

Memory Device Independent-Quantum Dialogue

A DISSERTATION

Submitted in partial fulfilment for the award of the degree

of

Master of Technology

in

Computer Science Engineering

by

Harsimran Bhasin

(17535006)



Department of Computer Science Engineering

Indian Institute of Technology Roorkee

Spring Semester, 2018-19

May 30, 2019

DECLARATION

I certify that

- (a) The work contained in this report has been done by me under the guidance of my supervisor.
- (b) The work has not been submitted to any other Institute for any degree or diploma.
- (c) I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.
- (d) Whenever I have used materials (data, theoretical analysis, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references. Further, I have taken permission from the copyright owners of the sources, whenever necessary.

Date: May 30, 2019

Place: Roorkee

(Harsimran Bhasin)

(17535006)

DEPARTMENT OF COMPUTER SCIENCE
ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE
ROORKEE - 247667, INDIA



CERTIFICATE

This is to certify that the project report entitled “Memory Device Independent-Quantum Dialogue” submitted by Harsimran Bhasin (Roll No. 17535006) to Indian Institute of Technology Roorkee towards partial fulfilment of requirements for the award of degree of Master of Technology in Computer Science Engineering is a record of bona fide work carried out by him under my supervision and guidance during Spring Semester, 2018-19.

Date: May 30, 2019

Place: Roorkee

Professor Sugata Gangopadhyay
Department of Computer Science

Engineering
Indian Institute of Technology Roorkee
Roorkee - 247667, India

Abstract

Name of the student: **Harsimran Bhasin**

Roll No: **17535006**

Degree for which submitted: **Master of Technology**

Department: **Department of Computer Science Engineering**

Thesis title: **Memory Device Independent-Quantum Dialogue**

Thesis supervisor: **Professor Sugata Gangopadhyay**

Month and year of thesis submission: **May 30, 2019**

During the last two decades of the 20th century, scientists have sought to combine elements of quantum mechanics and information processing. This has given birth to a new field of quantum computing. The importance of this new model can be learned from the fact that it gave researchers the ability to look at efficiency of an algorithm or robustness of a protocol without bothering about the underlying physical devices used for computation. This has led researchers to look at the classical algorithms in a different manner. Indeed researchers such as Gilles Brassard and Charles Bennett have shown ways in which non-classical properties of qubits provided a provably secure way of establishing cryptographic keys.(Charles H. Bennett, 1984)

Richard Feynman, Yuri Manin and others recognized quantum phenomena associated with entangled particles. This could not be simulated by Turing machines, which are supposedly the universal model of computation. This observation led researchers to think of ways in which these quantum phenomena could be used to speed up computation.(Feynman, 1981)

Chip makers have been releasing chips that fit twice as many transistors into the same space approximately in every two years. This is in compliance with an exponential curve called Moore's curve. This ongoing shrinkage in size of the chips and increased computing power led to the ubiquitous presence of computing devices all over the globe. This helped in bringing smartphones, Internet services, and new fields such as artificial intelligence and genetics to name a few. But since the early start of the second decade of 21st century, leading chipmakers like Intel have reported that it will be difficult to follow the Moore's law. Limits are being reached and there are lesser opportunities to make improvements in the given sphere of development. (Simonite, 2016)

Quantum information processing is a field that includes quantum computing, quantum cryptography, quantum communications, quantum games. The basic difference stems from the fact that the unit on which complex quantum systems are built is different from the classical one. Usual classical computes use bits which can have a low or high state. But quantum computers use quantum bits or qubits. Quantum computing provides exciting opportunities in the above respect. There are known algorithms that can perform tasks that are not feasible in polynomial time given a classical computer. Discoveries have been made of faster algorithms, novel cryptographic mechanisms and improved communications amongst entities.

Quantum computing is not parallel to optical computing or any such model. Other types of computing describe the substrate on which computation is done without changing the model of computation. A quantum computer is characterized by the way information is stored and processed. If the underlying basic principles follow quantum ways of implementation such as qubits.

Acknowledgements

I am extremely grateful to my supervisor Dr. Sugata Gangopadhyay who introduced me to the field of Quantum Computing. I express deep gratitude and thanks for the thorough teaching of concepts and motivation at every step. I would also thank sir for giving an opportunity to work in this new and booming field. I was encouraged to work on publicly available quantum computer and verify my results. I wish to thank sir for his constant guidance, without which this project would have been incomplete.



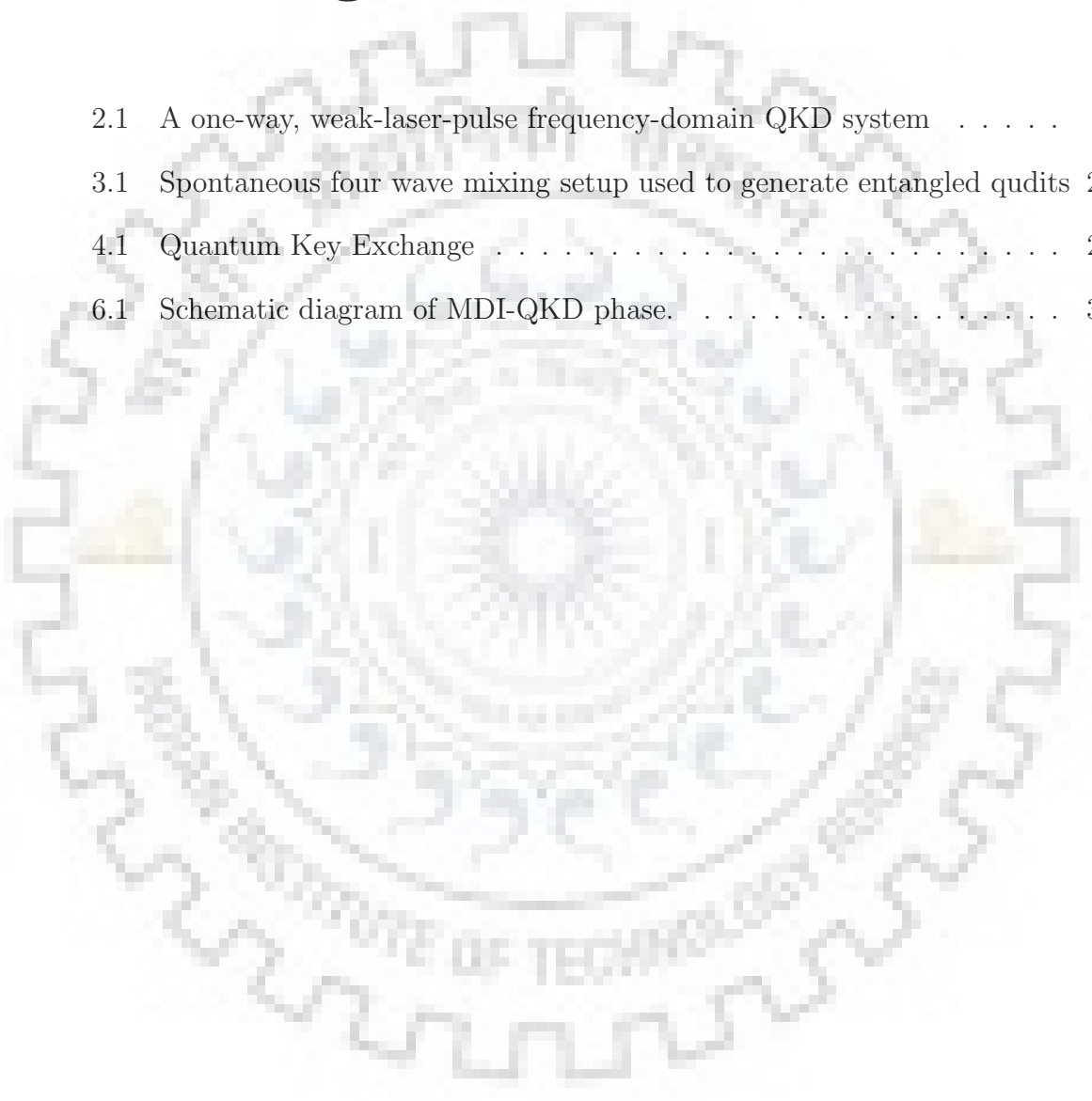
Contents

Declaration	i
Certificate	ii
Abstract	iii
Acknowledgements	v
Contents	vi
List of Figures	viii
List of Tables	ix
Abbreviations	x
Symbols	xi
1 Introduction	1
1.1 Problem Statement	1
1.2 Organisation of the report	2
2 Quantum Computing standards	3
2.1 Categorization of QKD systems based on photon source	3
2.1.1 Weak laser	3
2.1.2 One-way Mach-Zehnder	4
2.1.3 Send and return scheme(Mach-Zehnder)	5
2.1.4 Phase-intensity modulator	5
2.1.5 Coherent One-Way protocol	5
2.2 Entanglement based QKD implementations	6
2.2.1 Continuous-variable QKD	7
2.2.2 Transmitted Local Oscillator	8
2.2.3 Local Local Oscillator	8
2.3 Single photon detector	8

2.3.1	InGaAs single-photon avalanche photodiodes	10
2.3.2	Superconducting nanowire single-photon detectors	10
2.3.3	Photon detector for a CV-QKD set-up	11
2.3.3.1	Coherent detection	11
2.3.3.2	Single-quadrature homodyne detection	11
2.3.3.3	Dual-quadrature homodyne detection	11
2.3.3.4	Heterodyne detection	12
2.4	QKD Source	12
2.4.1	Parameters to specify a photon source	12
2.4.2	Types of sources	13
2.5	Modulators	14
2.5.1	Parameters to specify a modulator	14
2.6	Single photon source and detector properties for measurement	14
2.6.1	Single photon Source properties	14
2.6.2	Single photon detector properties	15
2.7	Functional security objectives	16
2.8	Security requirements	16
2.9	QKD application interface API specification	17
3	Current Technology	19
3.1	Quantum computer using microwave ion trapping technique	19
3.2	Generating entangled qudits	20
3.3	Observation of three-photon bound states	21
3.4	Silicon based two-spin qubit processor	21
3.5	Integrated photonic platform for quantum information with continuous variables	22
3.6	Universal quantum gates using spin qubits	23
3.7	High-speed quantum networking by ship	23
4	Quantum Key Distribution	25
5	Quantum Dialogue	28
6	Proposed Protocol	31
6.1	Protocol	31
6.2	Security Proof	34
6.3	Comparison with MDI-QKD	39
6.3.1	Numerical analysis	39
6.3.2	Results	43
7	Conclusion	44
7.1	Future scope	44

List of Figures

2.1	A one-way, weak-laser-pulse frequency-domain QKD system	6
3.1	Spontaneous four wave mixing setup used to generate entangled qudits	20
4.1	Quantum Key Exchange	26
6.1	Schematic diagram of MDI-QKD phase.	34




List of Tables

5.1	Different cases in transmitting qubits in QD.	30
6.1	Statistics for BB84 and B92 variants for different altitudes at 60 degrees zenith angle for GS link	43

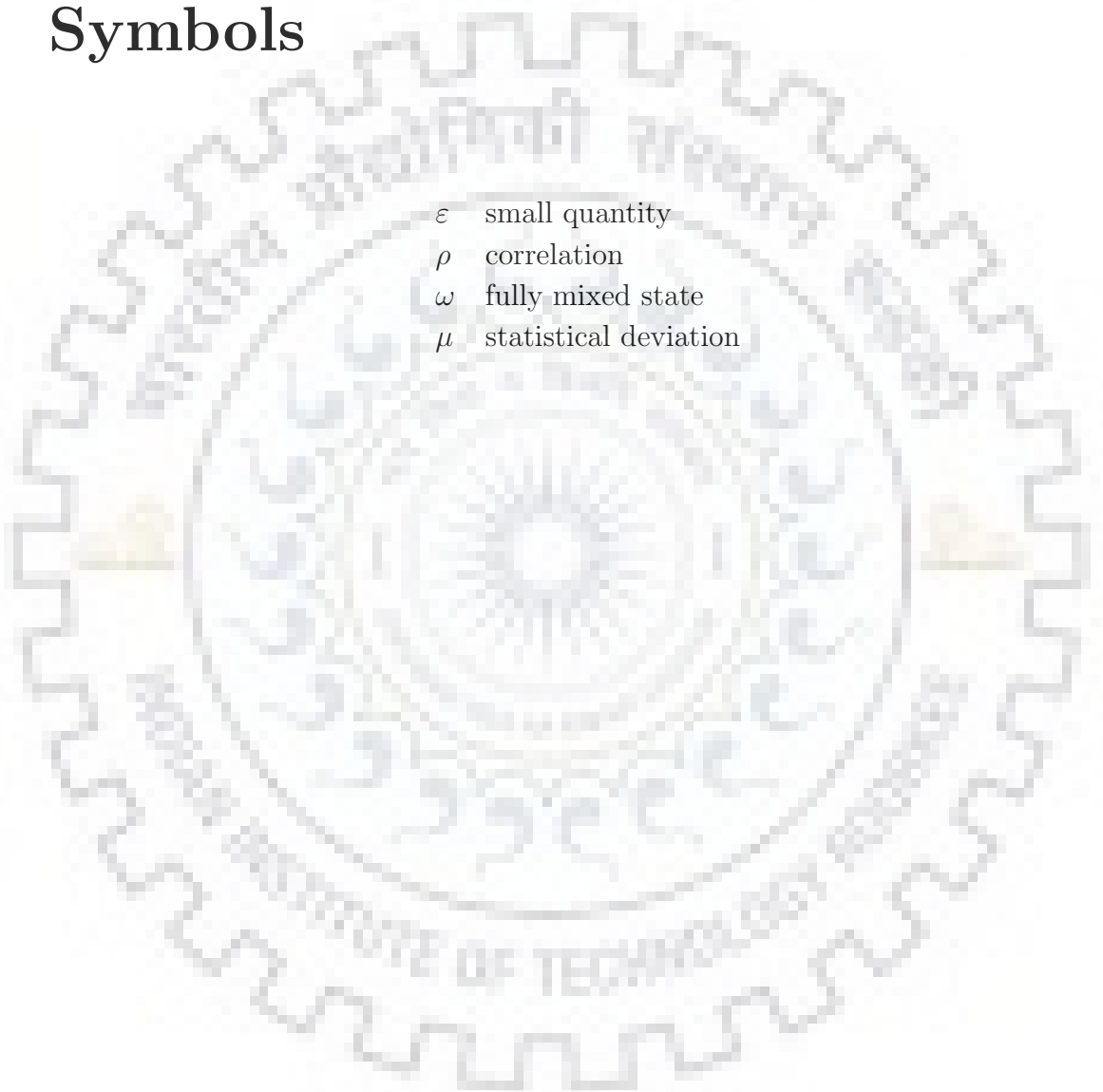


Abbreviations



QKD	Q uantum K ey D istribution
QND	Q uantum N on D emolition
AMZI	A synchronous M ach Z ehnder I nterferometer
PNS	P hoton N umber S plitting
GAPD	G eiger M ode A valanche P hotodiodes
SSB	S ingle S ide B and
WDM	W avelength D ivision M ultiplexing
COW	C oherent O ne-way P rotocol
QD	Q uantum D ialogue
QSDC	Q uantum S ecure D irect C ommunication

Symbols



ε	small quantity
ρ	correlation
ω	fully mixed state
μ	statistical deviation

Chapter 1

Introduction

Interest in quantum computing has increased over the years due to promising scope like secure key establishment and factoring of large numbers in polynomial time. The current work focuses on quantum dialogue which is a part of quantum key distribution domain. Quantum memory is expensive and not easily available due to current technological limitations. This is one of the reasons along with the fact that certain attacks can be carried out at the receiver's end where qubits could be stored, that motivated this work in memory device independent quantum key distribution.

1.1 Problem Statement

A memory device independent-quantum key distribution protocol has been proposed by (Maitra, 2017). BB84 has been used for quantum key distribution in the above protocol. The objective of this thesis is to use B92 instead of BB84 and analyse the pros and cons of B92 over BB84.

1.2 Organisation of the report

The report starts with a survey on quantum computing standards. A study has been made on categorization of QKD systems based on photon sources, entanglement based QKD implementations, photon detectors, sources, modulators, measurement properties, functional security objectives, security requirements and QKD application interface. Next, current quantum technological innovations are briefly discussed. The fourth chapter focuses on quantum key distribution which is the basic entity in quantum dialogue. Chapter five describes quantum dialogue. Chapter six discusses the proposed protocol on memory device independent- quantum key distribution. Chapter seven concludes the report and discusses the future scope of the current work.



Chapter 2

Quantum Computing standards

2.1 Categorization of QKD systems based on photon source

Most of the present implementations of QKD systems employ encoding bits using photon light sources. Orthogonal bases are used. The intended recipient needs to have knowledge of bases used by the sender for correct decoding of the sent message. In a basic model there needs to be a sender having a random sequence generator for selection of base and an encoding module. The message is sent through a quantum channel and possibly some information through a classical channel. The receiver has a random sequence generator and a decoding module. There are various electronic components for signaling and processing.

2.1.1 Weak laser

In weak laser sources, qubit values are encoded on lasers brought to one photon-level. There should be at least one weak laser source. If more than one such sources are there, they should be indistinguishable leaving the degrees of freedom. Attacks such

as PNS A A Gaidash (2016) should be accounted for privacy. In PNS attack the adversary performs quantum non-demolition measurement (QND) on every message from sender to receiver. In this technique the number of photons is known without disturbing the quantum states. When number of photons is more than one. They may be divided in a ratio where first half is sent to the receiver and the rest is stored in quantum memory of the adversary. Hence number of photons and intensity should be considered in the privacy amplification process.

2.1.2 One-way Mach-Zehnder

Weak lasers are used as carriers and asynchronous Mach-Zehnder interferometers (AMZIs) are used to encode quantum states. Decoy pulse protocol (Hwang, 2003) is used where the sender adds decoy states in the message. An adversary unknowingly uses PNS attack. The sender is able to detect anomalies by seeing higher decoy states than the accepted percentage. Higher security is obtained for weak lasers at constant intensity. Signal, decoy and vacuum pulses are produced using intensity modulation. Relative probabilities are assigned to these pulses beforehand. Attenuation is done so that the transmitted pulse consists of individual photons.

The receiver uses InGaAs avalanche photodiodes as single photon detectors operated in Geiger-mode. Geiger-mode avalanche photodiodes (GAPDs) are used in the p-n junction reverse biased mode which is operated above breakdown voltage. Photons that go to the depletion area generate recognisable current that is sustained by themselves. Certain meters are able to detect signal that are farce. Operation of GAPD is done in such a manner that sensing is done for small instants of time that are in synchronisation with the incoming signal.(Villela, 2012)

In this setup laser diode, intensity modulator and attenuator form the photon source. Intensity modulator is used for decoy pulse protocol and attenuator for intensity attenuation. AMZI is the encoder. Standard single mode fiber is used as quantum

channel. The receiver has active polarization recovery, active fiber stretcher and AMZI.

2.1.3 Send and return scheme(Mach-Zehnder)

In this scheme circulator, faraday mirror, pulse propagating short and long arms are used. Pulses generated by the source are sent to coupler where they split into two pulses. Pulses propagate through short and long arms with their polarization conditioned to enter the quantum channel. Beam-splitter provides timing signal and protection against trojan attacks. The transmitted pulses are reflected by a Faraday mirror to compensate birefringence and return orthogonally polarized pulses. Attenuator reduces intensity to a suitable weak intensity.

2.1.4 Phase-intensity modulator

SSB (single side-band) system is used. In this system single sideband either upper or lower is used for signal transmission. SSB is used due to efficiency in terms of power and radio spectrum used. A local oscillator is used with two Mach-Zehnder modulators. Optical signals are produced by the sources that are attenuated weak laser diodes. The optical signals have a central peak and two sidebands $\omega \pm \Omega$. Wavelength division multiplexing (WDM) is used at the receiver to separate the signals. A detector (DS) generates electrical signal at the receiver. The probability of a photon in the upper and lower sideband is obtained by sine and cosine squared of the phase difference ϕ_1 and ϕ_2 .

2.1.5 Coherent One-Way protocol

Encoding with respect to time is considered in this protocol. Signals having average number of photons lesser than unity are sent. A couple of signals are used in

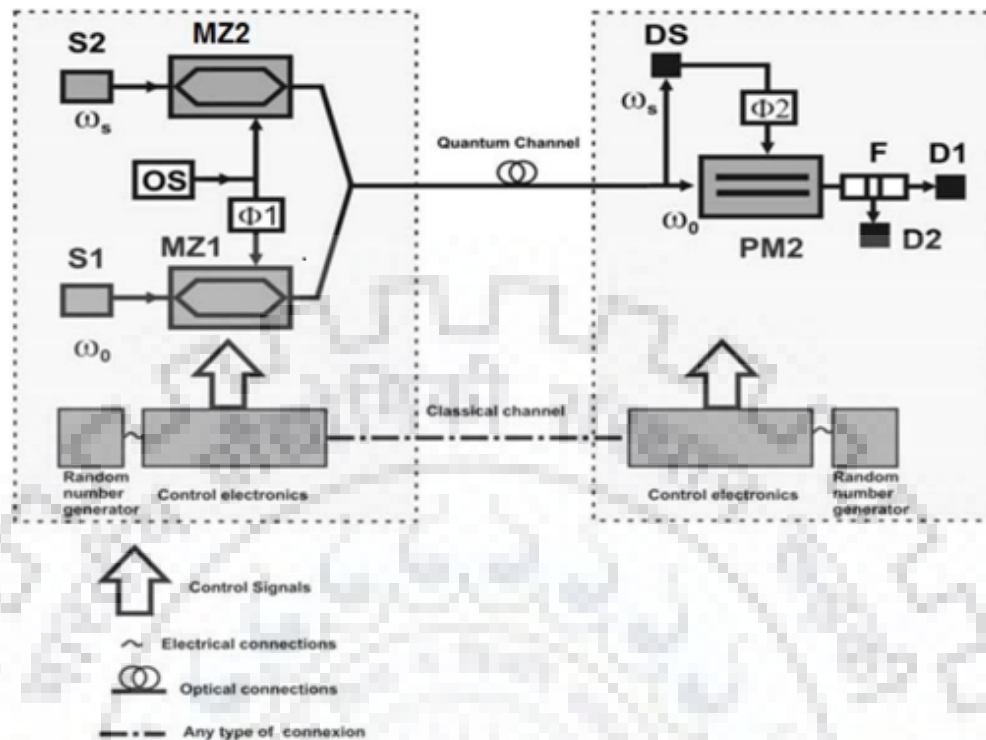


FIGURE 2.1: A one-way, weak-laser-pulse frequency-domain QKD system
 *From ETSI GR QKD 003V2.1.1(2018-03)

progression to send a bit of information. Decoy pulses can also be there. Interferometric devices are used to measure coherency of live signals. A loss of coherence and reduction in visibility reveals the presence of an eavesdropper. Eve's existence can be detected if coherency reduces or the discernibility is reduced. (Damien Stucki, 2007)

2.2 Entanglement based QKD implementations

The source at Alice emits an entangled photon pair, with one photon at 810 nm and the other at 1550 nm. The 810 nm photon is measured in four possible polarisation states (0 45 90nd 135 at Alice, using Si APDs. The 1550 nm photon is sent over the quantum channel (standard telecom fibre) to Bob, where its polarisation is also analysed along the four directions using InGaAs APDs. Several automated control

loops enable continuous operation and movable mirrors ensure that optimal coupling into fibres is maintained. Synchronization pulses multiplexed over the same fibre gate the single-photon detectors at Bob whenever one of Alice's detectors registers an event, and also provide a polarisation reference. By analysing the received polarisation state, dynamical compensation for unwanted polarisation rotation in the optical fibre can be performed.

2.2.1 Continuous-variable QKD

In discrete variable QKD(DV-QKD) photons acted as information carriers. Photon detectors at the receiver side decoded the message to establish secret key between the communicating entities. In continuous-variable QKD(CV-QKD) Gaussian-modulated model was used. There are various benefits of using CV-QKD instead of discrete variant like increasing efficiency, rate increment and optimisation of cost using homodyne detection.(Sanchez, 2007) Homodyne detection extracts information from a signal by comparing it with a signal without any information. In optical case, signals from same sources are compared to see deviations between the signals. In CV-QKD the two conjugate variables used to guarantee security are the real and imaginary parts of the electromagnetic field corresponding to the two quadratures of a coherent state. The transmitter uses continuous or discrete modulation for phase and amplitude of weak coherent signals. The receiver mixes the received electromagnetic signal with a strong signal. Functions are performed on it to get the real and imaginary parts of the wave. Shot noise is due to inherent uncertainty in amplitude and phase of a coherent state. Additional noise exceeding the shot noise can be used to detect intrusion. The real and imaginary parts of the field are defined with respect to a reference. A strong optical signal "Transmitted local oscillator" or weak signal for "Local oscillator" can be used to synchronize the reference.

2.2.2 Transmitted Local Oscillator

In TLO, the transmitter produces a local oscillator state and signal state having well-defined phase reference. The quantum signal is modulated and multiplexed to the local oscillator before sending. To multiplex, a delay line is inserted into one of the two channels. Time multiplexing can also be done. To separate channels without high losses, polarization multiplexing can be used using polarizing beam-splitter. The local oscillator and signal pulse can be sent using two different optical channels. They should be multiplexed in the same propagation channel due to less cost and same disturbances in the channel, which do not affect phase difference. A homodyne detector is put in place at the receiving end where the pulse and local oscillator interfere in a shot-noise limited environment. The result is a pulse where the intensity is a function of the squared value of the signal. Bob randomly selects a quadrature or its 90 degrees difference.

2.2.3 Local Local Oscillator

In LLO, a laser at the transmitter is used to generate the signal, while another laser at the receiver is used to generate the Local Oscillator. The transmitter uses CW (continuous wave)-Laser with IQ modulator. A splitter monitors the average photon flux and a variable optical attenuator (VOA) is used. At the receiver, polarization corrected quantum signal is mixed in the optical hybrid with the CW-laser. Digital signal processing is used to handle the flow of signals. Digital-analogue-converter is used at the transmitter and analogue-digital converter is used at the receiver.

2.3 Single photon detector

This is a device that is sensitive to optical signals. It changes a given photon to a noticeable signal. It has an electrical an optical input and it produces an electrical

output corresponding to the optical signal received. A qubit is detected when the electrical output crosses a given threshold. In systems having many photon detectors, all of them should be having same threshold and other properties for high efficiency. There are various parameters that specify a detector:

1. Detector gate repetition rate
2. Photon detection probability
3. Spectral responsivity
4. Dark count probability
5. After-pulse probability
6. Dead-time
7. Recovery time
8. Partial recovery time
9. Maximum count rate
10. Detector signal jitter
11. Photon number resolution profile

The operating conditions to be specified for a detector are:

1. Detector temperature
2. Environmental requirement
3. Mode of operation
4. Operating wavelength
5. Gating frequency

6. Gate width
7. DC bias
8. AC bias
9. Discrimination level

2.3.1 InGaAs single-photon avalanche photodiodes

InGaAs photodiodes were shown to have reduced dark current (current when no light was irradiated) in (A A Gaidash, 2016). InGaAs single-photon avalanche photodiodes are compact semiconductor devices that provide single-photon sensitivity over the wavelength range from 900 nm to 1700 nm, suitable for use in fibre-optic based QKD. They can be operated in gated or free-running mode. (T.P. Pearsall, 1981)

2.3.2 Superconducting nanowire single-photon detectors

Superconducting nanowire single-photon detectors are a submicron-wide film, which is operated at low temperatures. SNSPDs used at such temperature using liquid Helium or other methods can be used to report single far-infrared photons. (A.D. Semenov, 2001) SNSPDs require the use of liquid helium or a closed-cycle refrigerator, this is in contrast to SPADs that operate at room temperature. Early SNSPDs were made using niobium nitride. Recent experiments with using different materials like tungsten silicide have given much higher efficiency and low dark count. SNSPDs are the most efficient devices for photon detection as of 2018. (Boutin, 2013) SNSPDs are noted for their excellent timing properties, fast switching and natural recovery.

2.3.3 Photon detector for a CV-QKD set-up

2.3.3.1 Coherent detection

There are three steps where first a state is prepared, it is transmitted and then detected at the receiver. Operations such as Gaussian modulation are applied on states before transmission. (Fabian Laudenbach, 2018) These states are sent through quantum channel. Coherent detection is characterised by various features of the signal known before-hand by the receiver. The likelihood of this is given by:

$$\Gamma(x) = \prod_{x=1}^N p(x[n] - s[n]) / \prod_{x=1}^N p(x[n])$$

Where $s[n]$ is a known deterministic signal, p is a known probability density mass function. (Vaswani, 2008)

2.3.3.2 Single-quadrature homodyne detection

Adulterated coherent states are received while transmission for the key takes place. These states contain randomly modulated two quadrature components. Measurement of these states is done by mixing pulse with reference laser which uses homodyne technique with a balanced beam-splitter.

2.3.3.3 Dual-quadrature homodyne detection

When measuring the received signal, if both the quadratures are to be measured simultaneously dual-quadrature homodyne detection is used. Homodyne detection is used on two halves of the signal.

2.3.3.4 Heterodyne detection

The signal is compared with reference from a local oscillator. Heterodyne signifies more than one frequency while homodyne implies one frequency. The comparison between signals is usually done by combining them in photodiode detector. (Optical Heterodyne Detection, 2018)

2.4 QKD Source

Information is sent through light signals which are emitted by a QKD source. The requirement on the source is that data should be sent in such a manner that the receiver can decipher useful information only when measurement and basis while encoding are same. Quantum information can be encoded upon polarisation, phase and angular momentum. An ideal source should emit one photon on trigger. However, in practice single-photon sources have a single-photon efficiency less than one and a finite probability of generating one or more photons.

2.4.1 Parameters to specify a photon source

1. Optical pulse repetition rate
2. Photon number probability distribution
3. Mean photon number
4. Mean source optical power
5. Long-term power stability
6. Short-term power stability
7. Number of emitters

8. Second order correlation function
9. Wavelength spectral frequency
10. Spectral linewidth
11. Emission temporal profile
12. Timing jitter
13. Temporal profile
14. Spectral indistinguishability
15. Temporal indistinguishability
16. Emitter temperature
17. Environmental requirement
18. Mode of operation

2.4.2 Types of sources

1. True single-photon sources
2. Weak pulses:
 - (a) Weak laser
 - (b) Intensity-modulated weak laser
 - (c) Phase-coherent weak laser
 - (d) Composite weak laser
3. Entangled-photon sources
4. Continuous-variable QKD source

2.5 Modulators

Modulators can manipulate certain degrees of freedom of light by using a controlling signal.

2.5.1 Parameters to specify a modulator

1. Modulated degree of freedom
2. Deviations
3. Rise and fall time
4. Optical robustness
5. Environmental requirements
6. Wavelength range
7. Lifetime

2.6 Single photon source and detector properties for measurement

2.6.1 Single photon Source properties

1. Optical pulse repetition rate
2. Mean photon number
3. Source power
4. Long-term power stability

5. Short term power stability
6. Source emission temporal profile
7. Source timing jitter
8. Source temporal profile
9. Source wavelength
10. Spectral line width

2.6.2 Single photon detector properties

1. Detector gate repetition rate
2. Dark count probability
3. After-pulse probability
4. Photon detection probability
5. Linearity factor
6. Detection efficiency range due to polarization variation of input pulses
7. Dead time
8. Recovery time
9. Low and high partial recovery times
10. Detector signal jitter
11. Photon detection probability profile
12. Spectral responsivity

2.7 Functional security objectives

1. To employ a correct QKD protocol, that allows the user to be sure that two communicating entities generate and share the same secret random binary sequence, and no other related information is available to others.
2. To employ and correctly implement security functions.
3. To prevent unauthorized access to the system
4. To make sure if the system is modified then it should be detectable by the actual players. Unauthorized usage should be prevented that might leak sensitive information.
5. To provide true indications of the operational state of the QKD module.
6. To detect errors in operation and prevent the compromise of sensitive data resulting from these errors.
7. To ensure proper design, distribution and implementation.

2.8 Security requirements

1. Specifying system for QKD
2. Ports & system interface
3. Roles, services and authentication
4. Software security
5. Operational environment
6. Physical security
7. Security against non-invasive attacks

8. Sensitive security parameter management
9. Self-tests
10. Life-cycle assurance

2.9 QKD application interface API specification

- **QKD_OPEN** Reserve an association (`key_handle`) to a set of future keys at both ends of the QKD link through this distributed Key Management Layer and establish a set of parameters that define the expected levels of key service. This function shall return immediately and not block.
- **QKD_CONNECT_NONBLOCK** Verifies that the QKD link is available and the `key_handle` association is synchronized at both ends of the link. This function shall not block and returns immediately indicating that both sides of the link have rendezvoused, or an error has occurred.
- **QKD_CONNECT_BLOCKING** Verifies that the QKD link is available and the `key_handle` association is synchronized at both ends of the link. This function shall block until both sides of the link have rendezvoused, an error is detected, or the specified **TIMEOUT** delay has been exceeded.
- **QKD_CLOSE** This terminates the association established for this `key_handle` and no further keys will be allocated for this `key_handle`. Due to timing differences at the other end of the link, the peer operation will happen at some other time and any unused keys shall be held until that occurs and then be discarded.
- **QKD_GET_KEY** Obtain the required amount of key material requested for this `key_handle`. Each call shall return the fixed amount of requested key or an error message indicating why it failed. This function may be called as often

as desired, but the key manager only needs to respond at the bit rate requested through the QOS parameters, or at the best rate the system can manage. The key manager is responsible for reserving and synchronizing the keys at the two ends of the QKD link through communication with its peer. This function may be blocking (wait for the key or an error) or non-blocking and always return with the status parameter indicating success or failure, depending on the request made via the QKD_OPEN function. The TIMEOUT value for this function is specified in the QKD_OPEN() function. (Christopher J Chunnillal, 2018)



Chapter 3

Current Technology

3.1 Quantum computer using microwave ion trapping technique

A big quantum computer can be made using modular approach. Radiation quantum gates of deep wavelengths can be used for trapped ion-based scalable quantum computer architecture. The modules are made from silicon micro-fabrication techniques and are independent from each other. As for the communication between modules ion transport is used.

Trapped ions are a good choice for quantum computer since they are robust, preparing state and readout is of good fidelity, high-fidelity universal gate operations and qubit time for coherence is large. Universal quantum computer can be built on single and multi-qubit gates. Qubits in trapped-ion computing are the states that are inside atomic ions. Modules are X-junction arrays having different zones. Gate, state readout and loading are the three zones. Braiding operations are used to work with one and multiple qubit gates. (Austin G. Fowler and Cleland, 2012) In implementation, qubits are arranged in a fashion in which path transcends from one measure qubit to a logical qubit and back. (Bjoern Lekitsch, 2017)

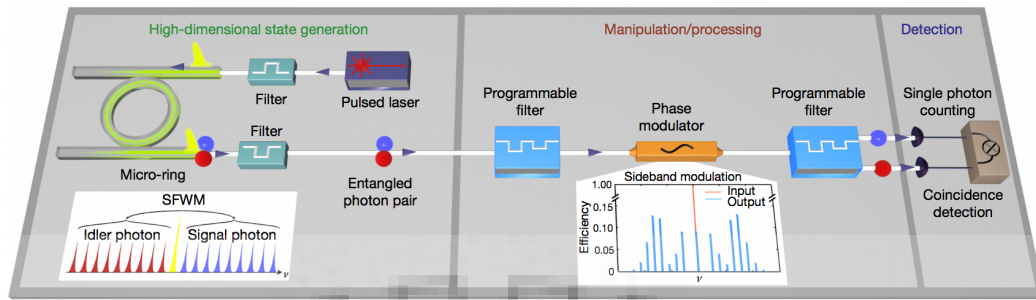


FIGURE 3.1: Spontaneous four wave mixing setup used to generate entangled qudits

*From <https://spectrum.ieee.org/tech-talk/computing/hardware/qudits-the-real-future-of-quantum-computing>

3.2 Generating entangled qudits

Till now quantum computing was being undertaken using qubits. Qubits adopt two possible states. Reserchers have now reported making a microchip that can make qudit having ten or more states. Classical computers use bits which can be in on or off state. On the other hand, a quantum bit can be in a superposition of two states. If qubits are entangled four calculations can be done using them at once. Theoretically, a quantum computer having two 32-qudit states can perform same number of operations as a quantum computer having ten qubits. Scientists at the National Institute of Scientific Research, Varennes, Quebec have reported that a chip has been developed that can make two entangled 10-states qudits having hundred dimensions. In a photonic chip, pulses of light were shot in a muti-ring resonator. This emits entangled pair of photons, each of which is a superposition of 10 wavelengths. These entangled photons were sent through a channel 24.2 kilometre long, for which entanglement was preserved. (Qudits: The Real Future of Quantum Computing?, 2017)

3.3 Observation of three-photon bound states

In comparison to nuclei, molecules and atoms, photons bind only lightly. Three-photon bound states have been recently observed using atomic Rydberg states. (Sibalic and Adams, 2018) Different characteristics of phase and unique bunches were seen. The wave-functions of trimers and dimers persist and show different shapes depending on the photon numbers. Non-linear phase in optics and formation of bunches are explained using photon interactions of Rydberg type and effective field. Photons when bounded form dimers. Non-linear effects of dispersive nature are nullified by packets like wave, called solitons. The body of classical solitons changes with sum of pulse energy. Solitons of quantum type have body that changes with quantity of photons. Ultra-cold atomic gas is used as a quantum non-linear medium for the experiment. Photons are coupled to excited Rydberg states using electromagnetically induced transparency. Strong interactions take place between atoms when they are within a Rydberg blockade radius. Correlation and phase of photons are observed to check the manner in which they interact. The dispersive and distance-dependent photon-photon interactions show up in a large conditional phase shift. The state of three bounded photons can be seen as solitons of photonic nature with respect to QKD. (Qi-Yu Liang, 2017)

3.4 Silicon based two-spin qubit processor

Silicon chips have been used to make electronic devices since the past century. When it comes to making quantum devices, manufacturers and researchers are looking at other materials. This might change with promising results due to research fueled by the chip-maker Intel. There are various benefits of using silicon to make quantum devices. Silicon based manufacturing is pervasive and a huge infrastructure is already in place. Methods are now in place to generate qubits using silicon chips. Silicon-based approaches have proved to be less popular than those using super cooled

aluminium and others. This can be attributed to the fact that qubits generated using silicon chips are difficult to control.

Spin qubits have been reportedly generated by Intel. Signals generated from microwaves are used in conjunction with electrons to check the silicon devices. This is further used to create qubits. (Old-fashioned silicon might be the key to building ubiquitous quantum computers, 2018) Research teams at Delft University of Technology and the University of Wisconsin-Madison were able to run algorithms on spin qubits. These algorithms are usually used to test the effectiveness of quantum machines. (T. F. Watson, 2018)

3.5 Integrated photonic platform for quantum information with continuous variables

Quantum computation, sensing and communication can be done with ease using integrated photonics. Quantum states are generated by confining light in miniaturised waveguide circuits. This combined with waveguide networks and integrated detectors establishes stability and scalability of this technology. Discrete variables are usually used to encode optical quantum information. This helps in near-unity gate fidelity. Quantum gates and sources using current technology are not feasible for using discrete variable approach. Information can be encoded using continuous variable operators, at the cost of fidelity but deterministic two-photon gates. Hence a mixture of continuous variable and discrete variable can be used as a practical implementation. Non-linear, reconfigurable integrated device can actively manipulate and perform interferometric stage of homodyne detection. Beam splitters, tuned electrooptical shifter for phase and squeezed vacuum sources are used for making this device. Quantum states of light can be generated, manipulated and characterised in a monolithically integrated device. Entanglement of quadrature type and

vacuum is used for reconfiguring in two spatial modes. Reverse photon exchange technique is used to enable low propagation losses.(Francesco Lenzini, 2018)

3.6 Universal quantum gates using spin qubits

When interaction takes place with electron spin following microwave scattering then geometric phase is generated. The geometric phase allows a logical qubit to be gated in a holonomic fashion. In the degenerate subspace of triplet spin qutrit, this is defined as geometric spin qubit. Nitrogenous environment is used where polarised microwave works in magnetic field. Two qubit holonomic gate can be used in such an environment. Universal holonomic gates allow fast and fault-tolerant manipulation. These gates can be used in repeaters , computers and communication. Polarised microwaves serve as Pauli operators that are non-commutable basis operators,satisfying the universality of single-qubit holonomic gates. This also allows geometric nuclear spin holonomic gate, which is not possible by optical gate. Entanglement is achieved between electron and nuclear geometric spin using a two qubit holonomic gate. (Kodai Nagata, 2018)

3.7 High-speed quantum networking by ship

Communication forms an essential aspect of quantum networking. Direct transmission of quantum signals is not reliable. This motivates the development of quantum repeaters. Quantum repeaters error-corrected and with high bandwidth needs novel innovation. Local networks can be formed using quantum memories on ships. This will enable low latency, high bandwidth transmission of quantum bits throughout the globe. This approach requires quantum memories with effective coherence time in months. This should be sufficient to transport qubits through traditional shipping

lines. This would also require a container on the ship with facilities such as super-cooling, stable power source, ultra high vacuum and classical control infrastructure. Time taken by the unit, T_{mem} , is related to per-error correction cycle failure probability, P_L , and chosen permissible infidelity of the entangled link, $P_{link} = 1 - F$, where F is the link fidelity between memory units and T_{corr} is the total time of memory correction cycle.

$$T_{mem} = \frac{\log(1 - P_{link})T_{corr}}{\log(1 - P_L)}$$

The space to install the required memories is limited by the space available in oceanic ships carrying goods. Seven containers are made to form one pair. Shipping terminal contains two units, three units are made to rotate locations. First, every mobile qubit is entangled using stationary qubit located at origin. One qubit is sent to terminus from point of origin. Logical qubits are entangled with more qubits both at the terminus and origin. (Simon J. Devitt and Meter, 2016)

Chapter 4

Quantum Key Distribution

Quantum key distribution (QKD) is used to establish symmetric key between two communicating entities. QKD can be used wherever key exchanging protocols are currently used like Diffie-Helman key exchange. The advantage of using QKD over other cryptographic key exchange protocols is that the security of QKD lies on quantum mechanical principles like entanglement. The security of regular protocols lies on the intractability of certain mathematical forms. Many cryptographic protocols depend on discrete logarithm problem. Since such problems can be solved in polynomial time on a quantum computer, such protocols provide little security. QKD protocol is based on natural principles and is more secure than current key exchange protocols. Quantum key distribution was first formulated by Charles Bennett and Giles Brassard in 1984. Two entities Alice and Bob are assumed to be communicating in presence of an adversary Eve. Alice sends a sequence of ones and zeros to Bob to establish a secret key. QKD provides provision to detect tampering with key. The bits that may have been tampered are left out and the other bits constitute the secret key. There is a bidirectional classical channel between Alice and Bob. There is a unidirectional quantum channel from Alice to Bob. Alice begins processing by encoding bits with random selection of one of the two bases agreed upon by Bob and herself.

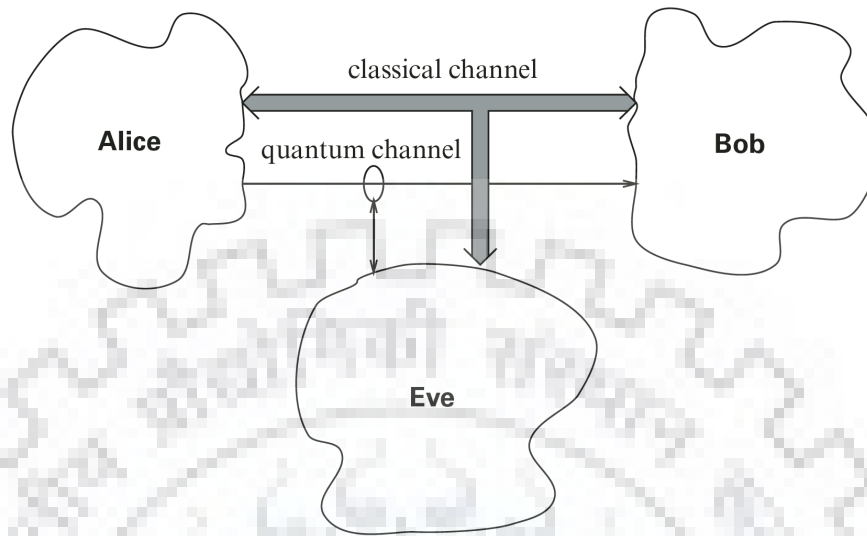


FIGURE 4.1: Quantum Key Exchange

*From Quantum Computing, Eleanor Reiffel and Wolfgang Polak, The MIT Press(2011)

The two basis could be standard basis and Hadamard basis.

In standard basis: $0 \rightarrow |0\rangle$ and $1 \rightarrow |1\rangle$

In Hadamard basis: $0 \rightarrow |\uparrow\rangle$ and $1 \rightarrow |\rightarrow\rangle$

When Bob and Alice use same basis for encoding and decoding, they obtain the same bit. If the choice of basis differs then half the time Bob's value of the bit matches Alice's bit value. After sending all the key bits, Alice sends the choice of basis through public channel. Those bits for which the bases were same are kept for the key. Some bits are also required to ensure no interference by intruder. These bits are discarded as well. When the intruder tries to attack, she has to measure the photon. Measuring the photon has the effect of destroying its value. If she sends it as it is, then she gains no information. The choice of bases is sent through the classical channel. But knowing the bases is not sufficient to decipher the key. Moreover, the bases are exchanged only when the bit transfer has completed. A polaroid would destroy the photon's state. But a calcite crystal can be used by Eve which splits the incoming beam into two beams in perpendicular direction. A photon detector

can detect one of the beams. The other beam is sent to Bob. Since the choice of bases is not yet known, incorrect basis is chosen half of the times. When wrong basis is chosen it changes the polarization of the photon before being sent to Bob. Even with correct choice of basis, Bob will detect the correct bit value only half the time. For each qubit Alice and Bob have, if Eve measured it before sending it to Bob. There is a 25% chance of measuring a different value than Alice sent. This increases the error rate than otherwise possible in Eve's absence. Hence intrusion can be detected.



Chapter 5

Quantum Dialogue

Quantum Secure Direct Communication(QSDC) is a form of communication where two communicating entities can exchange messages over a quantum channel without prior establishment of a private key between them. The channel is set by sending a quantum pair. The receiver receives the first photon. After that the second photon is encoded with one of the four operations I , σ_z , σ_x or σ_{iy} . These correspond to encoding 00, 01, 10 or 11 in the classical sense. The receiver does Bell measurements on the received qubit to decode information. Out of many photons used for communication some randomly chosen photons serve as security checks. This protocol removes the need for key management, brings speed and ensures security. Quantum memory is useful for controlling the transfer of messages effectively. Such a memory is flexible and effective in comparison to a delay line. A hybrid atom photon combination is used as an entangled state, showing memory-memory entanglement. Dense coding is used to retrieve information from transferred photon. AN optically thick array of Rb atoms in a 2D magneto-optical trap is used. Beam displacer and half-wave plates are used to manipulate atomic spin waves. (Zhang W., 2017) Quantum dialogue is a part of QSDC where secret messages can be sent both-ways during communication. In other protocols some bits are lost to adversary due to information leakage resulting due to quantum memory usage. This protocol is resistant to memory attacks and

side-channel attacks. The setup is such that a third party that is not trusted is made to measure the qubits. This external party may act as a malicious user. Four Bell states are used as follows $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$. BB84 is used first and then a version of MDI-QKD is used. In the first part, the sender (Alice) and the receiver (Bob) establish a secret key using BB84. This key will be used throughout the protocol for encoding. Let the agreed-on key be b of n bits. When $b_j = 0, j \in \{1, \dots, n\}$, Alice generates her state in standard basis. Where the standard basis comprises of $|0\rangle$ and $|1\rangle$. When $b_j = 1, j \in \{1, \dots, m\}$, Alice generates her state in Hadamard basis. Where Hadamard basis consists of $|+\rangle$ and $|-\rangle$. $|+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$ and $|-\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$. For randomly chosen a bits out of n bits, encoding is done as follows:

1. When $a_j = 0$ and $b_j = 0$, Alice prepares $|0\rangle$.
2. When $a_j = 1$ and $b_j = 0$, Alice prepares $|1\rangle$.
3. When $a_j = 0$ and $b_j = 1$, Alice prepares $|+\rangle$.
4. When $a_j = 1$ and $b_j = 1$, Alice prepares $|-\rangle$.

The sender sends her qubit to Eve, who is an untrusted third party (UTP). The UTP measures the qubits received from sender and receiver in Bell basis. Alice & Bob decipher information based on the announcement made by Eve.

Seeing from 5.1, when sender sends $|0\rangle$ and the announcement is $|\Phi^+\rangle$ or $|\Phi^-\rangle$, Alice is sure that the state sent by Bob is $|0\rangle$. By this Alice can know for sure that Bob has sent the classical bit 0. When sender generates $|0\rangle$ and the announcement from UTP is $|\Psi^+\rangle$ or $|\Psi^-\rangle$, sender makes out that the bit sent is 1. If sender makes $|+\rangle$ and the outcome of measurement is $|\Phi^+\rangle$ or $|\Psi^+\rangle$, then receiver wants to communicate 0. When Alice prepares $|+\rangle$, and the measurement is $|\Phi^-\rangle$ or $|\Psi^-\rangle$, Bob wants to communicate 1. Similarly, Bob can communicate with Alice. Hence, both entities can exchange information worth two classical bits at once. In

Qubits sent by		Eve's end				Received bits	
Alice	Bob	$ \Phi^+\rangle$	$ \Phi^-\rangle$	$ \Psi^+\rangle$	$ \Psi^-\rangle$	Alice	Bob
$ 0\rangle$	$ 0\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0
$ 0\rangle$	$ 1\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	1
$ 1\rangle$	$ 0\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	1	0
$ 1\rangle$	$ 1\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0	1	1
$ +\rangle$	$ +\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0
$ +\rangle$	$ -\rangle$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	1
$ -\rangle$	$ +\rangle$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	1	0
$ -\rangle$	$ -\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}$	0	1	1

TABLE 5.1: Different cases in transmitting qubits in QD.

the case of $|\Phi^+\rangle$, Eve knows that the bit to be communicated is either 00 or 11. Also, in the case of $|\Psi^-\rangle$ the communicated bit will be either 01 or 10. These measurements leak 1 bit of information to the adversary. Such cases should be avoided and $|\Phi^-\rangle$ and $|\Psi^+\rangle$ should be used. We need to check error that might have crept in due to eavesdropping. Eve has information about the phase of the protocol being undertaken. She might adjust her strategy to obtain secret information. To avoid this, both the entities choose a subset $\frac{\gamma n}{2}$ number of runs among the remaining $\frac{n}{2}$ number of runs. Here γ is a small fraction. For $\frac{\gamma n}{2}$ runs, Alice and Bob reveal their guesses about communicated bits by the communicator and check the noise introduced due to this. The two parties continue if the error is within their agreed limits. (Maitra, 2017)

Chapter 6

Proposed Protocol

6.1 Protocol

This protocol is made up of two segments. First a secret key is established between Alice and Bob using B92 protocol (Bennett, 1992). After that a MDI-QKD is undertaken. In the first part, B92 protocol is used to establish a secret key. This key will be used throughout the protocol for information exchange. There are two phases in this protocol. The first phase uses quantum channel to send photons. The second phase uses the classical channel to make announcements that help in establishing the secret key.(Mohamed Elboukhari, 2010)

1. First Phase over quantum channel

- Alice has a random collection of bits ' A ' $\in \{0, 1\}$ of length ' m '. When $A_i = 0$, Alice encodes her information in the standard basis. When $A_i = 1$, Alice encodes her information in the Hadamard basis. B92 uses only two states. Hence $|0\rangle$ is used when $A_i = 0$ and $|+\rangle$ is used when $A_i = 1$.

- Bob has a random collection of bits 'B' $\in \{0, 1\}$ of length 'm'. When $B_i = 0$, Bob chooses standard basis. When $B_i = 1$, Bob chooses Hadamard basis.
- Bob measures the qubits sent by Alice in one of the bases, depending on the value of B_i .
- Bob stores the result after measurement in a vector 'V'. If the measurement made by Bob equals $|0\rangle$, then $V_i = 0$. If the measurement made by Bob equals $|+\rangle$, then $V_i = 1$.

2. Second Phase over public channel

- A & B, which are the bases chosen by the communicating entities are sent through the public channel.
- Those bits for which the choice of bases are same $\forall, where A_i = B_i$, are kept.

After key has been established, MDI-QKD protocol is started. Four bell states are used as follows $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$. Let the agreed on key be b of n bits. When $b_j = 0, j \in \{1, \dots, n\}$, the sender generates the state to be transmitted in standard basis. Where the standard basis comprises of $|0\rangle$ and $|1\rangle$. When $b_j = 1, j \in \{1, \dots, n\}$, sender generates the state in Hadamard basis. Where Hadamard basis consists of $|+\rangle$ and $|-\rangle$. $|+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$ and $|-\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$. For randomly chosen a bits out of n bits, encoding is done as follows:

1. When $a_j = 0$ and $b_j = 0$, Alice prepares $|0\rangle$.
2. When $a_j = 1$ and $b_j = 0$, Alice prepares $|1\rangle$.
3. When $a_j = 0$ and $b_j = 1$, Alice prepares $|+\rangle$.
4. When $a_j = 1$ and $b_j = 1$, Alice prepares $|-\rangle$.

The sender sends her qubit to Eve, who is an untrusted third party(UTP). The qubits received from the communicating parties are measured by the UTP. Alice and Bob decipher information based on the announcement made by Eve.

Seeing from 5.1, when sender transmits $|0\rangle$ and the announcement is $|\Phi^+\rangle$ or $|\Phi^-\rangle$, Alice is sure that Bob sent $|0\rangle$. By this Alice can know for sure that Bob has communicated the classical bit 0. When sender generates $|0\rangle$ and the announcement from UTP is $|\Psi^+\rangle$ or $|\Psi^-\rangle$, Alice makes out that the bit sent is 1. If sender generates $|+\rangle$ and the outcome is $|\Phi^+\rangle$ or $|\Psi^+\rangle$, then Bob wants to transmit 0. When sender generates $|+\rangle$, and the outcome is $|\Phi^-\rangle$ or $|\Psi^-\rangle$, Bob wants to communicate 1. Similarly, Bob can communicate with Alice. With this, the two legitimate parties exchange two classical bits information at a time.

In the case of $|\Phi^+\rangle$, the adversary has knowledge that the bit sent is either 00 or 11. Also, in the case of $|\Psi^-\rangle$ the communicated bit will be either 01 or 10. The adversary can know about 1 bit of communication by such measurements. Such cases should be avoided and $|\Phi^-\rangle$ and $|\Psi^+\rangle$ should be used.

We need to check error that might have crept in due to eavesdropping. Eve has information about the phase of the protocol being undertaken. She might adjust her strategy to obtain secret information. In order to avoid this, the legitimate parties make a choice of $\frac{\gamma n}{2}$ runs among the remaining $\frac{n}{2}$ number of runs. γ in the above runs is a small fraction. For $\frac{\gamma n}{2}$ runs, the communicating entities show their estimations on the bits sent. Noise added due to this is also taken care of. The protocol is carried on, if the values of error are within the permissible limits. (Maitra, 2017) The setup for quantum dialogue is shown in 6.1. It is worth mentioning that the given protocols can be implemented using current technology. Perfect single photon sources and detectors guarantee the security of QKD due to quantum mechanics. These devices are not yet feasible. Attenuated coherent laser pulses are commonly used. These pulses can be exploited using photon number splitting attack. There are certain techniques like phase randomized weak coherent pulses and application

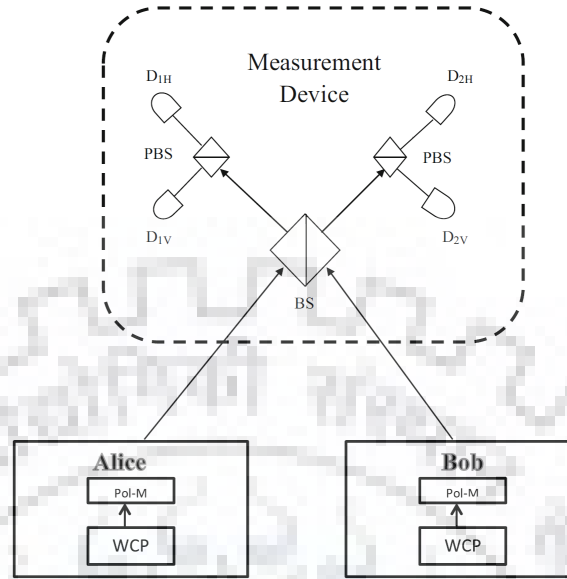


FIGURE 6.1: Schematic diagram of MDI-QKD phase.

*From (Maitra, 2017)

Weak coherent pulses sent by Alice and Bob interfere at 50-50 beam splitter. Each polarizing beam splitter projects incoming photon in vertical or horizontal polarization states. Photon detectors D_{1H} and D_{2V} or D_{1V} and D_{2H} signal a projection in state $|\Psi^-\rangle$. Similar clicks result in $|\Psi^-\rangle$

of decoy state can enhance security of practical implementations. Experimental demonstration of MDI-QKD with active phase randomization over 10km of telecom single-mode fiber with two decoy states has been reported. (Zhiyuan Tang and Lo, 2014)

6.2 Security Proof

The existing QSDC protocol analyse the security of a protocol with respect to certain attacks like photon number splitting attack. In the current protocol the composable security is proven against any arbitrary attack. Entropic uncertainty relations are considered for the same. (Marco Tomamichel, 2013)

Definition 1 Correctness: The key produced by the sender (K_A) should be equal to the one produced at the receiver's end (K_B), even when an adversary is monitoring

the communications.

$$K_A = K_B \quad (6.1)$$

Definition 2 ϵ_{cor} : A protocol is ϵ_{cor} if it is indistinguishable from a correct protocol.

$$Pr[K_A \neq K_B] \leq \epsilon_{cor} \quad (6.2)$$

Definition 3 Δ -secret: A key is called Δ -secret from Eve, if it is Δ_{sec}^{QKD} near to a uniformly distributed key that has no correlation with Eve.

$$\min \frac{1}{2} \{ \rho_{K_A E} - \omega_{K_A} \otimes \rho_E \} \quad (6.3)$$

where $\rho_{K_A E}$ is the correlation between key of sender and adversary, ω_{K_A} is the state that is a mix of K_A and ρ_E is adversary's marginal state.

Definition 4 Secrecy: For any attack by the adversary a protocol is fully secret if, $\Delta_{sec}^{QKD} = 0$ when key is outputted. The key is ϵ_{sec} if it cannot be distinguished from a secret protocol.

Definition 5 Security: If the given protocol is correct & secret, then it is said to be secure. A protocol is ϵ -secure, when it is both ϵ_{cor} and ϵ_{sec}

$$\epsilon_{cor} + \epsilon_{sec} \leq \epsilon \quad (6.4)$$

Definitions 1-4 are the standard definitions with respect to correctness, secrecy and security. Next set of definitions are adapted according to QSDC protocols and is due to (Maitra, 2017).

Definition 6 Correctness: A QSDC protocol is said to be correct if in the presence of Eve, Alice's guess (G_A) is same as Bob's communicated bits (C_B).

$$Pr(G_A = C_B) = Pr(G_B = C_A) = 1 \quad (6.5)$$

Definition 7 ϵ_{cor} – correct: A quantum protocol is ϵ_{cor} if cannot be distinguished from a correct protocol.

$$Pr[G_A \neq C_B] = Pr[G_B \neq C_A] \leq \epsilon_{cor}^{QSDC} \quad (6.6)$$

Definition 8 Δ -secret: A key is called Δ -secret from adversary, when any information derived from the adversary is close to random guess.

$$\min \frac{1}{2} \{ \rho' C_A E - \omega' C_A \otimes \rho' E \} \leq \Delta_{sec}^{QSDC} \quad (6.7)$$

where $\rho' C_A E$ is the correlation between communicated bits of the sender and adversary, $\omega' C_A$ is the state which is a full-mix of C_A and $\rho' E$ is adversary's marginal state.

Definition 9 Secrecy: For any manipulation by the adversary, a protocol is fully secret when, $\Delta_{sec}^{QSDC} = 0$. The protocol is ϵ_{sec} when it cannot be distinguished from a secret one.

Definition 10 Security: If a protocol is correct & secret, then it is secure. A protocol is ϵ -secure, when it is both ϵ_{cor} and ϵ_{sec}

$$\epsilon_{cor}^{QSDC} + \epsilon_{sec}^{QSDC} \leq \epsilon^{QSDC}. \quad (6.8)$$

In the first phase of the protocol the key b is established using B92. Security proof from (Marco Tomamichel, 2013) is used since we have a finite length key. The protocol is ϵ_{sec} -secret is secret length l follows the given condition:

$$l \leq \lfloor m(q - h(Q + \mu)) - Leak_{EC} - \log_2\left(\frac{2}{\epsilon_{cor}}\right) - 2 \log_2\left(\frac{1}{2\epsilon}\right) \rfloor \quad (6.9)$$

, where m represents raw key bits, q shows quality of source for qubits, Q is tolerable QBER, and μ is statistical deviation.

$$\mu = \sqrt{\frac{m+k}{mk} \frac{k+1}{k} \ln \frac{1}{\epsilon_Q}} \quad (6.10)$$

, where k bits are used for checking error and ϵ_Q is an infinitesimal small quantity. $Leak_{EC} + 2 \log\left(\frac{2}{\epsilon_{cor}}\right) + 2 \log_2\left(\frac{1}{2\epsilon}\right)$ is the upper limit on information leakage to the adversary. The truncated binary entropy function is $h(x) = -(1-x)\log(1-x) - x\log(x)$ when $x \leq \frac{1}{2}$ otherwise 1.

The latter part of the protocol's security, dealing with MDI-QKD is now considered. The security of the protocol rests on how secure is b . Suppose that in the first phase sender & receiver successfully establish a ϵ_{sec} key of length n . Let the bit sent by Alice be C_A . Let Bob's guess, after announcement of Bell basis be G_B and guess by Eve be G_E . From (Marco Tomamichel, 2013), if G_B is strongly correlated with C_A in one of the bases standard or Z, then G_E and C_A should not be correlated in Hadamard or X bases. Hence,

$$H(X|G_E) + H(Z|G_B) = -\log_2 c \quad (6.11)$$

, where maximum overlap between the bases is given by c . Considering X and Z bases, $-\log_2 c = 1$. Alice and Bob choose the bases as they have been determined using B92 QKD. Hence, they should be completely correlated. If the key distribution is ϵ_{sec} and from no-cloning principle, information can be gained by the adversary only by the usage of error introduction in the medium.

Say QBER at the standard basis is Q' . Hence, $H(Z|G_B) = H(Q')$. The protocol is symmetric, that is $H(X|G_B) = H(Q')$, the total uncertainty at receiver's end about C_A is $H(C_A|G_B) = 2H(Q')$. If correlation of adversary is nil with C_A , then $H(C_A|G_E) = H(C_A) = 1$. If Eve tries to attack, then she inadvertently introduces disturbance in the medium. This change is reflected as uncertainty by receiver about

C_A . Hence uncertainty of Eve about C_A becomes:

$$\begin{aligned} H(C_A|G_E) &= H(C_A) - H(C_A|G_B) \\ &= 1 - 2H(Q') \end{aligned} \quad (6.12)$$

The mutual information between Alice and Eve is:

$$\begin{aligned} I(C_A; G_E) &= H(C_A) - H(C_A|G_E) \\ &\leq 2H(q' + v). \end{aligned} \quad (6.13)$$

Here v is statistical deviation. The protocol is stopped depending on the error estimation phase. If QBER is within threshold, then

$$\Delta_{sec}^{QSDC} \leq \epsilon_{sec}^{QSDC} \quad (6.14)$$

The protocol is ϵ_{sec} -secure as:

$$\min \frac{1}{2} \{ \rho'_{C_A E} - \omega'_{C_A} \otimes \rho'_{E} \} \leq \Delta_{sec}^{QSDC} \leq \epsilon_{sec}^{QSDC} \quad (6.15)$$

When the announcement is correct, then Bob and Alice are able to predict the bits correctly.

$$Pr(G_A = C_B) = 1 \quad (6.16)$$

Due to noise in the channel:

$$Pr(G_A \neq C_B) \leq (Q' + v) \quad (6.17)$$

To ensure ϵ_{cor} -correctness of the protocol, value of Q' should be restricted by ϵ_{cor}^{QSDC} .

The protocol is ϵ -secure as long as:

$$\epsilon_{sec}^{QSDC} + \epsilon_{cor}^{QSDC} \sim \epsilon^{QSDC} \sim \epsilon^{QKD} \quad (6.18)$$

6.3 Comparison with MDI-QKD

The visible difference in the current protocol with the standard MDI-QKD protocol is the use of B92 instead of BB84 for key establishment. B92 is simpler and cost effective. B92 was developed to simplify BB84 and remove complexity. It is based on one quantum basis states, instead of more basis states in BB84. A bit can be in one of the four states that are non-orthogonal in BB84. On the other hand, B92 uses only two states. Angles and polarisation of photons are used to describe the B92 protocol. For example $|\theta_+\rangle$ can be used to represent 1 and $|\theta_-\rangle$ can be used to represent 0. The photons are linearly polarised at angles θ_+ and θ_- with respect to the vertical where $0 < \theta < \frac{\pi}{4}$. The direction of polarization is used to encode a classical bit. Horizontal polarisation is used to encode 0 and 45 degrees is used for bit 1. To decode the transmission, 1 is assumed when -45 degrees is observed and 0 is assumed when 90 degrees is observed by Bob. (R. Etengu, 2011)

6.3.1 Numerical analysis

Transmission distance and secure communication rate are considered for comparison and measurement. The secure communication rate is given by the following equation due to (Lutkenhaus, 2000).

$$R_{BB84} = \frac{1}{2} v p_{click} [1 - \tau(QBER, \beta) + f(QBER)h(QBER)] \quad (6.19)$$

Here, R_{BB84} is obtained by error correcting and amplification of the secure bits. The total secure communication rate is obtained by multiplying R_{BB84} by the repetition rate of the source. p_{click} is the signal of the system. It is the probability that receiver detects photon in the pulse. $f(QBER)$ depends on the algorithm for correcting errors.

$h(\text{QBER})$ is the conditional binary entropy.

$$p_{\text{click}} = p_{\text{exp}}^{\text{signal}} + p_{\text{exp}}^{\text{dark}} - p_{\text{exp}}^{\text{signal}} p_{\text{exp}}^{\text{dark}} \quad (6.20)$$

Here, $p_{\text{exp}}^{\text{signal}}$ is the probability of detection of photon emitted by Alice by Bob. $p_{\text{exp}}^{\text{dark}}$ is the dark count probability at Bob's end. Each detector at the receiver's end has a dark count probability per time slot sans real signal. The probability of dark count in the detection process is given by : $P_{\text{exp}}^{\text{dark}} = 4d$

Dark count is attributed to the detector properties such as thermal fluctuations. Dark counts are visible only when $P_{\text{exp}}^{\text{signal}}$ is small. The numeral 4 in the above equation is attributed to the use of four detectors in the system. Dark count per measurement window is :

$$d = Dt_w \quad (6.21)$$

Where, D is the detector dark count rate and t_w is the time window.

QKD is usually undertaken through fiber optical links or free space. The current calculations are considering free space. In free space channel, there is more link loss and transmission efficiency becomes important. The total transmission efficiency is given by:

$$\eta_{\text{tot}} = T_{\text{chan}} P_{\text{acq}} \eta_{\text{det}} \quad (6.22)$$

Here, T_{chan} is the quantum channel transmission and P_{acq} is the photon acquisition probability. T_{chan} & T_{acq} , the numbers corresponding to optical coupling and losses during transmission.

Four link scenarios are considered due to effect of turbulence being different for different scenarios. They are point-to-point, ground-to-satellite, satellite-to-ground and satellite-to-satellite. Emitted light covers distance in different environments in different scenarios. In satellite-to-ground link, light has to travel a long distance in vacuum. It is then subjected to turbulence and unpredictable atmosphere. In

ground-to-satellite link beam spreading effect occurs. In satellite-to-satellite link there is complete vacuum and no turbulence occurs.

$$A_{atm}^{GS_S} = \exp(-\alpha L) \quad (6.23)$$

(Isaac I. Kim and Korevaar, 2000) Here, α is the coefficient of light when attenuated after entering the earth's atmosphere.

$$\alpha = \frac{3.91}{v} \left(\frac{5.4545 * 10^{14}}{f} \right)^{-q} \quad (6.24)$$

Here, v is the atmospheric visibility, f is optical transmission frequency, q is the size distribution of scattering particles. $q = 0.585v^{\frac{1}{3}}$

$$A_{atm}^{GS_S L} = T_0^{B_\theta} \quad (6.25)$$

Here, T_0 is transmission through atmosphere at the zenith angle, B_θ is the zenith angle. In satellite-to-satellite link, there is vacuum and no atmosphere. Hence,

$$A_{atm}^{SLSL} = 1 \quad (6.26)$$

Quantum bit error rate(QBER) is useful during error correction and privacy amplification, analysis and simulation of QKD systems. QBER can be defined as the ratio of wrong bit counts to the received but counts. It can be stated as the probability of false detection to the total probability of detection per pulse.

$$QBER = \frac{\frac{1}{2}p_{exp}^{dark} + bp_{exp}^{signal}}{p_{click}} \quad (6.27)$$

Here, b is the base system error rate which is indistinguishable from interference.

On introduction of error QBER on the channel, conditional entropy resulting from a binary symmetrical channel is:

$$h(QBER) = [QBER \log_2 QBER + (1 - QBER) \log_2(1 - QBER)] \quad (6.28)$$

τ is the shrinking factor for amplification of privacy. It is part of the key that needs to be warded off to amplify privacy, considering single-photon pulses. p_c is the average collision probability. It shows adversary's information with the two legitimate parties.

$$\tau = -\log_2 P_c \quad (6.29)$$

$$\tau(QBER, \beta) = -\beta \log_2 \left[\frac{1}{2} + 2 \frac{QBER}{\beta} - 2 \left(\frac{QBER}{\beta} \right)^2 \right] \quad (6.30)$$

β is a part of individual photon states from source. The protocol is secure against PNS attack till β is positive. (Lutkenhaus, 2000)

$$\beta = \frac{P_{click} + P_{mult}}{P_{click}} \quad (6.31)$$

Photon source's quality's assessment is necessary for the system. Statistics and efficiency are analysed for the same. These are compared with weak coherent source having same number of photons per pulse. Considering the security features and assuming adversary has quantum memory that persists for a long time. We have:

$$\tau(QBER, \beta) = \frac{1 + \beta}{2} \log_2 \left[\frac{1}{2} + 4 \frac{QBER}{1 + \beta} - 8 \left(\frac{QBER}{\beta} \right)^2 \right] \quad (6.32)$$

In the B92 protocol Bob tells Alice about the detected events without divulging the measurement basis, on the classical channel. Alice generates sifted key using this information. When the bits selected by Alice and Bob are same, Bob measures a photon with half probability. Hence, only 25% bits are detected by receiver. There are more hindrances to detection due to chance of signal being lesser than 1. Thus, the transmission efficiency in B92 is 25% in absence of losses and imperfections. The

Distance(km)	R_{sift}^{B92}	R_{sift}^{B84}	R^{B92}	R^{B84}
100	306.6810 ³	613.3510 ³	70.08010 ³	280.3210 ³
300	54.18410 ³	108.3710 ³	12.38210 ³	49.52710 ³
500	20.48710 ³	40.97410 ³	4.68110 ³	18.72610 ³
700	10.59410 ³	21.18710 ³	2.420810 ³	9.683110 ³
1100	4.326710 ³	8.653010 ³	0.988710 ³	3.954710 ³

TABLE 6.1: Statistics for BB84 and B92 variants for different altitudes at 60 degrees zenith angle for GS link

secure communication rate of B92 protocol considering PNS and intercept-resend attacks is:

$$R_{B92} = \frac{1}{4} v p_{click} [1 - \tau(QBER, \beta) + f(QBER)h(QBER)] \quad (6.33)$$

6.3.2 Results

Using the equations mentioned in the previous sections, along with using wavelengths in 600-900 nm range QBER is calculated. For 800nm operating wavelength, $\mu = 0.1$ for a static distance of transmission, BB84 gives QBER = 2%, B92 gives QBER = 3.5%. These values are well within the permissible range of error of 15. QBER values can increase with losses due to channel. BB84 is more stable than B92 protocol with respect to channel losses.

Communication bit rate performance is another factor that is important for the quality of a QKD system. Bit rate is generally enhanced and sifted to form secure communication bit rate. The final secure bit rate is a measure of the average number of photons per pulse, μ . $\mu = 0.1$ is the optimised value for single photon based systems. In Poisson distribution of photons, multiple photons are generated and transmitted. In such an environment μ should be kept as low as $\mu \leq 1$. From 6.1 for signals at angle of zenith, 60 degrees, the communication bit rates range from 989Hz to 280 kHz. It is also observed that values obtained for B92 protocol is nearly half to that of BB84. (R. Etengu, 2011)

Chapter 7

Conclusion

The proposed MDI-QKD protocol uses B92 instead of BB84 for key exchange. B92 uses lesser number of states and is more economical. The QBER obtained for B92 is 3.5% which well below the permissible limit of 15%. This makes B92 a good candidate for key exchange. It is advantageous as it is easy to implement. But BB84 is more stable considering channel loss and provides high secure communication bit rate.

7.1 Future scope

The current protocol can be used along with symmetric cipher. Since the number of qubits are limited as per the current technology, if quantum dialogue is run for T times, considering T to be of a long duration. If we consider M-bits security against Eve where $t \gg 2M$. Symmetric cipher is better suited to reduce the number of qubits used. If we require 128 bits security, we need to repeat QD for 512 times. For this we need to generate 2048 bits stream using B92 protocol. This is true because bits corresponding to $|\phi^+\rangle$ and $|\psi^-\rangle$ are discarded. Error guessing would further

consume half the bits. So, in the key distribution process we require 8192 qubits. This is four times the key bits.(Maitra, 2017)

If only highly sensitive keys are constructed using B92 and symmetric cipher be used for other keys or cycles of key generation, then useful resources can be saved. Current QKD schemes are universally composable(UC).(Canetti, 2018) This implies that QKD can be used along with any other protocol which is also UC.



Bibliography

- A A Gaidash, V I Egorov, A. V. G. (2016). Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. *Journal Of Physics*.
- A.D. Semenov, G.N. Gol'tsman, A. K. (2001). Quantum detection by current carrying superconducting film. *Physics*, C 351.
- Austin G. Fowler, Matteo Mariantoni, J. M. M. and Cleland, A. N. (2012). Surface codes: Towards practical large-scale quantum computation. *Physical Review*.
- Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*.
- Bjoern Lekitsch, Sebastian Weidt, A. G. F. K. M. S. J. D. C. W. W. K. H. (2017). Blueprint for a microwave trapped ion quantum computer. *Science Advances*.
- Boutin, C. (2013).
- Canetti, R. (2018). Universally composable security: a new paradigm for cryptographic protocols. *IACR*.
- Charles H. Bennett, G. B. (1984). Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems and Signal Processing*, volume 1, pages 1–427.
- Christopher J Chunnillall, Romain Alléaume, H. B. I. P. D. C.-H. F. F. M. G. H. H. B. H. M. L. M. P. A. P. J.-K. K. R. A. G. S. K. T. M. W. Z. L. Y. (2018).

Quantum key distribution : Components and internal interfaces. Technical report, National Physical Laboratory, Institut Mines Telecom, Huawei Technologies, Istituto Nazionale di Ricerca Metrologica, Austrian Institute Of Technology, ID Quantuze SA, Toshiba Research, Qunion, Nippon Telegraph and Telephone Corporation.

Damien Stucki, Sylvain Fasel, N. G. Y. T. H. Z. (2007). Coherent one-way quantum key distribution. *Universite de Geneve*.

Fabian Laudenbach, Christoph Pacher, C.-H. F. F. A. P. M. P. B. S. M. H. P. W. H. H. (2018). Continuous-variable quantum key distribution with gaussian modulation- the theory of practical implementation. *Adv. Quantum Technol.*, srXiv: 1703.09278v3[quant-ph].

Feynman, R. P. (1981). Simulating physics with computers. *International Journal of Theoretical Physics*.

Francesco Lenzi, Jiri Janousek, O. T. M. V. B. H. S. K. L. C. H.-P. P. D. V. D. H. Y. P. K. L. E. H. H. M. L. (2018). Integrated photonic platform for quantum information with continuous variables. *Science Advances*.

Hwang, W.-Y. (2003). Quantum key distribution with high loss. *Department of Electrical and Computer Engineering*.

Isaac I. Kim, B. M. and Korevaar, E. J. (2000). Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications. In *Proceedina of SPIE*, volume 4214, Boston,MA, United States.

Kodai Nagata, Kouyou Kuramitani, Y. S. H. K. (2018). Universal holonomic quantum gates over geometric spin qubits with polarised microwaves. *Nature Communications*.

Lutkenhaus, N. (2000). Security against individual attacks for realistic quantum key distribution. *Physical Review*.

- Maitra, A. (2017). Measurement device independent-quantum dialogue. *Quantum Information Processing*, DOI 10.1007/s11128-017-1757-x.
- Marco Tomamichel, a. E. H. (2013). The link between entropic uncertainty and nonlocality. *Journal Of Physics*.
- Mohamed Elboukhari, Mostafa Azizi, A. A. (2010). Quantum key distribution protocols : A survey. *International Journal of Universal Sciences*.
- Old-fashioned silicon might be the key to building ubiquitous quantum computers (2018). Old-fashioned silicon might be the key to building ubiquitous quantum computers.
- Optical Heterodyne Detection (2018). Optical heterodyne detection.
- Qi-Yu Liang, Aditya V. Venkatramani, S. H. C. T. L. N. M. J. G.-A. V. G. J. D. T. C. C. M. D. L. V. V. (2017). Observation of three-photon bound states in a quantum nonlinear medium. *Science*.
- Qudits: The Real Future of Quantum Computing? (2017). Qudits: The real future of quantum computing?
- R. Etengu, F. M. Abbou, H. Y. W. A. A. N. N. A. S. (2011). Performance comparison of bb84 and b92 satellite-based free space quantum optical communication systems in the presence of channel effects. *Journal Of Optical Communications*.
- Sanchez, R. G.-P. (2007). *Quantum information with optical continuous variables from Bell tests to key distribution*. PhD thesis, Université libre de Bruxells.
- Sibalic, N. and Adams, C. S. (2018). Rydberg physics. *IOP Science*.
- Simon J. Devitt, Andrew D. Greentree, A. M. S. and Meter, R. V. (2016). High-speed quantum networking by ship. *Scientific Reports*.
- Simonite, T. (2016). Intel puts the brakes on more's law.

- T. F. Watson, S. G. J. Philips, E. K. D. R. W. P. S. M. V. D. E. S. M. G. L. M. F. S. N. C. M. A. E. . L. M. K. V. (2018). A programmable two-qubit quantum processor in silicon. *Nature*.
- T.P. Pearsall, M. Piskorski, A. B. J. C. (1981). A $Ga_{0.47}In_{0.53}As/InP$ heterophotodiode with reduced dark current. *IEEE Journal of Quantum Electronics*, QE-17.
- Vaswani, N. (2008). Coherent detection.
- Villela, E. (2012). Gated geiger mode avalanche photodiode pixels with integrated readout electronics for low noise photon detection. *Nuclear Instruments and Methods in Physics Research A* 695(2012), pages 218–221.
- Zhang W., Ding D.S., S. Y. Z. L. S. B. G. G. (2017). Quantum secure direct communication with quantum memory. *Physical Review Letters*.
- Zhiyuan Tang, Zhongfa Liao, F. X. B. Q. L. Q. and Lo, H.-K. (2014). Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical Review Letters*.