

The decoy state method was proposed in 2003 by W.-Y. Hwang [11] as a means to counter Eve's attempt at eavesdropping. There are of course more than one types of attacks at Eve's disposal, the benefit of Decoy States is that it helps us identify Eve's presence. Since technology has not caught up with theory, it is not possible to generate perfect single photon signals. Which is why we send our signals as weak coherent pulses (WCP). Eve can carry out a photon number splitting attack (PNS) or the intercept and resend attack on our signals and gain information that we want to transmit securely. We will take a look at the decoy state method as applied to the BB84 setup [14].

The BB84 setup has the following key generation rate expression:

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\} \tag{3.3}$$

q in this case is a factor of implementation and if we use an efficient variant of the BB84 protocol, we have $q \approx 1$. The factors that have subscript 1, all tell us about the single photon case, while μ and ν and so on, represent the intensities for the WCP's. Q is known as the gain, E is the overall Quantum Bit Error Rate (QBER), e_1 is the error rate for the single photon only. f is the function of the error correction protocol, and depends on the particular protocol used, its value is always $f(x) \geq 1$. $H(x)$ is the Shannon Entropy. The factors Q_μ and E_μ can be measured experimentally from the results of the protocol, while we need to find out Q_1 and e_1 ourselves using the mathematical expressions we will soon generate. But before we move on to the expressions that help us obtain bounds on the error and gain, we begin by defining certain parameters to be used in the expressions.

3.3.1 Modeling

We need to understand on what parameters the protocol is built upon in order to better understand how the gain and error are effected.

Source

When using the weak coherent pulses, the signals states that we generate have the following density matrix:

$$\rho_A = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} \left|i\right\rangle \left\langle i\right| \tag{3.4}$$

Where the state with $i = 0$, $|0\rangle\langle 0|$, is our vacuum state and with $i \geq 1$ we are given the matrix which has its entries as the probabilities for that state to occur. The photon probabilities are poisonian for the WCP's, as can be seen from the expression.

Channel

To model the channel, we need to account for the kind of quantum channel that is in use, as such, the channel assumed is the optical fiber. The expression that gives us the transmittance of the channel for communication between A and B.

$$t_{AB} = 10^{-\frac{\alpha l}{10}} \tag{3.5}$$

Here, α[db/Km] is the loss coefficient and l[Km] is the length of the optic fiber

Detector

The detectors at Bob's end have an efficiency of η_D. While the total efficiency at Bob's end means that the signal was transmitted to Bob through the channel successfully first, hence it is given by the expression: $\eta_{\text{Bob}} = t_{\text{Bob}}\eta_{\text{D}}$. Using this we can define the overall efficiency to be

$$\eta = t_{\text{AB}}\eta_{\text{Bob}} \tag{3.6}$$

We have to note that this case is describing a scenario where Alice is the sender and Bob is the receiver, only on quantum channel is in use between the two parties. Furthermore, we assume the use of threshold detectors for the protocol, which are commonly used in QKD protocols. These detectors can only distinguish between a zero (vacuum) and a non-zero photon ($|i\rangle\langle i|$)

state. Assuming that the photons in the i photon state are independent, the transmittance can be written as

$$\eta_i = 1 - (1 - \eta)^i \tag{3.7}$$

Which gives us the probability of the i^{th} photon being detected.

Yield & Gain

We have the yield which is defined as the probability of a photon being detected. We note here that the detection event is not only restricted to the case where Alice (or Bob) send a photon (true signal) but also when there is a dark count, i.e. a photon from the background detected. As such, the expression for the yield is as follows.

$$Y_i = Y_0 + \eta_i(1 - Y_0) \tag{3.8}$$

The first term Y_0 is the probability of a dark count, which is around $Y_0 = 10^{-5}$ while the second term is that a photon is transmitted and there is no dark count, for which we say that $1 - Y_0 \approx 1$. Hence we can now write the yield as

$$Y_i = Y_0 + \eta_i \tag{3.9}$$

The gain is the product of a detection event at the receiver and the probability that the source sends out a photon in the i^{th} state, hence the gain of the i^{th} state is given by.

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{3.10}$$

While for the overall gain we have simply

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{3.11}$$

Which then simplifies to the expression below after putting the form of Y_i

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{3.12}$$

Error & QBER

To find the Quantum Bit Error Rate (QBER) we must have the error rate, this is given by

$$e_i = \frac{e_0 Y_0 + e_{\mathrm{det}} \eta_i}{Y_i} \tag{3.13}$$

Where we define e_{det} as the probability that the photon hits a part of the detector leading to an error, such as a misaligned face. While e_0 is the error due to the random background, which is given the value of $e_0 = \frac{1}{2}$ Now in order to define the QBER we have the expression

$$\mathrm{QBER} = E_\mu Q_\mu \tag{3.14}$$

Substituting in for the overall gain, we can get the expression

$$QBER = e_0 Y_0 + e_{\mathrm{det}}(1 - e^{-\eta\mu}) \tag{3.15}$$

3.3.2 Decoy State Methods

Given above are all the elements that factor in to finding our secret key rate, R. Our goal, as always in a QKD protocol, will be to maximize R and hence we must make a selection of μ that does so. Noting first that $R \propto Q_1$ we need to have a maximal value for Q_1. Q_μ on the other hand needs to be low in order to ensure security. Hence we have that $\frac{Q_1}{Q_\mu}$ should be a large value for which it is straightforward to see that $Q_\mu \in (0,1]$. Now in order to determine the values for Y_1 and e_1 we will look at a few cases of the decoy state method.

3.3.2.1 General Decoy State method

With the general method we assume there to be m decoy states. So the expected photon numbers for these states are represented as $\mu, \nu_1, \nu_2, ..., \nu_m$. Now Alice and Bob will have the following equations for their gain and QBER. First noting that we can rewrite the expression for gain as

$$Q_\mu e^\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} \tag{3.16}$$

and the QBER expression as

$$E_\mu Q_\mu e^\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} \tag{3.17}$$

We can similarly write out all the decoy states in such a manner upto the general decoy state with ν_m as

$$Q_{\nu_m} e^{\nu_m} = \sum_{i=0}^{\infty} Y_i \frac{\nu_m^i}{i!} \tag{3.18}$$

$$E_{\nu_m} Q_{\nu_m} e^{\nu_m} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_m^i}{i!} \tag{3.19}$$

The main task at hand is to obtain a tight lower bound on the value of R. For this the values of e_1 and Y_1 are necessary as discussed earlier. In order to bound R we need to be able to find a lower bound on Y_1 and an upper bound on e_1, that will be enough to analyze the protocol to compare its values with other implementations. With the general method in the asymptotic case, where $m \longrightarrow \infty$, the results were assessed in an earlier body of work by the authors. This is of course a theoretical implementation of the procedure and is impractical. For real world application we will now explore only the following two cases where we will have:

a . 2 Weak Decoy States

b . 1 Vacuum and 1 Weak Decoy State

3.3.2.2 Two Weak Decoy States

The key to using the decoy states is that the decoy signals should be weaker than the signal state μ [11]. As such the decoy states that the protocol uses have the following restrictions:

$$0 \leq \nu_2 \leq \nu_1$$

$$\nu_1 + \nu_2 < \mu \tag{3.20}$$

Using the equations for gains of the decoy states in 3.18 We generate an expression to begin finding a lower bound on the background yield Y_0

$$\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu 1} e^{\nu 1} \tag{3.21}$$

$$\nu_1 \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!} e^{-\nu_2} e^{\nu_2} \;\; - \;\; \nu_2 \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!} e^{-\nu_1} e^{\nu_1} \tag{3.22}$$

The Y_1 contributions are seen to cancel out while the rest of the expression can be written as follows.

$$Y_0(\nu_1 - \nu_2) \ - \ \nu_1\nu_2(Y_2\frac{\nu_1 - \nu_2}{2!} + Y_3\frac{\nu_1^2 - \nu_2^2}{3!} + ...) \tag{3.23}$$

So now we have that

$$Y_0(\nu_1 - \nu_2) \ - \ \nu_1\nu_2(Y_2\frac{\nu_1 - \nu_2}{2!} + Y_3\frac{\nu_1^2 - \nu_2^2}{3!} + ...) \ \leq \ Y_0(\nu_1 - \nu_2) \tag{3.24}$$

Hence

$$\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu 1} e^{\nu 1} \ \leq \ Y_0(\nu_1 - \nu_2) \tag{3.25}$$

$$Y_0 \ \geq \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu 1} e^{\nu 1}}{\nu_1 - \nu_2} \tag{3.26}$$

Obtaining the lower bound on Y_0 to be

$$Y_0 \ \geq \ Y_0^L = max[\ \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu 1} e^{\nu 1}}{\nu_1 - \nu_2}\ , \ 0\ ] \tag{3.27}$$

Which is that the greater of the two values is then the lower bound. Also, we have that for $\nu_2 = 0$ (the vacuum state), $Y_0 \ = \ Y_0^L$ while otherwise $Y_0 \ > \ Y_0^L$

Now we can move on to find the lower bound on Y_1

We first note that we can rewrite the equation for the overall gain as:

$$Q_\mu e^\mu - Y_0 - Y_1\mu \ = \ \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} \tag{3.28}$$

As well as noting the following conditions on ν_1, ν_2 and μ

$$\begin{aligned} \nu_1 + \nu_2 < \mu \ &\longrightarrow \ \frac{\nu_1 + \nu_2}{\mu} < 1 \\ 0 \leq \nu_1 \leq \nu_2 \ &\longrightarrow \ 0 \leq \nu_1 - \nu_2 \end{aligned} \tag{3.29}$$

We write out an expression to help us get the lower bound on Y_1

$$Q_{\nu_1}e^{\nu_1} \ - \ Q_{\nu_2}e^{\nu_2} = \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!} e^{-\nu_1} e^{\nu_1} \ - \ \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!} e^{-\nu_2} e^{\nu_2} \tag{3.30}$$

Which helps us get the following form

$$Y_1(\nu_1 - \nu_2) \ + \ \sum_{i=2}^{\infty} Y_i \frac{\nu_1^i - \nu_2^i}{i!} \tag{3.31}$$

The following mathematical condition holds: $a^i - b^i \ \leq \ a^2 - b^2$ if $0 < a + b < 1$ and that $i \geq 2$. Hence $\nu_1^i - \nu_2^i \ \leq \ \nu_1^2 - \nu_2^2$

Now we see that if we multiply $\frac{\nu_1^2 - \nu_2^2}{\mu^2}$ with $\sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!}$ we can go on to build the following inequality:

$$Y_1(\nu_1 - \nu_2) \ + \ \sum_{i=2}^{\infty} Y_i \frac{\nu_1^i - \nu_2^i}{i!} \ \leq \ Y_1(\nu_1 - \nu_2) \ + \ (\frac{\nu_1^2 - \nu_2^2}{\mu^2}) \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!} \tag{3.32}$$

Using the right hand side of the above inequality along with the expression in (3.28) and $Y_0 \geq Y_0^L$. A second inequality is generated:

$$Y_1(\nu_1 - \nu_2) + (\frac{\nu_1^2 - \nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0 - Y_1\mu) \ \leq \ Y_1(\nu_1 - \nu_2) + (\frac{\nu_1^2 - \nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0^L - Y_1\mu) \tag{3.33}$$

Solving now the right hand side of the second inequality to obtain Y_1^L we now get:

$$\begin{aligned} &Y_1(\nu_1 - \nu_2) \ + \ (\frac{\nu_1^2 - \nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0 - Y_1\mu) \\ &\qquad \leq \ Y_1(\frac{\mu(\nu_1 - \nu_2) + \nu_1^2 - \nu_2^2}{\mu}) \ + \ (\frac{\nu_1^2 - \nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0^L) \end{aligned} \tag{3.34}$$

While also noting that the left hand side was obtained from the expression $Q_{\nu_1}e^{\nu_1} \ - \ Q_{\nu_2}e^{\nu_2}$ so we rewrite the inequality:

$$Q_{\nu_1}e^{\nu_1} \;-\; Q_{\nu_2}e^{\nu_2} \leq \; Y_1(\frac{\mu(\nu_1-\nu_2)+\nu_1^2-\nu_2^2}{\mu}) \;+\; (\frac{\nu_1^2-\nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0^L) \tag{3.35}$$

$$[Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - (\frac{\nu_1^2-\nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0^L)]\frac{\mu}{\mu(\nu_1-\nu_2)+\nu_1^2-\nu_2^2} \leq Y_1 \tag{3.36}$$

Finally we have the lower bound on Y_1 being:

$$Y_1 \geq Y_1^{L,\nu_1,\nu_2} = [Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - (\frac{\nu_1^2-\nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0^L)]\frac{\mu}{\mu(\nu_1-\nu_2)+\nu_1^2-\nu_2^2} \tag{3.37}$$

It is then straightforward to see the lower bound on the gain for the single photon signal, Q_1

$$Q_1 \geq Q_1^{L,\nu_1,\nu_2} = [Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - (\frac{\nu_1^2-\nu_2^2}{\mu^2})(Q_\mu e^\mu - Y_0^L)]\frac{\mu^2 e^{-\mu}}{\mu(\nu_1-\nu_2)+\nu_1^2-\nu_2^2} \tag{3.38}$$

Now that we have obtained the lower bounds on the yield, and hence, gain, the error needs to be upper bounded for the single photon case. We start the process by using the following two equations.

$$E_{\nu_1}Q_{\nu_1}e^{\nu_1} = e_0 Y_0 + e_1\nu_1 Y_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_1^i}{i!} \tag{3.39}$$

$$E_{\nu_2}Q_{\nu_2}e^{\nu_2} = e_0 Y_0 + e_1\nu_2 Y_1 + \sum_{i=2}^{\infty} e_i Y_i \frac{\nu_2^i}{i!} \tag{3.40}$$

Then in similar fashion to how we obtained the equations for our lower bound, subtracting the above two expressions from one another, (3.39) - (3.40), we shall obtain the upper bound on the error. The expression is as follows:

$$e_1 \leq e_1^{U,\nu_1,\nu_2} = \frac{E_{\nu_1}Q_{\nu_1}e^{\nu_1} - E_{\nu_2}Q_{\nu_2}e^{\nu_2}}{(\nu_1-\nu_2)Y_1^{L,\nu_1,\nu_2}} \tag{3.41}$$

Having obtained all the necessary bounds on the single photon signal state, we can now use these in the key generation rate formula to obtain the lower bound on it. The lower bounded key generation rate is then obtained and the protocol can now be completely defined.

$$R \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1^{L,\nu_1,\nu_2}[1 - H_2(e_1^{U,\nu_1,\nu_2})]\} \tag{3.42}$$

This concludes the section on the two weak decoy state protocol. Next we will examine the Weak + Vacuum state protocol as an optimized decoy state protocol.

3.3.2.3 One Vacuum and One Weak Decoy State

To 'send' what is a vacuum state, Alice will simply turn off her source, and all the times that she has done this are then of course recorded. Hence, this method can be used to get the background rate estimate. We have the following forms for the gain and error of the vacuum state:

$$Q_{\text{vacuum}} = Y_0 \tag{3.43}$$

$$E_{\text{vacuum}} = e_0 = \frac{1}{2} \tag{3.44}$$

As discussed previously, that the error rate for the background is random and set at a half, also known as the dark count.

Now for the weak decoy state the expressions obtained earlier for the 2 decoy state protocol will be used where we say that one of the decoy state's (ν_2) tends to zero. Since Y_0 can be accurately obtained from the vacuum state signals it will basically serve as the value for Y_0^L. As for the lower bound on the yield of the single photon state, we have that

$$Y_1 \geq Y_1^{L,\nu,0} = Y_1^{L,\nu_1,\nu_2}|_{\nu_2\to 0}$$

$$Y_1^{L,\nu_1,\nu_2}|_{\nu_2\to 0} = \frac{\mu}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \tag{3.45}$$

In the same manner as before we then have the lower bound on the gain:

$$Q_1 \geq Q_1^{L,\nu,0} = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0) \tag{3.46}$$

The next step is to find the upper bound on the single photon error rate.

$$e_1 \leq e_1^{U,\nu,0} = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^{L,\nu,0} \nu} \tag{3.47}$$

This concludes the section on the decoy state protocol in which we have explored only two kinds of decoy states. However, for most protocols implementing the decoy state, the methods discussed above shall be enough to understand them. Next we shall look at the nature of a few attacks on our QKD protocols.

3.4 Eve's Attacks

In any QKD protocol we must always factor in the effects of an eavesdropper, named Eve for short, in order to better develop the security measures used to deal with their interference. Interference of this sort is generally also referred to as hacking or quantum hacking. Due to the ever present gap between theory and implementation including the assumptions made in security proofs, Eve will always find imperfections to exploit and gain information, these are knows as side-channels. It is important to note that each QKD protocol has associated security proofs that rely on certain assumptions to guarantee security. In the event that one or more of these assumptions cannot be upheld, Eve finds herself some useful side-channels to exploit.Protocols like BB84 and B92 [2] make the assumptions of using signle-photon sources and since this technology does not allow this, Eve can make use of the imperfections introduced. [8]

3.4.1 Photon-Number Splitting Attack

One of the most basic yet potent of Eves' hacks is the photon-number splitting (PNS) attack. As the name suggests, in this hack Eve makes use of the fact that while most elementary protocols such as BB84 and B92 make use of a single-photon source, practically we use of strongly attenuated laser pulses. These laser pulses have a probability with which single photons are sent while also containing some multiple photon signals. Eve makes use of this imperfection by beam splitting the multiple photon signal sending a single photon back in the quantum channel while saving the other signal in her quantum memory. Point to be noted here is that even though the implementation of quantum memories is still imperfect, we must always assume that Eve is only restricted by the laws of physics but not technology. With the signal states stored she waits for the classical communication phase where the preparation states are declared by Alice. Using this knowledge Eve shall perform the required measurements on her stored signals and gain perfect information about all those signals that were sent via multiple photons. Now there is a counter-measure to the PNS attack described above, which is the incorporation of the Decoy States in order to understand the action of the channel, in so doing we should be able to detect a PNS attack. This is possible because Eve would not know, prior to Alice's declaration through the classical channel, which of the signal states was a decoy, hence Eve would attack indiscriminately upon all multiple photon signals. However, a further problem arises when it was found [10] that different intensity settings cause varying but distinguishable time delays in the signals. This would mean that Eve could exploit this fact and attack only the pulses she understands to be the true signals and not the decoys. Remaining undetected even through the application of the decoy state protocol. However, it was also found that if the intensity was to be modulated after generation of the signals, there no longer existed a correlation between intensities and time-delays of the signals, providing a countermeasure to Eve's counter to the decoy states.

3.4.2 Trojan Horse attack

In essence, a Trojan Horse Attack (THA) [9] is a multi-pronged mechanism through which Eve can obtain information about the system in use by Alice and Bob. This information can be about various settings, from their basis choice to the decoy state settings. This all depends on the reflected signals that Eve receives, by a process known as reflectometry. The different kinds of information that she can receive will all compromise the security of the protocol, some to greater degree than others. To start off, Eve can, in some DV protocols like SARG04 and B92, get information from Bob's device instead [20]. If she obtains information about the measurement basis she will be able to perform an intercept and resend attack which would be undetectable since she would have perfect knowledge of the measurement Bob was supposed to make. Since most protocols that use BB84 implementation always use decoy states for increased security, Eve, using THAs can obtain information on the states that are decoy and the signal states. Knowing which states are which, she will target only the signal states using PNS attacks and get information undetected. Eve does this by targeting the intensity modulator that generates the decoy states to gain information on its settings. Ultimately, a THA is Eve's attempt to send signals to Alice and Bob's setup so that she can obtain any kind of information that may compromise the protocol information transfer. However, in order to actually get said information, she does ultimately have to pair a THA with a PNS or an intercept-resend attack.

3.4.3 Backflash Attacks

Whereas in THAs Eve relied on the reflected signals that she sent, the backflash is actually an unintended side-channel due to the types of detectors that Bob uses in the BB84 scenarios. The avalanche photodiodes (APDs) when detecting a pulse [12], signal state or otherwise, probabalistically emit light which is called backflash light. With the probability of occurrence being significant, and the fact that this light can carry with it polarization information from the devices it passes through, Eve has a significant side channel to exploit.

In order to overcome some, if not all, side channels that Eve introduces there have been many developed QKD protocols with increased security. How they work and what are some of the assumptions involved will be discussed in the upcoming chapters.

Chapter 4

Device Independence

In this chapter we will seek to understand Device Independent Quantum Key Distribution and how the flaws in the prior QKD protocols lead to it. Also take a look at the application of the beam splitters as they apply in most DIQKD protocols.

The initial protocols for QKD: E91, BB84, B92 and others, assumed the use of equipment that the eavesdropper Eve could not tamper with. There was also the assumption that the devices that were in use would not be flawed. Given that these assumptions hold, the amount of information that Eve could obtain was restricted by physical principles and each protocol had a security proof based on these principles. But indeed theoretical and practical applications have many differences, and as with any practical application of physics, devices are never perfect, a fact which Eve can use to her advantage by using the flaws in our devices to gain more information than the amount given by the security proof. Eve has at her disposal a number of sophisticated attack strategies to exploit the imperfections of the devices and we shall discuss them in the following sections.

4.1 DI QKD

In order to overcome some of the side channels, ones that arise due to Eve's exploiting flaws in the devices, the Device Independent approach was put forth. We will briefly go through this approach to build towards the Measurement Device Independent(MDI) approach.

The crux of Device Independence is that the devices may as well be of Eve's making, however, as long as we can establish a correlation, that violates a Bell inequality, between the signal states of Alice and Bob, we should be able to generate our secret key. This concept is what helps in building protocols that do not rely on the security of the measurement devices and hence denying Eve at least those side channels that were introduced by the devices. Eve still has other attacks that she can execute to obtain information about the secret key. The violation of the Bell Inequality ensures that our outputs are random and hence cannot be predetermined by Eve. In order to elaborate, we can make use of a DI protocol, but first we must outline the assumptions that we still need to make to carry out DI QKD.

1. Within their own laboratories, Alice and Bob control all incoming and outgoing channels. Meaning Eve cannot get to the devices within the labs.

2. Alice and Bob can carry out their post processing (Privacy Amplification and Error Correction) reliably.

3. They are able to generate perfectly random, as well as secure (given by 1), bits.

4. They have an insecure classical channel which is still authenticated.

The eavesdropper can intercept all data on the classical channel without detection.

5. Their quantum channel is also insecure and Eve can use any quantum mechanical device to interact with our signals.

Device independent protocols, such as the CHSH spot checking protocol have been tested. However, a problem quickly arises from these protocols, that of obtaining suitable key generation rates. DI protocols do indeed make QKD very secure since we rely on the violation of Bell inequalities which can only be done by a quantum system, but, practical implementation yields low key rates and hence we have to further develop our approach. Additionally, DI protocols make use of single photon sources, which are not readily available.

4.2 The Beam Splitter

Important to the discussion of DI protocols, will be the understanding of what happens to light when it passes a beam splitter. In what follows, we shall take a look at the action of a Beam Splitter (BS) on light, and more specifically, how a 50-50 BS acts on light. [1]

We start our discussion by mentioning first that light, made up of the electric and magnetic fields, is going to be represented by field operators or the ladder operators from the harmonic oscillator description. The operators we shall be working with, are of course the creation and annihilation operators (a , $a^\dagger$) and it will be sufficient to see how they change after the 50-50 BS action.

The way the beam splitter works is by allowing some of the light to pass on through (transmittance) while reflecting the rest of the incident light. It has two inputs and two outputs. Since our discussion takes place in the realm

of Quantum Mechanics, we make note of the fact that when we send light through only one of the inputs, at the other input we must account for the vacuum state $|0\rangle$.
The beam splitter action on the input modes is defined by the following unitary operator.

$$U(\theta) = e^{\theta(a^\dagger b - b^\dagger a)} \tag{4.1}$$

$U(\theta)$ is indeed unitary. Since we can clearly see that

$$U^\dagger(\theta) = e^{\theta(ab^\dagger - ba^\dagger)} \;=\; e^{-\theta(a^\dagger b - b^\dagger a)}$$

Hence

$$U(\theta)U^\dagger(\theta) = \mathbb{1} \tag{4.2}$$

Now that we have our operator, we define its action on the inputs a and b.

$$U(\theta)\; a\; U^\dagger(\theta) \;=\; a(\theta) \tag{4.3}$$

The following commutators are of importance throughout this discussion. $[a, a^\dagger] \;=\; [b, b^\dagger] \;=\; 1$ While all other commutators are 0. Using the BCH identity on the above expression, we obtain the forms for $a(\theta)$ and similarly for $b(\theta)$ as well as those for $a^\dagger(\theta), b^\dagger(\theta)$. So for all the input modes we have the following transformation by the beam splitter:

$$a(\theta) = a\cos(\theta) - b\sin(\theta) \tag{4.4}$$

$$b(\theta) = b\cos(\theta) + a\sin(\theta) \tag{4.5}$$

$$a^\dagger(\theta) = a^\dagger \cos(\theta) - b^\dagger \sin(\theta) \tag{4.6}$$

$$b^\dagger(\theta) = b^\dagger \cos(\theta) + a^\dagger \sin(\theta) \tag{4.7}$$

Now we make the following simplification, relating the changed input modes to the output modes $a(\theta) = c$, $b(\theta) = d$, $a^\dagger(\theta) = c^\dagger$, $b^\dagger(\theta) = d^\dagger$ Furthermore, for a 50-50 BS, the value of $\theta = \frac{\pi}{4}$. Where the value of θ relates to the reflectivity and transmitivity of the BS. Now finally before applying the 50-50 BS on an input state, we express the output modes in terms of the input modes to help us in the process of transforming our states.

$$c = \frac{a-b}{\sqrt{2}} \tag{4.8}$$

$$c^\dagger = \frac{a^\dagger - b^\dagger}{\sqrt{2}} \tag{4.9}$$

$$d = \frac{a+b}{\sqrt{2}} \tag{4.10}$$

$$d^\dagger = \frac{a^\dagger + b^\dagger}{\sqrt{2}} \tag{4.11}$$

For the output modes we have the following important commutators, $[c, c^\dagger] = [d, d^\dagger] = 1$, while all others are 0

4.2.1 Input State: $|0\rangle_A |1\rangle_B$

$$|0\rangle_A |1\rangle_B \longrightarrow b^\dagger |0\rangle_A |0\rangle_B \overset{BS}{\longrightarrow} \frac{d^\dagger - c^\dagger}{\sqrt{2}} |0\rangle_C |0\rangle_D$$

So we have that the input state go to the following output state:

$$|0\rangle_A |1\rangle_B \overset{BS}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle_C |1\rangle_D - |1\rangle_C |0\rangle_D) \tag{4.12}$$

4.2.2 Input State: $|1\rangle_A |1\rangle_B$

$$|1\rangle_A |1\rangle_B \longrightarrow a^\dagger b^\dagger |0\rangle_A |0\rangle_B \overset{BS}{\longrightarrow} (\frac{d^\dagger + c^\dagger}{\sqrt{2}})(\frac{d^\dagger - c^\dagger}{\sqrt{2}}) |0\rangle_C |0\rangle_D$$

Which leads to the following expression:

$$(\frac{d^\dagger + c^\dagger}{2})(|0\rangle_C |1\rangle_D - |1\rangle_C |0\rangle_D) \longrightarrow \frac{1}{2}(\sqrt{2}\,|0\rangle_C |2\rangle_D - |1\rangle_C |1\rangle_D + |1\rangle_C |1\rangle_D - \sqrt{2}\,|2\rangle_C |0\rangle_D)$$

After canceling the like terms, the final expression becomes:

$$|1\rangle_A |1\rangle_B \xrightarrow{BS} \frac{1}{\sqrt{2}}(|0\rangle_C |2\rangle_D - |2\rangle_C |0\rangle_D) \tag{4.13}$$

Which is an interesting outcome. Here we find that if one were to send two photons, number states or Fock states, 1 in each input, the photons bunch together on either of the output ports but do not come out 1 on each port. This effect was discovered by Hong-Ou-Mandel and was hence given that name.

This concludes the chapter discussing Device Independence. In the next chapter we will see the development of DI to MDI or Measurement Device Independence as well as some associated protocols.

Chapter 5

Measurement Device Independence

This chapter deals with Measurement Device Independence, its requirements and implementation as well as a protocol that was recently developed to overcome a few more side channels. Additionally we shall have a brief look at the Coherent State in this chapter as well, since it plays a major role in one of the MDIQKD protocols.

5.1 MDI QKD

Measurement Device Independent (MDI) QKD, as the name suggests, grants us independence from only our measurement devices. This gives us less independence than proposed in DI protocols, however, we will see how this protocol is not only secure but gives reasonably better key generation rates than DI protocols. MDI-QKD was initially proposed in a 2012 paper [13] and the goal was to have a secure and effective QKD protocol that could also be implemented using the devices available on the market at the time.

5.1.1 Protocol Outline

The assumptions made for both DI and MDI QKD are similar except for the added assumption in MDI that Alice and Bob should be able to generate their states perfectly, i.e. no state preparation flaws. Let us now look at a simplified MDI protocol that was proposed by the authors of the original paper.

1. Alice and Bob send their signals, which in this case are phase randomized Weak Coherent Pulses (WCPs) and their decoy states in the BB84 state setting, to an untrusted middle party, Charles.

2. Charles has been given the task to perform a Bell State Measurement (BSM) on the incoming signals and to announce the success or failure of this operation as well as which Bell State was obtained.

3. After the quantum communication with Charles, Alice and Bob use an authenticated public channel to select only those events where a successful result was announced by Charles. Furthermore, just like in BB84, they keep only those events where they used the same basis. Lastly, based on an earlier decision, either one of them, Alice or Bob flip their bit values based on the Bell State obtained by Charles, to ensure the correct correlation of their bits.

4. The sifting process complete, Alice and Bob can now move on to obtain a QBER and gain for their experiment.

In this protocol, we have used a BB84 like setup due to its ability to expose Eve in the errors that she introduces. Since quantum states cannot be cloned, Eve will always introduce errors when wanting to gain information about the system and we can find out this information by calculating the Quantum Bit Error Rate (QBER). Afterwards, just like the BB84 protocol, privacy amplification is carried out to further restrict Eve's information.

The use of the quantum channel is only during the communication of the WCPs from Alice & Bob to Charles. All other communications are carried out on an authenticated public channel, and hence, are completely open to Eve. Furthermore, we also have that it may as well be Eve acting as the relay between Alice & Bob and yet still the protocol will remain secure from Eve, given that she announces the BSM results. Theoretically, the signal states can be projected into one of the four possible Bell States, however, in the experimental realization of the protocol, we are restricted to only two Bell States: The state which is anti-symmetric under particle exchange $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ and the symmetric state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$. $|H\rangle$ & $|V\rangle$ here are representing the horizontal and vertical polarization states respectively. They arise from the physical realization of the BSM apparatus which houses a Photon Beam-Splitter (PBS) and a Beam Splitter (BS). To generate the Bell states, we show the quantum circuits used and the inputs required for each state in figures 5.1, 5.2, 5.3 and 5.4.

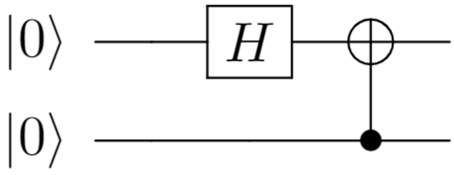

Figure 5.1: Φ^+

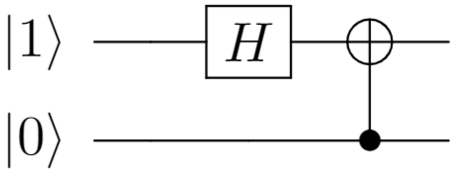

Figure 5.2: Φ^-

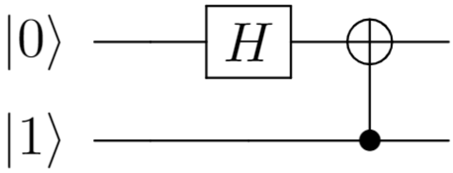

Figure 5.3: Ψ^+

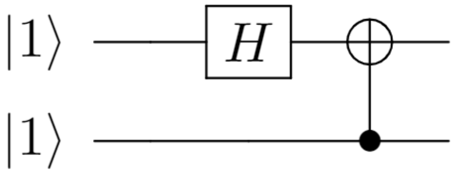

Figure 5.4: Ψ^-

Even though through the Quantum Circuit Diagram (QCD) it looks simple enough to generate the four Bell States, however, in practical application it is easier to generate and identify the two states of Ψ^+ & Ψ^-. In the MDI protocol discussed above, the particular setup that we have is one which acts on the inputs from Alice and Bob to output either Ψ^+ or Ψ^- or neither. This is achieved in the following way:

Input State: $|0\rangle_A |0\rangle_B$

For this input state, we have quite simply that the output state will also just be the same after the BS action.

$$|0\rangle_A |0\rangle_B \xrightarrow{BS} |0\rangle_C |0\rangle_D \tag{5.1}$$

Input State: $|1\rangle_A |0\rangle_B$

This follows from (4.12) and in the same way we have the output as

$$|1\rangle_A |0\rangle_B \xrightarrow{BS} \frac{1}{\sqrt{2}}(|0\rangle_C |1\rangle_D \; + \; |1\rangle_C |0\rangle_D) \tag{5.2}$$

Input State: $|0\rangle_A |1\rangle_B$

This is the input state from (4.12)

Input State: $|1\rangle_A |1\rangle_B$

This is the input state from (4.13)

Since we have polarizing beam splitter in the measurement apparatus, it is important to know how the polarization modes are related to the spatial modes [21]. For the two Bell states that we can obtain in our outputs, we have the following relations when the beams leave the 50:50 BS and into the PBS:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|H_1\rangle |V_2\rangle + |V_1\rangle |H_2\rangle)(|a_1\rangle |b_2\rangle + |b_1\rangle |a_2\rangle) \tag{5.3}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H_1\rangle |V_2\rangle - |V_1\rangle |H_2\rangle)(|a_1\rangle |b_2\rangle - |b_1\rangle |a_2\rangle) \tag{5.4}$$

The action of the PBS is such that it transmits the vertically polarized photon while reflecting the horizontal one. As such, for the cases of the input states $|1\rangle_A |1\rangle_B$ and $|0\rangle_A |0\rangle_B$ the output does not resemble a Bell State. While the two input states $|1\rangle_A |0\rangle_B$ and $|0\rangle_A |1\rangle_B$ are likened to the Bell States Ψ^+ or Ψ^- respectively. This is so because in the polarization states we see $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle |V\rangle + |V\rangle |H\rangle)$ and $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle |V\rangle - |V\rangle |H\rangle)$ where the two output states are symmetric and anti-symmetric respectively. Hence in a detection event where the horizontal and vertical detectors on the same side, after the BS, detect photons then we have the state $|\Psi^+\rangle$ while if the opposite side horizontal and vertical detectors go off we'll have an output of the state $|\Psi^-\rangle$.

It is useful to see how the input bits are correlated for each BSM result. In the practical case where we got only two of the Bell States as the outputs, the correlation between the measurement basis and BSM result is represented in the following table.

Table 5.1: State Correlations

Alice & Bob	Charles' Output: $\|\Psi^-\rangle$	Charles' Output: $\|\Psi^+\rangle$
Rectilinear Basis	Bit Flip	Bit Flip
Diagonal Basis	Bit Flip	-

In this protocol, our basis choices are like those of BB84. We use the polarization states which are in the Diagonal and the Rectilinear basis. We will now analyze our protocol, how the key is generated and how Eve's information is limited after we get to know of the error she introduces. The rectilinear basis are going to be used to obtain the sifted key, while the diagonal basis is used only for the purpose of finding the amount of privacy amplification required. The diagram in 5.5 shows a most simplistic of setups, given the proper optical elements of course, to execute an MDI type protocol.

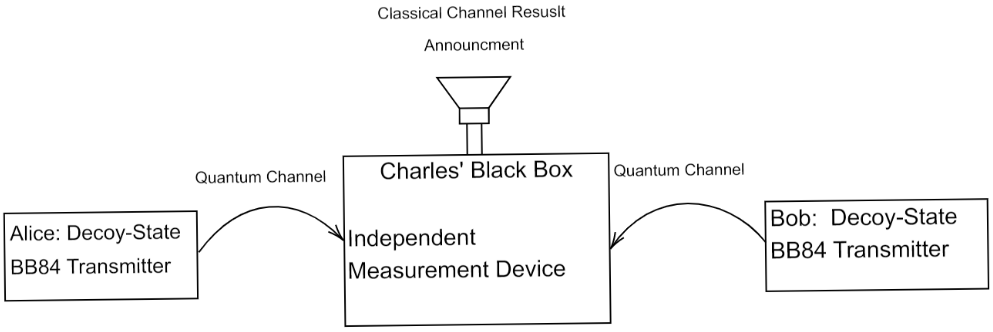

Figure 5.5: Black Box Diagram

While when we look at the measurement device itself for the MDI protocol under discussion, we find that it is structured in the following way.

5.1.2 Protocol Analysis

Going forward, we will be using the following notation for gain and QBER in the rectilinear and diagonal basis respectively: $Q^{n,m}_{\text{rect}}, Q^{n,m}_{\text{diag}}$ & $e^{n,m}_{\text{rect}}, e^{n,m}_{\text{diag}}$. For this protocol, when talking about the error in the rectilinear basis we have assumed first that Alice and Bob have perfect state preparation, without flaws such as misalignment of optical elements. Given this assumption, we say that the only way for an error to occur is if both Alice and Bob send their states in the same polarization state and Charles to output a successful measurement. Surely, since their results need to be anti-correlated for the rectilinear case for either output, we have that so long as the same polarization states were sent by Alice and Bob, $e^{n,m}_{\text{rect}} = 0$ for all choices of n,m.

Now for the diagonal case, which is to say that the states sent were in the diagonal basis, when we say an error has occurred, it means the output of $|\psi^-\rangle$ while they sent the same state and output of $|\psi^+\rangle$ when they prepared orthogonal states. This is so due to how the particular Bell States correlate Alice and Bobs input states. Going with the same assumption as given above, for the ideal preparation of states, we have that $e^{1,1}_{diag} = 0$.

All of this is to say that since in this protocol one can identify exactly when the error has occurred, in the ideal case, and hence the key generation rate is given very simply by just the gain in the rectilinear basis. Since only the rectilinear basis are used to get our sifted key, the key generation rate is $R = Q^{1,1}_{\text{rect}}$ in the special case of sending an infinite number of signals, i.e. the asymptotic scenario.

Realizing however that an ideal scenario cannot be achieved physically due to a host of errors, we find that the key generation rate for the asymptotic case is actually given by

$$R \geq Q^{1,1}_{\text{rect}}[1 - H(e^{1,1}_{\text{diag}})] - Q_{\text{rect}} f(E_{\text{rect}}) H(E_{\text{rect}}))$$

$Q^{1,1}_{\text{rect}}$ gives us the gain in the rectilinear basis for the single photon case. This gain implies that Alice and Bob sent single photon signals to Charles, who then declared a successful BSM result. This is similar to the ideal scenario without errors as mentioned prior. However, this time there is a factor multiplying with our single photon gain. Here,

$$H(x) = -xlog_2(x) - (1-x)log_2(1-x)$$

is the Shanon Binary Entropy function while $e^{1,1}_{\text{diag}}$ is the error rate calculated using the diagonal basis, which we established at the start of the protocol. It gives us the expression $Q^{1,1}_{\text{rect}} - Q^{1,1}_{\text{rect}} H(e^{1,1}_{\text{diag}})$ where the second term tells us about the information, to be taken out of the final key, lost during the privacy amplification for the protocol.

The next term represents the information that is to be taken out of the sifted key due to the the error correction part of the protocol. This information gets revealed by Alice and hence must be discarded. Here, Q_{rect} is the gain in the rectilinear basis for all signal states and for this protocol it has the form $Q_{\text{rect}} = \sum_{n,m} Q^{n,m}_{\text{rect}}$. While E_{rect} has the form $E_{\text{rect}} = \sum_{n,m} Q^{n,m}_{\text{rect}} e^{n,m}_{\text{rect}} / Q_{\text{rect}}$. The term $f(E)$ or f_e is known as the error correction inefficiency function whose value is greater than equal to 1, $(f_e \geq 1)$. The exact value depends upon the error correction protocol that is used within the QKD protocol.

It must be noted here that Q_{rect} and E_{rect} can be obtained from the experiment itself, such is the setup of the protocol, while in order to obtain $Q^{1,1}_{\text{rect}}$ and $e^{1,1}_{\text{rect}}$ we turn to a slightly modified version of the Decoy State protocol as it applies on this MDI setup. As discussed in the Decoy State section. The way we calculate gain and the error rate is in much the same way. The equations for gain and error rate are indeed mostly the same with the difference here being that both parties are the ones sending signals, so both will have their own decoy state settings. Hence the modified expressions are:

$$Q^{i,j}_{\text{rect}} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n}{n!} e^{-\mu_i} \frac{\mu_j^m}{m!} e^{-\mu_j} Y^{n,m}_{rect} \tag{5.5}$$

$$Q^{i,j}_{\text{diag}} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n}{n!} e^{-\mu_i} \frac{\mu_j^m}{m!} e^{-\mu_j} Y^{n,m}_{diag} \tag{5.6}$$

While for the QBER in both basis we have:

$$Q^{i,j}_{\text{rect}} E^{i,j}_{\text{rect}} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n}{n!} e^{-\mu_i} \frac{\mu_j^m}{m!} e^{-\mu_j} Y^{n,m}_{\text{rect}} e^{n,m}_{\text{rect}} \tag{5.7}$$

$$Q^{i,j}_{\text{diag}} E^{i,j}_{\text{diag}} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n}{n!} e^{-\mu_i} \frac{\mu_j^m}{m!} e^{-\mu_j} Y^{n,m}_{\text{diag}} e^{n,m}_{\text{diag}} \tag{5.8}$$

The index i and j here denote the different decoy state settings for Alice and Bob respectively. There can of course theoretically be an infinite amount of decoy state settings, but practically we need only a few to obtain the relevant parameters involved in the determination of the key generation rate. As was also demonstrated in the decoy state protocol section. In order to begin solving the large system of equations, we should note here that the following simplifications can be made. Firstly looking to find the gain in the rectilinear basis $Q^{i,j}_{rect}$ we can write eq.(5.5) as

$$Q^{i,j}_{\text{rect}} = \sum_{n=0}^{\infty} \frac{\mu_i^n}{n!} e^{-\mu_i} Y^{j}_{n;\text{rect}} \tag{5.9}$$

Here we have that

$$Y^{j}_{n;\text{rect}} = \sum_{m=0}^{\infty} \frac{\mu_j^m}{m!} e^{-\mu_j} Y^{n,m}_{\text{rect}} \tag{5.10}$$

We note first that eq.(5.9) looks very similar to eq.(3.16) if we hold j fixed. This is how we can then find out the parameter $Y^{j}_{n;\text{rect}}$. Having done so we realize that eq.(5.10) follows through in similar fashion so now both parties can obtain an estimate on the parameter $Y^{n,m}_{\text{rect}}$. As for the diagonal gain, it follows the same idea as applied on the rectilinear gain. Next we turn our attention to the QBER for this protocol, we shall realize that this also relies on the same tactic as applied on the previous case for the gain. We start off by rewriting the the QBER expression as:

$$Q^{i,j}_{\mathrm{rect}} E^{i,j}_{\mathrm{rect}} = \sum_{n=0}^{\infty} \frac{\mu_i^n}{n!} e^{-\mu_i} W^j_{n;\mathrm{rect}} \tag{5.11}$$

Where

$$W^j_{n;\mathrm{rect}} = \sum_{m=0}^{\infty} \frac{\mu_j^m}{m!} e^{-\mu_j} Y^{n,m}_{\mathrm{rect}} e^{n,m}_{\mathrm{rect}} \tag{5.12}$$

Here also we draw a similar equivalence as before, that eq.(5.11) resembles eq.(3.17) for fixed j. For now we can evaluate $W^j_{n;\mathrm{rect}}$ and then make the same equivalence to estimate $e^{n,m}_{\mathrm{rect}}$ from eq.(5.12). The same can be then done for the diagonal basis as well.

5.1.3 Experimental Realization

Theoretically, MDI-QKD offers a very secure and effective way for communication, however, a practical application has very many short comings. Of course single photon sources have not been an issue for this protocol since it establishes the key using weak coherent pulses. There is, however, a requirement in this protocol that the signal photons produced from two independent sources (Alice and Bob) need to be indistinguishable. This requirement exists for the **photon bunching effect** to occur, which in turn is what allows us to realize this protocol. It was shown that two off-the-shelf lasers could indeed produce indistinguishable photons when, by interfering the signals from these two sources, a Hong-Ou-Mandel dip was obtained.

Furthermore, one can alter the encoding schemes for the signals. For the case of the polarization encoding scheme discussed in this protocol, one has to be mindful about the errors induced while the signal travels the length of a long cable. Polarization rotation error in the fibre can be overcome using polarization feedback control, which was indeed demonstrated in [7]

5.2 The Coherent State

Before we can move on to the next protocol, we shall first have a look at the Coherent State. We shall only briefly look at the Coherent State as it relates to the action of the BS. The coherent state is expressed as: [18]

$$|\alpha\rangle \;=\; e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle \tag{5.13}$$

We see that it is a state made by the superposition of the number states. From this we can get the probability of having a particular number state. So we have then that the probability of getting the state $|m\rangle$ from the coherent state is $P_n \;=\; e^{-|\alpha|^2}\frac{(|\alpha|^2)^n}{n!}$ This probability is a Poissonian distribution for n.

Now lets express the coherent state in terms of the vacuum state which would then help us in the BS action. The coherent state can be written in the following way:

$$|\alpha\rangle \;=\; D(\alpha)\,|0\rangle \tag{5.14}$$

Where $D(\alpha)$ is known as the displacement operator and defined as

$$D(\alpha) \;=\; e^{(\alpha a^{\dagger} - \alpha^{*} a)} \tag{5.15}$$

While we can also express this exponent using the disentanglement formula as:

$$D(\alpha) \;=\; e^{-\frac{1}{2}|\alpha|^2}e^{\alpha a^{\dagger}}e^{-\alpha^{*}a} \tag{5.16}$$

For the coherent state, an interesting property to note is for $D^{\dagger}(\alpha)$, for which we have that:

$$D^{\dagger}(\alpha) \;=\; D(-\alpha) \;=\; D^{-1}(\alpha) \;=\; e^{-(\alpha a^{\dagger}-\alpha^{*}a)}$$

Now to see how the beam splitter action effects inputs that have the coherent states.

5.2.1 Input State: $|0\rangle_A |\alpha\rangle_B$

$$|0\rangle_A |\alpha\rangle_B \longrightarrow D(\alpha)\,|0\rangle_A |0\rangle_B \longrightarrow e^{(\alpha a^{\dagger}-\alpha^{*}a)}\,|0\rangle_A |0\rangle_B$$

$$e^{(\alpha a^{\dagger}-\alpha^{*}a)}\,|0\rangle_A |0\rangle_B \xrightarrow{BS} e^{(\alpha(\frac{c^{\dagger}+d^{\dagger}}{\sqrt{2}})-\alpha^{*}(\frac{c+d}{\sqrt{2}}))}\,|0\rangle_A |0\rangle_B$$

By rearranging the terms in the exponential we get the following form.

$$e^{\frac{1}{\sqrt{2}}(\alpha c^{\dagger}-\alpha^{*}c)+\frac{1}{\sqrt{2}}(\alpha d^{\dagger}-\alpha^{*}d)}\,|0\rangle_A |0\rangle_B$$

Now since the two terms in the exponent, for input c and input d, commute with one another, we can disentangle them easily. So:

$$e^{\frac{1}{\sqrt{2}}(\alpha c^{\dagger}-\alpha^{*}c)+\frac{1}{\sqrt{2}}(\alpha d^{\dagger}-\alpha^{*}d)} \;\longrightarrow\; e^{\frac{1}{\sqrt{2}}(\alpha c^{\dagger}-\alpha^{*}c)}e^{\frac{1}{\sqrt{2}}(\alpha d^{\dagger}-\alpha^{*}d)}$$

Where on the right of the expression, the two terms of the exponent basically just represent modified displacement operators of the form $D_C(\frac{\alpha}{\sqrt{2}})D_D(\frac{\alpha}{\sqrt{2}})$

Finally then, we get,

$$|0\rangle_A |\alpha\rangle_B \;\xrightarrow{BS}\; \left|\frac{\alpha}{\sqrt{2}}\right\rangle_C \left|\frac{\alpha}{\sqrt{2}}\right\rangle_D \tag{5.17}$$

5.2.2 Input State: $|\alpha\rangle_A |{-\alpha}\rangle_B$

Here, the state $|{-\alpha}\rangle$ is defined by the action of $D(-\alpha)$ on the vacuum state. So then we have that:

$$|\alpha\rangle_A |\alpha\rangle_B \longrightarrow D_A(\alpha)D_B(-\alpha)|0\rangle_A |0\rangle_B$$

$$D_A(\alpha)D_B(-\alpha)|0\rangle_A |0\rangle_B \longrightarrow e^{(\alpha a^\dagger - \alpha^* a)} e^{(\alpha^* b - \alpha b^\dagger)}$$

Noting that the operators in the exponent transform through the BS action, we have the prior transformation equations to help us transform $a, a^\dagger, b, b^\dagger$

$$e^{(\alpha a^\dagger - \alpha^* a)} e^{-(\alpha b^\dagger - \alpha^* b)} \xrightarrow{BS} e^{(\alpha(\frac{c^\dagger + d^\dagger}{\sqrt{2}}) - \alpha^*(\frac{c+d}{\sqrt{2}}))} e^{(\alpha^*(\frac{c-d}{\sqrt{2}}) - \alpha(\frac{c^\dagger - d^\dagger}{\sqrt{2}}))}$$

Rearranging the first exponent as done earlier, we have

$$e^{(\alpha(\frac{c^\dagger + d^\dagger}{\sqrt{2}}) - \alpha^*(\frac{c+d}{\sqrt{2}}))} \longrightarrow e^{\frac{1}{\sqrt{2}}(\alpha c^\dagger - \alpha^* c)} e^{\frac{1}{\sqrt{2}}(\alpha d^\dagger - \alpha^* d)}$$

The other exponent term that came from $D_B(-\alpha)$ modifies in the following way.

$$e^{(\alpha^*(\frac{c-d}{\sqrt{2}}) - \alpha(\frac{c^\dagger - d^\dagger}{\sqrt{2}}))} \longrightarrow e^{\frac{1}{\sqrt{2}}(\alpha^* c - \alpha c^\dagger) - \frac{1}{\sqrt{2}}(\alpha^* d - \alpha d^\dagger)}$$

Where the exponent at the end can be disentangled in much the same way as the one associated with $D_A(\alpha)$,

$$e^{\frac{1}{\sqrt{2}}(\alpha^* c-\alpha c^\dagger)}e^{-\frac{1}{\sqrt{2}}(\alpha^* d-\alpha d^\dagger)} \longrightarrow e^{-\frac{1}{\sqrt{2}}(\alpha c^\dagger-\alpha^* c)}e^{\frac{1}{\sqrt{2}}(\alpha d^\dagger-\alpha^* d)}$$

,

Putting all of the exponents together from the term $e^{(\alpha(\frac{c^\dagger+d^\dagger}{\sqrt{2}})-\alpha^*(\frac{c+d}{\sqrt{2}}))}e^{(\alpha^*(\frac{c-d}{\sqrt{2}})-\alpha(\frac{c^\dagger-d^\dagger}{\sqrt{2}}))}$ we will be able to simplify the expression.

$$e^{\frac{1}{\sqrt{2}}(\alpha c^\dagger-\alpha^* c)}e^{\frac{1}{\sqrt{2}}(\alpha d^\dagger-\alpha^* d)}e^{-\frac{1}{\sqrt{2}}(\alpha c^\dagger-\alpha^* c)}e^{\frac{1}{\sqrt{2}}(\alpha d^\dagger-\alpha^* d)}$$

,

Notice that the two exponents in the middle have operators that commute, and hence we can switch their positions, simplifying the expression and leaving us only with the exponents associated with the operators for the output d.

$$e^{\frac{1}{\sqrt{2}}(\alpha d^\dagger-\alpha^* d)}e^{\frac{1}{\sqrt{2}}(\alpha d^\dagger-\alpha^* d)} \longrightarrow e^{\frac{2}{\sqrt{2}}(\alpha d^\dagger-\alpha^* d)} \longrightarrow e^{\sqrt{2}(\alpha d^\dagger-\alpha^* d)}$$

,

where the term $e^{\sqrt{2}(\alpha d^\dagger-\alpha^* d)}$ is just $D_D(\sqrt{2}\alpha)$, so going from the input to the output, we can finally express our output state in the following way:

$$D_A(\alpha)D_B(-\alpha)\left|0\right\rangle_A\left|0\right\rangle_B \overset{BS}{\longrightarrow} \left|0\right\rangle_C\left|\sqrt{2}\alpha\right\rangle_D \tag{5.18}$$

We can similarly get the output states for a few other cases where in both inputs we have a combination of the states $|\alpha\rangle$ or $|-\alpha\rangle$. Accounting for all the possible inputs, we have:

a: $\left|\alpha\right\rangle_A\left|\alpha\right\rangle_B$

b: $\left|-\alpha\right\rangle_A\left|-\alpha\right\rangle_B$

c: $\left|-\alpha\right\rangle_A \left|\alpha\right\rangle_B$

d: $\left|\alpha\right\rangle_A \left|-\alpha\right\rangle_B$

For the above mentioned inputs, by the action of the BS, we shall have the following outputs, respectively:

➨
$$\left|\sqrt{2}\alpha\right\rangle_C \left|0\right\rangle_D \tag{5.19}$$

➨
$$\left|-\sqrt{2}\alpha\right\rangle_C \left|0\right\rangle_D \tag{5.20}$$

➨
$$\left|0\right\rangle_C \left|-\sqrt{2}\alpha\right\rangle_D \tag{5.21}$$

➨
$$\left|0\right\rangle_C \left|\sqrt{2}\alpha\right\rangle_D \tag{5.22}$$

5.3 Curty 2020 MDI Protocol

Despite MDI-QKD protocol proposed in the original 2012 paper being an effective and secure protocol given physical constraints, we still had certain assumptions that needed to be satisfied. Primarily, the assumption on the state preparation of Alice and Bob being perfect. It is hard for them to to do so in reality due to the errors that can be introduced by the devices themselves or indeed the presence of the eavesdropper Eve. Eve can carry out what's known as a Trojan Horse Attack (THA) and obtain information about the internal settings of the devices inside Alice and Bob's labs, devices assumed to be secure. The goal is to remove all side channels that are introduced by the devices, as stated in Device Independent QKD. The authors hence proposed a simple MDI protocol that can makeup for the security loophole due to Alice and Bob's devices [16].

5.3.1 Protocol Outline

The present protocol carries out similarly to the original MDI protocol, in that there is still the untrusted observer, Charles, who is in control of the measurement device. Again, the assumption is that Eve may as well be the one controlling the measurement device, as long as she announces the result of the measurement outcome.

1. Alice and Bob both send coherent states to Charles.
   (a) The states are $|\nu\rangle_a \,\&\, |\omega\rangle_b$ where $\nu, \omega \in \tau := [\alpha, -\alpha, vac]$ with respective probabilities $p_a \& p_b$
   (b) Here, $|\alpha\rangle$ is registered as the bit value 0 and $|-\alpha\rangle$ is the bit value 1. The vacuum states are sent in order to estimate the parameters required for the secret key rate.
2. Charles interferes the two incoming signals in a 50:50 beamsplitter(BS). We assume Charles is honest and performs the task given.
   (a) There are two threshold detectors where the signals from the 50:50 BS reach. Detectors are labeled D_c & D_d.
   (b) Measurement outcomes in this case are $\Omega \in \{\Omega_c, \Omega_d\}$, corresponding to a click in D_c and D_d respectively. Otherwise the measure-

ment is a failure.

3. This process is repeated N times. Alice and Bob will reveal all those states where at least one vacuum state was sent by either party. The remaining events where Charles announced a successful measurement will constitute the sifted key.

4. Using the sifted key, Alice and Bob can estimate the bit and phase error rate, after which they perform error correction and privacy amplification.

Since this is a MDI type setup, we know that the side-channels related to the measurement device will not effect the security of the protocol. Hence the discussion can be focused on the side-channels on the transmitter end.

Protocol Diagram:

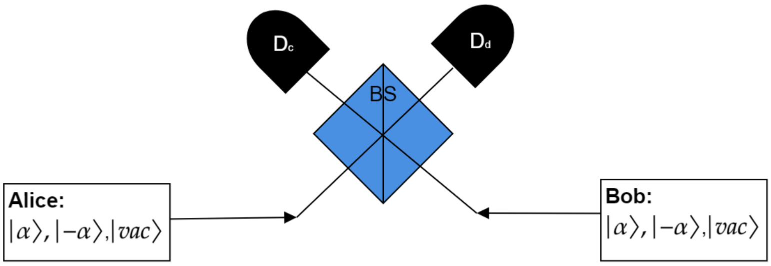
D_c
D_d
BS
Alice:
$|\alpha\rangle, |-\alpha\rangle, |vac\rangle$
Bob:
$|\alpha\rangle, |-\alpha\rangle, |vac\rangle$

Figure 5.6: MDI Protocol

In the diagram in figure 5.6, we have the two detectors D_c and D_d which are respectively associated with constructive and destructive interference. As seen in the results of eq.(19-22) we have that when they send the opposite signal states, detector D_d should click while if they send the same states, then

D_c should click. For a click in D_d, their states are seen to be anti-correlated and hence one of the parties involved, Alice and Bob, must perform a bit flip to have the correct correlation.

5.3.2 Secret Key Rate

The secret key rate for this protocol is given by

$$R \geq Q[1 - H(e_{ph}^{U}) - f_e H(e_{bit})] \tag{5.23}$$

Since we will be using only those instances where both Alice and Bob send key states and Charles outputs a successful result, Q denoted the probability of such an event taking place. The phase error rate, denoted by e_{ph} is to be defined in the upcoming section as it is not clearly observable from the protocol itself. While the bit error rate e_{bit} is given by:

$$e_{bit} = \frac{p_d}{2p_d + e^{2\sqrt{\eta}\alpha^2} - 1} \tag{5.24}$$

5.3.3 Phase Error

In order to understand what a phase error looks like in this protocol, we make use of the virtual scenario constructed earlier, and go through the following bit of maths, which does use the results of the coherent states passing through beam splitters, obtained in the section on Beam Splitters.

First we write out our virtual state fully, as:

$$|\Psi\rangle^{vir} = \frac{1}{2}\left(|00\rangle_{AB}|\alpha,\alpha\rangle_{ab} \ + \ |01\rangle_{AB}|\alpha,-\alpha\rangle_{ab} \ + \ |10\rangle_{AB}|-\alpha,\alpha\rangle_{ab} \ + \ |11\rangle_{AB}|-\alpha,-\alpha\rangle_{ab}\right) \tag{5.25}$$

It is important to note that the virtual states [AB] are expressed in the z-

basis. When the above state is passed through the beam splitter, or rather, after applying the beam splitter operation on the inputs [ab].

$$|\Psi\rangle^{vir} = \frac{1}{2}\left(|00\rangle_{AB}\left|\sqrt{2}\alpha\right\rangle_c + |11\rangle_{AB}\left|-\sqrt{2}\alpha\right\rangle_c\right) \\ + \frac{1}{2}\left(|01\rangle_{AB}\left|\sqrt{2}\alpha\right\rangle_d + |10\rangle_{AB}\left|-\sqrt{2}\alpha\right\rangle_d\right) \quad (5.26)$$

Now we look at the terms dealing with the output at c, and recall the form of the coherent state when it was expressed as a superposition of number states. Modifying the expression for $|\alpha\rangle$ to get the expression for $\left|\sqrt{2}\alpha\right\rangle$

$$\left|\sqrt{2}\alpha\right\rangle = e^{-\frac{1}{2}|\sqrt{2}\alpha|^2}\sum_{n=0}^{\infty}\frac{(\sqrt{2}\alpha)^n}{\sqrt{n!}}|n\rangle \quad (5.27)$$

And similarly for $\left|-\sqrt{2}\alpha\right\rangle$.

Labeling the virtual state that deals with the output at c as $|\Psi\rangle_c$ we have that:

$$|\Psi\rangle_c = \frac{1}{2}\left(|00\rangle_{AB}\left|\sqrt{2}\alpha\right\rangle_c + |11\rangle_{AB}\left|-\sqrt{2}\alpha\right\rangle_c\right) \quad (5.28)$$

We separate the odd and even portions of the sum of states and get

$$|\Psi\rangle_c = \frac{e^{-|\alpha|^2}}{2}\left(|00\rangle_{AB}\left[\sum_{n=1;odd}^{\infty}\frac{(\sqrt{2}\alpha)^n}{\sqrt{n!}}|n\rangle + \sum_{n=2;even}^{\infty}\frac{(\sqrt{2}\alpha)^n}{\sqrt{n!}}|n\rangle + |0\rangle\right] + \\ |11\rangle_{AB}\left[\sum_{n=1;odd}^{\infty}\frac{(-\sqrt{2}\alpha)^n}{\sqrt{n!}}|n\rangle + \sum_{n=2;even}^{\infty}\frac{(-\sqrt{2}\alpha)^n}{\sqrt{n!}}|n\rangle + |0\rangle\right]\right) \quad (5.29)$$

After rearranging the terms a bit and simplifying, we finally get the form of $\left|\Psi\right\rangle_c$ as

$$\left|\Psi\right\rangle_c = \frac{e^{\alpha^2}}{\sqrt{1-e^{2\alpha^2}}}\left(\left[\sum_{n=1;odd}^{\infty}\frac{(\sqrt{2}\alpha)^n}{\sqrt{n!}}\left|n\right\rangle\right]\otimes\frac{1}{\sqrt{2}}\left(\left|00\right\rangle_{AB}-\left|11\right\rangle_{AB}\right)\right.$$
$$\left.+\left[\sum_{n=2;even}^{\infty}\frac{(\sqrt{2}\alpha)^n}{\sqrt{n!}}\left|n\right\rangle\right]\otimes\frac{1}{\sqrt{2}}\left(\left|00\right\rangle_{AB}+\left|11\right\rangle_{AB}\right)\right) \tag{5.30}$$

Now we make the approximation for small α which gives us the expression

$$\left|\Psi\right\rangle_c \approx \frac{e^{\alpha^2}\alpha}{\sqrt{1-e^{2\alpha^2}}}\left(\left|00\right\rangle_{AB}-\left|11\right\rangle_{AB}\right)\otimes\left|1\right\rangle_c \tag{5.31}$$

Where we see the $n = 1$ term only in the above expression. Since the measurement on the ancilla bits was supposed to be done in the X-basis, we have one final transformation of the above expression. Since the ancilla bits expressed up till now were done so in the Z-basis, making the change to the X-basis we get:

$$\left|\Psi\right\rangle_c = \frac{e^{\alpha^2}\alpha}{\sqrt{1-e^{2\alpha^2}}}\left(\left|0_x1_x\right\rangle_{AB}+\left|1_x0_x\right\rangle_{AB}\right)\otimes\left|1\right\rangle_c \tag{5.32}$$

As for $\left|\Psi\right\rangle_d$ we obtain the result,

$$\left|\Psi\right\rangle_d = \frac{e^{\alpha^2}\alpha}{\sqrt{1-e^{2\alpha^2}}}\left(\left|1_x0_x\right\rangle_{AB}-\left|0_x1_x\right\rangle_{AB}\right)\otimes\left|1\right\rangle_d \tag{5.33}$$

It is now that we can finally see how in the virtual scenario a phase error can be defined, it is when Alice and Bob observe outcomes $\left|0_x0_x\right\rangle$ or $\left|1_x1_x\right\rangle$ we would then say that a phase error has occurred. This is most important for the protocol to know the errors and hence incorporate them in the Key Generation rate.

Chapter 6

Conclusion

In this thesis we have was presented the development from BB84 with decoy states to a measurement device independent protocol that is secure against trojan horse attacks. The development was traced in terms of how the protocols work with their particular signal states and the devices involved. As is the case with all QKD protocols, they are secure so long as the assumptions in their respective security proofs are upheld. We have also seen that with each imperfection in the devices, there arise side-channels for Eve to exploit and since imperfections are a part of our physical reality, there will always be a need for more secure QKD protocols. In terms of Discrete Variable (DV) QKD, which has been discussed in this document, MDI protocols are so far the optimal. There are further avenues of research to pursue for the current protocol. This is the case since the last protocol discussed here [16] satisfies an MDI setup and any development in the DVQKD realm will now have to at least include some form of device independence. The reason for this is simple, security. In conclusion, the pursuit of an optimal QKD protocol will continue, dare i say, endlessly and will always need countermeasures the more we learn to characterize the environment through which the signals travel hence the more side-channels that pop up.

Bibliography

[1] Girish S. Agarwal. *Quantum Optics*. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139035170.

[2] Charles H Bennett. “Quantum cryptography using any two nonorthogonal states”. In: *Physical review letters* 68.21 (1992), p. 3121.

[3] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science* 560 (2014), pp. 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025.

[4] Dagmar Bruß. “Optimal Eavesdropping in Quantum Cryptography with Six States”. In: *Physical Review Letters* 81.14 (1998), pp. 3018–3021. ISSN: 1079-7114. DOI: 10.1103/physrevlett.81.3018. URL: http://dx.doi.org/10.1103/PhysRevLett.81.3018.

[5] W. Diffie and M. Hellman. “New directions in cryptography”. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[6] Artur K Ekert. “Quantum Cryptography and Bell’s Theorem”. In: *Quantum Measurements in Optics*. Springer, 1992, pp. 413–418.

[7] T. Ferreira da Silva et al. “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits”.

In: *Phys. Rev. A* 88 (5 Nov. 2013), p. 052303. DOI: 10.1103/PhysRevA.88.052303. URL: https://link.aps.org/doi/10.1103/PhysRevA.88.052303.

[8] Andrei Gaidash, Vladimir Egorov, and Artur Gleim. "Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices". In: *Journal of Physics: Conference Series* 735 (Aug. 2016), p. 012072. DOI: 10.1088/1742-6596/735/1/012072.

[9] N. Gisin et al. "Trojan-horse attacks on quantum-key-distribution systems". In: *Physical Review A* 73.2 (2006). ISSN: 1094-1622. DOI: 10.1103/physreva.73.022320. URL: http://dx.doi.org/10.1103/PhysRevA.73.022320.

[10] Anqi Huang et al. "Quantum key distribution with distinguishable decoy states". In: *Physical Review A* 98.1 (2018). ISSN: 2469-9934. DOI: 10.1103/physreva.98.012330. URL: http://dx.doi.org/10.1103/PhysRevA.98.012330.

[11] Won-Young Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Physical Review Letters* (2003).

[12] Christian Kurtsiefer et al. "The breakdown flash of silicon avalanche photodiodes - back door for eavesdropper attacks? J Mod Opt". In: *Journal of Modern Optics* 48 (Nov. 2001), pp. 2039–2047. DOI: 10.1080/09500340108240905.

[13] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. "Measurement-Device-Independent Quantum Key Distribution". In: *Physical Review Letters* 108.13 (Mar. 2012). ISSN: 1079-7114. DOI: 10.1103/physrevlett.

108.130503. URL: http://dx.doi.org/10.1103/PhysRevLett.108.130503.

[14] Xiongfeng Ma et al. "Practical decoy state for quantum key distribution". In: *Physical Review A* 72.1 (2005). ISSN: 1094-1622. DOI: 10.1103/physreva.72.012326. URL: http://dx.doi.org/10.1103/PhysRevA.72.012326.

[15] N. Mermin. "Period finding, factoring, and cryptography". In: *Quantum Computer Science-An Introduction-Cambridge University Press.* 2007.

[16] Álvaro Navarrete et al. "Practical Quantum Key Distribution That is Secure Against Side Channels". In: *Physical Review Applied* 15.3 (2021). ISSN: 2331-7019. DOI: 10.1103/physrevapplied.15.034072. URL: http://dx.doi.org/10.1103/PhysRevApplied.15.034072.

[17] Valerio Scarani and Christian Kurtsiefer. *The black paper of quantum cryptography: real implementation problems.* 2012. arXiv: 0906.4547 [quant-ph].

[18] Marlan O. Scully and M. Suhail Zubairy. "Coherent and squeezed states of the radiation field". In: *Quantum Optics*. Cambridge University Press, 1997, pp. 46–71. DOI: 10.1017/CBO9780511813993.004.

[19] C. E. Shannon. "Communication theory of secrecy systems". In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[20] Artem Vakhitov, Vadim Makarov, and Dag R. Hjelme. "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography". In: *Journal of Modern Optics* 48.13 (2001), pp. 2023–2038. DOI: 10.1080/09500340108240904. eprint: https://www.

tandfonline.com/doi/pdf/10.1080/09500340108240904. URL: https://www.tandfonline.com/doi/abs/10.1080/09500340108240904.

[21] GREGOR Weihs and ANTON Zeilinger. “Photon statistics at beam-splitters: an essential tool in quantum information and teleportation”. In: *Coherence and Statistics of Photons and Atoms* (2001), pp. 262–288.