



Security of Quantum Key Distribution and Quantum State Sharing

by

Comfort Sekga

Reg.no 14102079

BSc (Radiation and Health Physics) (University of Botswana)

Department of Physics and Astronomy,

College of Sciences,

Botswana International University of Science and Technology

duxecekga@gmail.com, +267 76 057 523

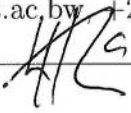
A Thesis Submitted to the College of Sciences in Partial Fulfilment of the Requirements for the Award of the Degree of Master of Science in Physics of BIUST

Supervisor: Dr Mhlambululi Mafu

Department of Physics and Astronomy,

College of Sciences, BIUST

mafum@biust.ac.bw +267 4900117

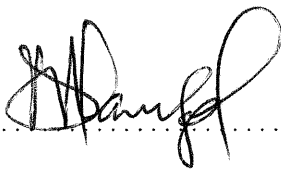
Signature:  Date 15/01/2018

November, 2017

Declaration and Copyright

I, Comfort Sekga, declare that this thesis is my own original work and that it has not been presented and will not be presented to any other university for a similar or any other degree award.

Signature



This thesis is copyright material protected under the Berne Convention, the Copyright Act of 1999 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for researcher private study, critical scholarly review or discourse with an acknowledgement, without the written permission of the office of the Provost, on behalf of both the author and the BIUST.

Certification by Supervisor

The undersigned certifies that he has read and hereby recommends for acceptance by the College of Sciences a thesis titled: Security of Quantum Key Distribution and Quantum State Sharing, in fulfilment of the requirements for the degree of Master of Science in Physics of the BIUST.



.....

Dr. M. Mafu
(Supervisor)

Date: 15/01/2018

Acknowledgements

First and foremost, I wish to express my sincerest gratitude to my thesis supervisor Dr Mafu for guiding me and providing me with valuable insights and advices at all stages of the research project. It was great pleasure to have collaborated with him during the last two years.

I would like to thank my fellow colleagues in Department of Physics and Astronomy: Charles Moditswe, Keadiretse Lefatshe, Ndakidzilo Nthoiwa, Tiro Lebane, Pako Phumaphi, Brantony Mozola, Edigar Muchuweni, Huggins Nyakotyo and Adolf Motetshwane for the stimulating discussions, their guidance, encouragement and many valuable advices.

I acknowledge BIUST for offering me financial support and its facilities to carry out my research project.

Last of all, I am greatly indebted to my family. Thanks to my mother, for giving me life in the first place, for educating me, for unconditional support and encouragement to pursue my interests. All the glory to my Lord God.

Contents

Declaration and Copyright	i
Certification by Supervisor	ii
Acknowledgements	iii
Table of contents	vi
List of tables	viii
List of figures	x
Abstract	xii
1 Introduction	1
1.1 Cryptosystems	2
1.1.1 Classical Cryptosystems	2
1.1.2 Quantum Cryptography	3
1.2 Secret Sharing	4
1.3 Motivation	4
1.4 Outline of the Thesis	5
2 Information Theory	7
2.1 Classical Information Theory	7
2.1.1 Entropy of Random Variables	7
2.1.2 Joint Entropy	8
2.1.3 Conditional Entropy	8
2.1.4 Mutual Information	9
2.1.5 Shannon's Noisy Channel Coding Theorem	9
2.2 Quantum Information Theory	10

2.2.1	Qubit	10
2.2.2	Linear Operators	12
2.2.3	Density Operators	13
2.2.4	Unitary Transformations	14
2.2.5	Quantum Measurements	14
2.2.6	Composite Systems and Entanglement	16
2.2.7	Quantum Information Measures	18
3	Quantum Cryptography	22
3.1	QKD Schemes	22
3.1.1	Prepare and Measure (P& M) Schemes	22
3.1.2	Entanglement Based (EB) Schemes	25
3.1.3	Decoy State QKD	27
3.1.4	Distributed Phase Reference Protocols	27
3.2	Key Distillation Process	29
3.2.1	Error Correction	29
3.2.2	Privacy Amplification	29
3.3	Implementation of QKD	30
3.3.1	Single Photon Sources	30
3.3.2	Quantum Channels	31
3.3.3	Detectors	32
3.4	Security of QKD	33
3.4.1	Eavesdropping Strategies	35
3.4.2	Collective Attacks	39
3.4.3	Joint Attacks	39
3.4.4	QKD attacks	40
3.5	Security Proofs of QKD Schemes	41
3.6	Approaches to Security Proofs	42
3.6.1	Twisted Pair Approach	42
3.6.2	Complimentary Principle	43
3.6.3	Entanglement Distillation	43
3.7	Composability of the Key	43
4	Secret Sharing	45
4.1	Classical Secret Sharing	46
4.1.1	Shamir (k, n) Threshold Scheme	46
4.1.2	Blakley Scheme	48

4.1.3	Proactive Secret Sharing (PSS)	48
4.1.4	Verifiable Secret Sharing (VSS)	49
4.1.5	Applications of Secret Sharing	50
4.2	Quantum Secret Sharing	51
4.2.1	Applications of QSTS	51
5	Reference Frame Independent QKD Protocol	53
5.1	Reference Frame Independent Protocol	53
5.1.1	Operation of the Protocol	54
5.1.2	Security Analysis	55
6	Security Proof of a Generic Three Party QKD Protocol	63
6.1	Operation of the Protocol	63
6.2	Security Analysis	63
7	Multiparty QSTS of an Arbitrary Unknown Three Particle State with GHZ State Measurements	70
7.1	Five Party QSTS of an Arbitrary Three Particle Unknown State using GHZ States	70
7.2	The Generalized Scheme for Multi-Party QSTS of an Arbitrary Three Particle State with GHZ States Measurements	75
7.3	QSTS of an Arbitrary m -Particle State with n Agents	76
8	QSTS of an Arbitrary 3-Particle State using Einstein-Podolsky-Rosen Pairs and GHZ State Measurements	79
8.1	Operation of the Scheme	79
8.2	QSTS of an Arbitrary 3 Particle State to N Agents	82
9	Conclusion	91
	Bibliography	92
	Appendix	103

List of Tables

3.1	A BB84 Protocol Implementation	23
7.1	The comparison between our scheme and the other previous schemes for sharing three particle state and two particle state with five parties. QR-quantum resources, NO-necessary operations, CR-Classical resources, GHZM-GHZ state joint measurement, BM-Bell state measurement, SM- single particle measurement, Single particle unitary operation, η_t -total efficiency	77
8.1	The comparison between our scheme and the other previous schemes for sharing three particle state and two particle state. QR-quantum resources, NO-necessary operations, CR-Classical resources, GHZM-GHZ state joint measurement, BM-Bell state measurement, SM- single particle measurement, Single particle unitary operation, η_t -total efficiency	82
8.2	The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2}, V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2, yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}, P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.	87
8.3	The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2}, V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2, yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}, P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.	88
8.4	The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2}, V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2, yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}, P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.	89

8.5	The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2} , V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2$, $yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}$, $P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.	90
-----	--	----

List of Figures

2.1	The bloch sphere visualisation of a single qubit	11
3.1	Poincare sphere representation of Ekert's protocol	25
3.2	Homodyne detection scheme showing the high intensity local oscillator and the signal beam passing through a beamsplitter. Photodiodes make up the proportional detectors which produces photoelectrons. The difference in current is shown in the display and provide us with quantum information about the signal state [1].	33
4.1	Shamir $(4, n)$ threshold secret sharing scheme. (a) Four player can collaborate to recover the original third degree polynomial $P(x)$. (b) Three players can get infinitely many solutions of the polynomial hence cannot retrieve the secret [2].	47
4.2	Blakley's scheme in three dimensions: each share is a plane, and the secret is the point at which three shares intersect. Two shares are insufficient to determine the secret, although they do provide enough information to narrow it down to the line where both planes intersect [3].	48
5.1	Comparison between the secret key rate of the BB84 protocol [48], 2-party rfi protocol [23] and our proposed 3-party rfi protocol.	61
7.1	The steps for the proposed five party QSTS of unknown three particle quantum state. In 1 Alice starts by sharing 4 GHZ states with Bob1, Bob2, Bob3 and Bob4 and then performs a Controlled Not gate operation (CNOT) on particles $(y, 11), (z, 10)$. In 2 Alice then carries out GHZ state measurement (GHZM) on particles $(x, 1, 2), (y, 4, 5)$ and $(z, 7, 8)$. In 3 Alice executes single particle measurements(SM) on particle 10 and 11. In 4 Bob4 perform single particle measurement(SM) on particle 12. Finally, in 5 Bob1, Bob2 and Bob3 perform unitary operations $(U_1, U_2$ and $U_3)$ on their particles.	72

7.2	The principles of our QSTS scheme of an arbitrary m -particle state. Alice perform m GHZ state measurements (GHZM) and $2(n - m)$ single particle measurements (SM). Controllers carries out $(n - m)$ single particle measurements and other agents performs single particle unitary operations (SUOs) to recover the unknown state.	76
8.1	QSTS of arbitrary three-particle quantum state with two parties. Alice starts by sharing two EPR pairs with Bob1 and Bob2. Alice then carries out GHZ state measurement (M_1, M_2 and M_3) on particles $(x, a_1, a_2), (y, c_1, c_2)$ and (z, e_1, e_2) . Bob1 executes product measurement (M_{B1}) on his particles and Bob2 performs unitary operations (U_{B2}) on his particles	81

Abstract

Quantum key distribution (QKD) and quantum secret sharing play a pivotal role in securing confidential information. QKD allows legitimate parties to create a cryptographic key which they can use to communicate privately without being intercepted by a malicious eavesdropper. QKD exploits the laws of quantum mechanics such as the Heisenberg uncertainty principle, the no cloning theorem and the principle of entanglement to detect any eavesdropper who tries to gain the knowledge of the secret key. Another method of securing confidential information is quantum secret sharing (QSS). QSS is a cryptographic protocol aimed at distributing secret information to untrusted agents. In this method, a secret can be distributed to agents in a way that some subsets of agents can collaborate to fully recover the secret key or message while all other subsets have insufficient information to enable them to reconstruct the key or message even if in possession of unlimited computing power.

The objective of this thesis is to review various security proof methods and to propose security proofs for two QKD protocols. In the first protocol, a key is generated by using Greenberger-Horne-Zeilinger (GHZ) states in an environment of unknown and slowly varying reference frame. We also compute the secret key rate for this protocol. In the second protocol, a second security proof is derived for QKD protocol in which Eve's information is conditioned on a random variable which describes all projective measurements performed by communicating parties.

Furthermore, we propose two quantum state sharing (QSTS) schemes which uses GHZ states and Einstein-Podolsky-Rosen (EPR) states to share an unknown three-particle state to n agents. Firstly, we introduce the five party QSTS of an arbitrary three particle unknown state where Alice starts by sharing four GHZ entangled states with her four agents and performs three GHZ state measurements on her particles followed by two single particle measurements on the Hadamard basis. One of the agents, Bob1, performs single measurements on her particle and the three other agents perform unitary transformations on their particles to recover the unknown state. Subsequently, we propose the generalised multi-party QSTS of an arbitrary three particle state. Secondly, we present a scheme in which Alice shares an arbitrary three-particle unknown state with Bob1 and Bob2. Alice starts by

sharing six EPR pairs with her agents and then performs joint three-particle GHZ state measurements on her particles. Bob1, who acts as controller performs a product measurement $\sigma_x \otimes \sigma_x \otimes \sigma_x$ whilst Bob2 retrieves the original state by performing three unitary operations on his particles. Thereafter, we propose the generalised multi-party QSTS of an arbitrary three particle state.

Chapter 1

Introduction

Information has been crucial since the ancient times where it was used for military purposes and can be considered as old as the communication itself. For example, it has been of great importance in diplomatic, military, health and financial applications [4]. In this era of fast technological advances in telecommunications large amounts of information is being shared across the Internet. For instance, sensitive data such as bank accounts and personnel records, from people at all social levels are transmitted daily. Thus, there is a need for protection of vital and confidential information. In this regard, new cryptographic and secret sharing techniques have been proposed.

Cryptography is the art of protecting information from unauthorised access. The main focus of cryptography is for a sender and an intended recipient to be able to communicate in a form that is unintelligible to third parties, and for the authentication of messages to prove that they were not tampered with in transit. This can be achieved with provable security if the communicating parties possess a shared, secret key [5]. In a cryptosystem, the sender (known conventionally as Alice) starts by encoding the message P in such a way that it is unintelligible to any third party, i.e., she generates the cryptogram,

$$C = E_K(P) ,$$

where E is the encryption algorithm and sends it to recipient (known as Bob) who decrypts it by applying a key to the cipher,

$$P = E_K^{-1}(C),$$

recovering the plaintext P [6]. The transmission of the cryptogram takes place in the presence of an eavesdropper (Eve) who clearly must not be able to acquire the key, K , or she will be able to read Alice and Bob's messages. This can be achieved through quantum key distribution which allows two parties connected by a quantum channel to establish a secret

key that is unknown to any unauthorized third party. In general, the encryption algorithm, E , by which a plaintext message, P , is converted into a cryptogram, C , can be publicly known, because in any particular communication it depends on a parameter, known as a key, K , which is a secret shared only by the sender and intended recipient. Indeed, a second important assumption of cryptography, known as Kirchhoff's rule, is that the secrecy must lie entirely in the key and not the algorithm [7].

Information can also be protected through secret sharing. Secret sharing is a useful procedure of information processing which involves the splitting and distribution of message to a group of agents [2]. The split message is sent to untrusted agents who have to collaborate to recover the message. However, only a certain subset of agents can recover the message whilst other participants cannot get the information about it.

1.1 Cryptosystems

1.1.1 Classical Cryptosystems

Classical cryptosystems have been traditionally used for encryption of messages. It is composed schematically by two systems; symmetric encryption and asymmetric encryption. Below we give a description of each system.

Symmetric Encryption

The system uses the one key to encrypt and decrypt the messages and the key is preserved secret by the communicating parties. For instance, if there are n communicating parties, $n(n-1)/2$ distinct keys have to be created and distributed. One example of symmetric cryptosystem is the one time pad or the Vernam cipher [8]. Two legitimate users are assumed to share a long random bit string as a key, which is as long as the message. This key is not known to anyone else. At Alice's (a legitimate sender) side, a ciphertext is generated by performing the XOR (Exclusive OR) operation between the key and the message. The XOR operation, sometimes called modulus 2 addition, is a logic gate that gives 1 as an output when the number of inputs is odd. A legitimate receiver, Bob, can reconstruct the message by performing the XOR operation between the key and the ciphertext.

Asymmetric Encryption

The scheme operates by handling two keys which are the secret key and the public key. Each party distributes a public key in his or her name and if anyone wants to communicate with

him or her, he or she encrypts the message using the key. The secret key is then used to decipher the message. The public key and the secret key are related mathematically [6].

The RSA algorithm (named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) [9] is the most widely used public key encryption protocol at the moment. The strength of the security of this cryptosystem depends on presumed complexity of factoring large numbers. The algorithm works as follows; the message M is encrypted with a public encryption key (e, n) , where e and n are a pair of positive integers. The message is broken into a series of blocks and each block is represented with an integer between 0 and $n - 1$. The message is decrypted using a pair of integers (d, n) . The values e , d and n are determined as follows; let $n = pq$ be a product of two large prime numbers, d , the encryption exponent is chosen such that $\gcd(d, (p-1) \cdot (q-1)) = 1$, where $\gcd$ stands for the greatest common divisor and e is the encryption exponent such that $e \cdot d = 1 \pmod{(p-1) \cdot (q-1)}$. The cyphertext is obtained by raising the message to the power e modulo n . To decrypt the message, the cipher is raised to the power d modulo n . The encryption and decryption algorithms E and D are thus,

$$C \equiv E(M) \equiv M^e \pmod{n}$$

and

$$M \equiv D(C) \equiv C^d \pmod{n}$$

respectively.

1.1.2 Quantum Cryptography

The security of classical cryptosystems are based on the difficulty of mathematical encryption algorithms but with development of quantum computers these algorithms have been proven easy to break [10, 11]. Quantum cryptography is the emerging technology that has shown to be provably secure for transmission of messages between the communicating parties. Before the communicating parties can exchange messages they need to share a secret key to encrypt and decrypt their messages. This is achieved through quantum key distribution (QKD) [12]. QKD uses the laws of quantum mechanics to securely transmit the secret key between the communicating parties conventionally referred to as Alice and Bob [13]. Quantum mechanics has unique properties which provides the ability to detect the presence of an eavesdropper who is attempting to learn the key. Various protocols that exploits these law of quantum mechanics have been developed to distribute the key between communicating parties [14, 15].

1.2 Secret Sharing

Secret sharing is an important cryptographic protocol aimed at splitting and distributing secret information to untrusted agents. Suppose, Alice wants to send an important message to untrusted agents who are far away from her, she can do so by splitting the message into parts and share each part of the message with her agents. The agents have to collaborate to recover the original message, otherwise none of them can obtain any useful information about the message. Secret sharing was first proposed by Shamir in 1979 with a threshold scheme [16]. His scheme was such that if the secret was to be shared among n players, a certain k number of players has to meet to reconstruct the secret otherwise the players cannot gain any information about the secret. In quantum information processing, the information is distributed in the form of quantum states to agents, hence it is referred to as quantum state sharing (QSTS). The first work in quantum state sharing was proposed by Hillery et al [17] who used three and four particle Greenberger-Horne-Zeilinger (GHZ) states to distribute a private message to two and three agents respectively. QSTS has a wide range of applications which include joint sharing of quantum money, quantum error correction and quantum information networks [18].

1.3 Motivation

Quantum key distribution (QKD) can be used to securely exchange the secret key between the communicating parties which are conventionally referred to as Alice and Bob. The protocol exploits the laws of quantum mechanics to detect any eavesdropper who tries to gain the knowledge of the key. The first QKD protocol was proposed by Bennett and Brassard in 1984 and referred to as BB84 [13]. The protocol uses four non orthogonal states, in which Alice sends one of four states of qubit to Bob who measures them in one of two orthogonal bases. Another breakthrough in QKD was made by Ekert in 1991 who discovered a protocol based on quantum entanglement [19]. The protocol makes use of entangled pair of photons which are distributed to Alice and Bob. Both Alice and Bob must randomly pick one of three coplanar axes in which to measure the incoming particles. The eavesdropper is detected by using the Bell's inequality: its violation implies Eve's absence whilst its satisfaction detect her presence. Moreover, many QKD protocols based on the BB84 and E91 have been proposed [20–22].

For most existing QKD protocols, it is essential to have a known reference frame between the communicating parties [23]. For instance, alignment of polarisation states for polarizing encoding and interferometric stability for phase coding. However, unstable fibre communi-

cation links or imperfections in the measuring devices may lead to unknown and varying reference frame and has detrimental effects on the states received by Bob [24]. Efforts have been made to tackle potential reference frame misalignment by encoding qubits with larger systems. However, this requires creation and manipulation of many photon entangled states which are very difficult to generate and are very sensitive to losses. Therefore, reference frame independent (rfi) QKD provide solutions to those problems as it does not require any alignment of shared reference frame between the communicating parties. The rfi QKD has applications, for example, in earth to satellite communications and path-encoded QKD [25].

Secret sharing provides another mechanism for sharing secret information. The restricted access to secret information makes secret sharing suitable for applications such as securing corporate funds. For instance, if a financial company wants to secure money in one of its accounts, it can use the threshold secret sharing scheme to share account access code among authorised employees. In order to retrieve the secret, certain number of employees have to collaborate to access the funds and this reduces the chances of money be stolen by particular individual [2].

In quantum information processing, secret sharing has a wide range of applications which include quantum error correction and quantum information networks. A secret sharing scheme can also be used to secure a secret over multiple servers and still be restored even in case of multiple server failures. Each share of the secret may be distributed and stored on a different server, but the dealer can recover the secret even if several servers break down as long as they can recover a number of shares required to form the access structure. Secret sharing is also robust against many eavesdropping attacks, as it makes it very difficult for any illegitimate person to obtain information about the secret.

1.4 Outline of the Thesis

This thesis is structured in the following way:

The first chapter gives a general overview of cryptography and secret sharing which are the main subjects of this thesis. The motivation behind this study is also highlighted and lastly the outline of the thesis.

Chapter 2 gives a review of some of the elements of classical information theory that are vital to cryptography. It also introduces some of the quantum mechanics concepts which are important in quantum information processing and in particular to our proposed proofs. These concepts are going to be used to derive the security proofs for our QKD schemes.

In chapter 3 we provide a review of various QKD schemes. We describe the processes

involved in the implementation of QKD protocols and introduce the security aspect of QKD by explaining the fundamental principles of quantum mechanics behind the security of QKD protocols. We extend this to the eavesdropping strategies that might be employed by Eve in her pursuit to learn the shared secret key.

Chapter 4 introduces another major subject of our study i.e., secret sharing. A general description of secret sharing is given in this chapter beginning with the classical secret sharing and extending it to its quantum counterpart.

Chapter 5 is devoted to a security proof of the three party reference frame independent QKD protocol. We describe operation of our protocol and the tools used for calculation of the error bounds for secure key generation.

Chapter 6 focuses on the derivation of a security proof for a generic QKD protocol. The communicating parties' qubits measurement results are described by a random variable which has to be maximised to obtain the secret key rate.

In chapter 7 we propose a scheme for sharing an arbitrary unknown quantum state by using GHZ states. The scheme is described for the case of sharing a quantum state to four agents and then it is generalised to a multiparty case.

Chapter 8 considers another quantum secret sharing scheme which makes use of EPR pairs to distribute the unknown quantum state to various agents. The scheme is described in terms of the quantum resources and the classical resources required to reconstruct the quantum state.

Finally in chapter 9 we provide the concluding remarks of the thesis.

Chapter 2

Information Theory

2.1 Classical Information Theory

Information theory was proposed by Claude E. Shannon to find fundamental limits on information processing operations such as compressing data and on reliably storing and communicating data [26]. Since its inception, information theory has applications in various disciplines such as thermal physics, quantum computing and cryptography [27, 28]. A key measure of information is entropy, which is usually expressed by the average number of bits needed to store or communicate one symbol in a message. Entropy quantifies the uncertainty involved in predicting the value of a random variable. For example, specifying the outcome of a fair coin flip (two equally likely outcomes) provides less information (lower entropy) than specifying the outcome from a roll of a die (six equally likely outcomes). In this chapter, we are going to briefly review the basic entropy definitions and highlight some of the most important properties which are going to be used later, for example in calculating information gain in quantum measurements and also in the derivation of various security proofs.

2.1.1 Entropy of Random Variables

Shannon defined the entropy of a discrete random variable X , which we denote by $H(X)$ as

$$H(X) = E[\log_2(p(X))] = - \sum_x p(x) \log_2 p(x) \quad (2.1)$$

where E is the expectation value of the discrete random variable X , whose possible values x are drawn from the probability distribution $p(x)$ [29]. He did this by proving a coding theorem showing that if one wishes to code the given process into a sequence of binary symbols so that a receiver viewing the binary sequence can reconstruct the original process

perfectly (or nearly so), then one needs at least $H(X)$ binary symbols or bits and one can accomplish the task with very close to $H(X)$ bits. This coding theorem is known as the noiseless source coding theorem [26].

Binary Entropy

The information entropy for a random variable with two possible outcomes is the binary entropy function [30], usually taken to the logarithmic base 2, denoted as:

$$H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p), \quad (2.2)$$

where p and $1 - p$ are the probabilities of the outcomes. In QKD this entropy is used to calculate the error rates in the derivation of security proofs.

2.1.2 Joint Entropy

If we have two random variables X and Y then their joint entropy $H(X, Y)$ which measure the combined uncertainty of the two is given by

$$H(X, Y) = - \sum_{x,y} p(x, y) \log_2 p(x, y), \quad (2.3)$$

where x and y are particular values of X and Y and $p(x, y)$ correspond to the joint probability of the values occurring together. In security analysis of QKD protocols, the random variables X and Y represents Alice and Bob's bit strings respectively. The joint entropy measures the total uncertainty about Alice and Bob's bit strings.

2.1.3 Conditional Entropy

The conditional entropy of X given random variable Y is the average conditional entropy over Y . That is, in case we know the value of the other variable, say Y then we can calculate the uncertainty of X from their joint entropy.

$$\begin{aligned} H(X|Y) &= - \sum_{y \in Y} p(y) \sum_{x \in X} p(x|y) \log p(x|y) \\ &= - \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(y)}. \end{aligned} \quad (2.4)$$

Conditional information can also be interpreted as:

$$H(X|Y) = H(X, Y) - H(Y). \quad (2.5)$$

In quantum communication conditional entropy defines the information that Bob has attained given Alice's results. It is the information that has leaked to Eve during public discussion [31].

2.1.4 Mutual Information

Another Shannon's entropy quantity is the mutual information which measures how much information is contained in both variables [32]. The mutual information of X relative to Y is given by

$$I(X : Y) = \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)}. \quad (2.6)$$

Mutual information can also be represented as:

$$I(X : Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y : X). \quad (2.7)$$

It is important in quantum communications as it can be used to show the degree of correlation of the bit strings shared by the communicating parties.

2.1.5 Shannon's Noisy Channel Coding Theorem

Another important discovery by Shannon was the noisy channel coding theorem which gives the amount of information that can be reliably transmitted through a noisy channel [26]. In particular, suppose Alice wants to send a message to Bob through a noisy channel. To do so, she sends the encoded input message X to Bob who receives the output message Y . Due to the inevitable noise through the channel, the message received by Bob will not be the same as the one sent by Alice. For negligible noise, the received message almost resemble the original message sent by Alice. When discussing the amount of information that can be transmitted across a communication channel between two parties, the mutual information becomes the important measure. With the help of a random-coding argument Shannon proved that for any noisy channel, optimizing the mutual information between the channel input and output, gives the maximum rate at which information can be transmitted through the communication channel. This is referred to as the channel capacity C and is

given by

$$C = \max_{p(x)} I(X : Y), \quad (2.8)$$

where the maximum is taken over all input distributions $p(x)$ for X . The input X is described by a random variable with probability distribution $p(x)$, where x is an element from the set of all possible input strings [32].

2.2 Quantum Information Theory

In order to have a good grasp of quantum information and quantum computation we first need to understand the principles of quantum mechanics. Quantum mechanics explains the behaviour of matter and its interactions with energy on the scale of atoms and subatomic particles [28]. It gives a mathematical framework for the development of physical theories. This section introduces elementary concepts of quantum mechanics which will be used for most parts of this report.

2.2.1 Qubit

The simplest quantum mechanical system is the quantum bit or qubit [28]. The qubit is a two-level quantum system. An example of a qubit systems are the spin of an electron, the polarization of a photon, or a two-level atom with a ground state and an excited state. A qubit is a unit vector state in two dimensional complex space. The Dirac notation is mostly used to express the state vector. In the Dirac notation, a state vector is denoted by $|\psi\rangle$ and its dual vector by $|\psi\rangle^\dagger = \langle\psi|$. The inner product between two vectors $|\psi\rangle$ and $|\varphi\rangle$ is then written as $\langle\varphi|\psi\rangle$. The normal vector representation of orthonormal basis of a qubit are $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Just as classical bit has a state 0 or 1, the two possible states for qubit are $|0\rangle$ and $|1\rangle$. However, unlike the classical bit which can either be in state 0 or 1, a qubit exists as a superposition of the states $|0\rangle$ and $|1\rangle$ i.e.,

$$\begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \end{aligned} \quad (2.9)$$

where α and β are complex numbers such that

$$|\alpha|^2 + |\beta|^2 = 1, \quad (2.10)$$

or

$$\langle \psi | \psi \rangle = (\alpha^* \ \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = 1.$$

A qubit can also be visualised on a bloch sphere as shown in Figure 2.1. A single qubit can

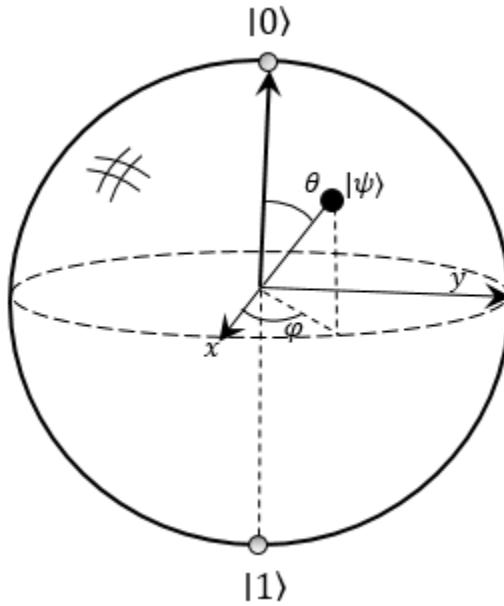


Figure 2.1: The Bloch sphere visualisation of a single qubit

be defined as a point on a unit three dimensional sphere. An arbitrary qubit $|\psi\rangle$ can, by using two parameters θ and ϕ , always be represented in the form,

$$\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle, \quad (2.11)$$

where $\alpha = \cos \frac{\theta}{2}$ is taken to be real because it has no observable effect. Pure states lie on the surface of the sphere, for example the qubit state $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ lie on the equator of the sphere in the positive y-axis. A qubit can also exist as a mixed state which is represented by points within the sphere. The mixed state possesses three degrees of freedom; the angles θ , ϕ and the length r of the vector [33].

2.2.2 Linear Operators

Linear operators are the matrices that are used to represent the transformations of state vectors from one vector space to another [28, 34]. A linear operator between vector spaces V and W is defined to be any function $A : V \rightarrow W$ which is linear in its inputs,

$$A \left(\sum_i a_i |v_i\rangle \right) = \sum_i a_i A(|v_i\rangle). \quad (2.12)$$

The Pauli Matrices

These are useful 2×2 Hermitian and unitary matrices in quantum information. They represent unitary single qubit operations. They are expressed as;

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = -i(|0\rangle\langle 1| - |1\rangle\langle 0|) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Inner Product

An inner product is a function which takes two vectors from the same space and evaluates to a single complex number [33]. For example, if $|w\rangle = \sum_i w_i |i\rangle$ and $|v\rangle = \sum_j v_j |j\rangle$ are vectors with respect to some orthonormal basis $|i\rangle$. Then, the inner product of the two vectors is given by;

$$\langle v|w\rangle = \left(\sum_i v_i |i\rangle, \sum_j w_j |j\rangle \right) = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i,$$

where v^* denotes the complex conjugate of the complex number v and $\delta_{ij} = \langle i|j\rangle$.

Outer Product

Suppose $|v\rangle$ is a vector in an inner product space V , and $|w\rangle$ is a vector in an inner product space W . We can define an outer product, $|w\rangle\langle v|$, to be the linear operator from V to W whose action is defined by $(|w\rangle\langle v|)(|v\rangle) \equiv \langle v|v\rangle|w\rangle$ [28]. Linear combinations of outer products operators $|w\rangle\langle v|$ can be treated as of inner products. By definition $\sum_i a_i |w_i\rangle\langle v_i|$ is the linear operator which, when acting on $|v\rangle$ produces $\sum_i a_i |w_i\rangle\langle v_i|v\rangle$ as an output. The importance of outer product can be discovered from the completeness relation for orthonormal vectors. Let $|i\rangle$ be any orthonormal basis for a vector space V , so an arbitrary vector $|v\rangle$ can be written as $|v\rangle = \sum_i v_i |i\rangle$ for some sets of complex numbers v_i . Note that $\langle i|v\rangle = v_i$. Therefore,

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i |i\rangle = |v\rangle.$$

Since the last equation is true for all $|v\rangle$ it follows that $\sum_i |i\rangle\langle i| = I$.

Eigenvectors and Eigenvalues

An eigenvector of a linear operator A on the vector space is a non zero vector $|v\rangle$ such that $A|v\rangle = v|v\rangle$ where v is a complex number known as the eigenvalue of A corresponding to $|v\rangle$ [35]. A diagonal representation for an operator A on a vector space V is a representation $A = \sum_i \lambda_i |i\rangle\langle i|$ where the vectors $|i\rangle$ form an orthonormal set of eigenvectors for A , with corresponding eigenvalues λ_i .

2.2.3 Density Operators

A density operator is an ensemble of states used to describe a quantum system whose state is not completely known [36]. Suppose a quantum system is in one of states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i . Then, we can define $p_i, |\psi_i\rangle$ as an ensemble of pure states. The density operator for the system is defined by the equation

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|. \quad (2.13)$$

Suppose, for instance, if we consider the closed quantum system whose evolution is described by the unitary operator U and was initially in the state $|\psi_i\rangle$ with probability p_i , then after the evolution has occurred the system will be in the state $U|\psi\rangle$ with probability p_i . Thus,

the evolution of the density operator is described by the equation

$$\rho = \sum_i p_i |\psi\rangle\langle\psi| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger.$$

2.2.4 Unitary Transformations

The evolution of a closed quantum system is described by a unitary transformation. The state $|\psi\rangle$ of the system at time t_0 is related to the state $|\psi\rangle$ of the system at time t_1 by a unitary operator U which depends only on the times t_0 and t_1 [28]. This is described by the Schrödinger equation:

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H|\psi\rangle, \quad (2.14)$$

where H refers to the Hamiltonian of the physical system. If we know the Hamiltonian of a system, then in principle we understand its dynamics completely. Integrating the Schrödinger equation we obtain:

$$|\psi(t_1)\rangle = \exp\left(\frac{-iH(t_1 - t_0)}{\hbar}\right) |\psi(t_0)\rangle \quad (2.15)$$

$$= U(t_1 - t_0) |\psi(t_0)\rangle.$$

Generally, a closed quantum system evolves according to a unitary operator U . Unitary evolution operator satisfies the condition:

$$U^\dagger U = 1. \quad (2.16)$$

2.2.5 Quantum Measurements

Suppose we perform a measurement described by measurement operators M_m . If the initial state was $|\psi_i\rangle$, then the probability of getting result m is evaluated as:

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \text{Tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|).$$

Using the law of total probability we get

$$p(m) = \sum_i p(m|i)p_i = \sum_i p_i \text{Tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) = \text{Tr}(M_m^\dagger M_m \rho).$$

If the initial state was $|\psi_i\rangle$ then the state after obtaining the result m is expressed as;

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}}.$$

Thus, after a measurement which yields the result m we have an ensemble of states $|\psi_i^m\rangle$ with respective probabilities $p(i|m)$. The corresponding density operator is given by

$$\rho_m = \sum_i p(i|m) |\psi_i^m\rangle \langle\psi_i^m| = \sum_i p(i|m) \frac{M_m|\psi_i\rangle \langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}.$$

From the elementary probability theory, $p(i|m) = p(m, i)/p(m) = p(m|i)p_i/p(m)$. By substituting in the above equations we get:

$$\rho_m = \sum_i p_i \frac{M_m|\psi_i\rangle \langle\psi_i|M_m^\dagger}{\text{Tr}(M_m^\dagger M_m \rho)} = \frac{M_m \rho M_m^\dagger}{\text{Tr}(M_m^\dagger M_m \rho)}.$$

If a quantum system is prepared in the state ρ_i with probability p_i then one can show that the system is described by a density matrix $\sum_i p_i \rho_i$ [28]. To prove this, suppose that ρ_i arises from some ensemble $p_{ij}, |\psi_{ij}\rangle$ of pure states, so the probability for being in the state $|\psi_{ij}\rangle$ is $p_i \rho_{ij}$. The density matrix for the system is thus $\rho = \sum_{ij} p_{ij} \rho_{ij} |\psi_{ij}\rangle \langle\psi_{ij}| = \sum_i p_i \rho_i$.

Projective Measurements

A projective measurement is described by an observable Q represented by a Hermitian operator $\hat{Q}$ whose eigenvalue are $\{q_1, q_2, \dots, q_n\}$ and associated eigenstates $\{|q_1\rangle, |q_2\rangle, \dots, |q_n\rangle\}$ [35]. The spectral decomposition of the observable $\hat{Q}$ is then

$$\hat{Q} = \sum_n q_n P_n, \quad (2.17)$$

where $P_n = |q_n\rangle \langle q_n|$ is the projector on the eigenspace of Q with eigenvalue q_n . The probability q_n , which result from measurement of $|\psi\rangle$ is given by

$$p(q_n) = \langle\psi|P_n|\psi\rangle. \quad (2.18)$$

If the result q_n is obtained, then the post measurement state is expressed as

$$\frac{P_n|\psi\rangle}{\sqrt{p(q_n)}}.$$

Positive Operator Valued Measure (POVM)

Projective measurements provide us with probabilities of different possible measurement outcomes and the post measurement state of the system. For QKD applications, the main interest is the probability of respective measurement outcomes. The POVM formalism is adopted for such instances.

Consider a set of measurement operators M_m performed on a quantum system in the state $|\psi\rangle$. The possible outcome m of the measurement is given by $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. If we define a set of operators:

$$E_m = M_m^\dagger M_m, \quad (2.19)$$

then E_m is a positive operator which satisfies the completeness relation $\sum_m E_m = I$ and $p(m) = \langle\psi|E_m|\psi\rangle$. The operators E_m are defined as POVM elements associated with the measurement [28].

2.2.6 Composite Systems and Entanglement

A composite quantum system made up of two or more distinct systems can be described as a tensor product of the state spaces of the component systems. For instance, suppose we have systems $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ then the joint system or the total system is

$$|\psi\rangle_{1,2,\dots,n} = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_n\rangle.$$

The tensor product can be made more concrete by writing out its effect in terms of explicit vectors. Let consider two basis states $|0\rangle_A \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle_B \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. The joint Hilbert space is

$$|0\rangle_A \otimes |1\rangle_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

In general, the Kronecker product states operates as

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

Composite systems cannot only be decomposed into a product of their component states. There exist another composite system which cannot be written as product form of their component systems called entangled states. An entangled state of a composite system encodes information about the system as a whole that cannot be measured locally (that is, by measurements on the subsystems alone) [37]. This information describes the correlation between the subsystems. In general, the state of a subsystem cannot be described by a state vector in the Hilbert space of the subsystem. If the bipartite system is in an entangled state, then any subsystem is in a statistical mixture of states. The most useful entangled states in quantum computing are the Bell states and the GHZ states. The Bell states are four maximally entangled quantum states of two qubits. These qubits are correlated such that a measurement on any of the qubit gives an automatic knowledge of the state of other qubit. The states are sometimes referred to as EPR (Einstein, Podolsky and Rosen) pairs after a famous paper by the trio who postulated that the behaviour of the qubits should be explained using hidden variables [38,39]. These states are written as below;

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).$$

The GHZ state is an entangled quantum state of $N > 2$ subsystems [40]. For two dimensional subsystems, that is for qubits, it can be written as:

$$|\Psi\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}.$$

The mostly used GHZ states are the three-particle states described below

$$|\phi^\pm\rangle = \frac{1}{2\sqrt{2}}(|000\rangle \pm |111\rangle),$$

$$|\varphi^\pm\rangle = \frac{1}{2\sqrt{2}}(|011\rangle \pm |100\rangle),$$

$$|\Psi^\pm\rangle = \frac{1}{2\sqrt{2}}(|101\rangle \pm |010\rangle),$$

$$|\Phi^\pm\rangle = \frac{1}{2\sqrt{2}}(|001\rangle \pm |110\rangle).$$

2.2.7 Quantum Information Measures

Classical information theory dealt with Shannon entropy which measures the uncertainty associated with the random variables. For quantum information theory where we are dealing with an ensemble of quantum states which are described by density operator, we use a different information measure called the Von Neumann entropy [41]. It is defined as

$$S(\rho) = -\text{tr} \rho \log_2 \rho. \quad (2.20)$$

If we choose the orthonormal basis $|i\rangle$, the density operator ρ is given by

$$\rho = \sum_i \lambda_i |i\rangle\langle i|, \quad (2.21)$$

where λ_i are the eigenvalues and $|i\rangle, i = 1, 2, 3$, is a basis for which ρ is diagonal.

Properties of Von Neumann Entropy $S(\rho)$

Below we outline some of the useful properties of the Von Neumann entropy $S(\rho)$. These properties are similar to those of the Shannon entropy [41, 42].

1. Pure States

A pure state $\rho = |\varphi\rangle\langle\varphi|$ has $H(\rho) = 0$.

2. Unitary Invariance

The entropy is unchanged by a unitary change of basis, $H(U\rho U^{-1}) = H(\rho)$, because $H(\rho)$ depends only on the eigenvalues of ρ .

3. Maximum

The maximum value of the Von Neumann entropy is $\log D$ where D is the dimension of the system, and it occurs for the maximally mixed state.

4. Concavity

For $\lambda_1, \lambda_2, \dots, \lambda_n \geq 0$ and $\lambda_1 + \lambda_2 + \dots + \lambda_n = 1$, then

$$S(\lambda_1\rho_1 + \dots + \lambda_n\rho_n) \geq \lambda_1 S(\rho_1) + \dots + \lambda_n S(\rho_n).$$

This means the Von Neumann entropy is larger if we are more ignorant about how the state was prepared.

5. Entropy of measurement

Suppose that, in a state ρ , we measure the observable

$A = \sum_y |a_y\rangle a_y \langle a_y|$, so that the outcome a_y occurs with probability

$p(a_y) = \langle a_y | \rho | a_y \rangle$, then the Shannon entropy of the ensemble of measurement outcomes $Y = a_y, |a_y\rangle$ satisfies

$$H(Y) \geq S(\rho),$$

with equality when A and ρ commute.

6. Entropy of preparation

If a pure state is selected at random from the ensemble $\{|\varphi_x\rangle, p(x)\}$, such that the density matrix is

$$\rho = \sum_x p(x) |\varphi_x\rangle \langle \varphi_x|, \tag{2.22}$$

then

$$H(X) \geq S(\rho). \tag{2.23}$$

The two are equal only if the signal states $|\varphi_x\rangle$ are mutually orthogonal.

7. Subadditivity and Strong Subadditivity

If the bipartite system AB is described by ρ_{AB} , then

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B). \quad (2.24)$$

The property holds with equality only if the system A and B are unentangled, that is $\rho_{AB} = \rho_A \otimes \rho_B$. Another property of the von Neumann entropy is the strong subadditivity which applies to tripartite systems of any state ρ_{ABC} . It states that

$$S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC}). \quad (2.25)$$

Accessible Information

The accessible information $Acc(\varepsilon)$ of an ensemble $\mathcal{E}$ refers to the maximum mutual information between a random variable encoded into quantum states, and the probabilistic outcome of a quantum measurement [41]. Let ρ_x be the state prepared by Alice from an ensemble $\{\rho_x : x = 0, \dots, n\}$ with the probability $p_0, \dots, p_n$. If we define Bob's measurements by POVM elements $\{E_y : E_0, \dots, E_n\}$ on the state, with the measurement outcome Y , the conditional probability for the measurement outcome Y is

$$p(Y|X) = \langle \varphi_x | E_y | \varphi_x \rangle, \quad (2.26)$$

and these probabilities together with ensemble X gives us the amount of information Bob gains on average. From the optimal measurements performed by Bob the maximal information gain is given by

$$Acc(\varepsilon) = \max_{E_y} I(X : Y). \quad (2.27)$$

This quantity is called the accessible information of the ensemble $\mathcal{E}$. The accessible information of an ensemble of mixed states $\{\rho_x, p_x\}$ satisfies

$$Acc(\varepsilon) \leq \chi(\varepsilon), \quad (2.28)$$

and is known as the Holevo bound [43]. This bound is not tight in general, though it holds with equality for ensembles of mutually orthogonal mixed states. It asserts that for any such

measurement Bob may execute

$$H(X : Y) \leq S(\rho) - \sum_x p_x S(\rho_x), \quad (2.29)$$

where $\rho = \sum_x p_x \rho_x$ is the statistical operator describing Alice's signals.

Chapter 3

Quantum Cryptography

Quantum cryptography or more specifically Quantum key distribution (QKD) is the emerging technology that has shown to be provably secure for transmitting messages between the communicating parties [44]. Unlike its classical counterpart, its security is based on the difficulty of mathematical encryption algorithms, QKD uses the laws of quantum mechanics to distribute the secret key between the communicating parties conventionally referred to as Alice and Bob. Quantum mechanics possesses unique properties which provides the ability to detect the presence of an eavesdropper who is attempting to learn the key. For instance, if an eavesdropper Eve tries to extract some information from quantum states by performing measurement on them, she will introduce a disturbance on the quantum system which can be detected by Alice and Bob. Alternatively, if Eve's goal is to make a perfect copy of the state Alice sent to Bob; her attempt is however prohibited by the no cloning theorem [45].

3.1 QKD Schemes

QKD schemes can be categorised according to the quantum resources used in the protocol and their mode of implementation. A description of each scheme is going to be presented and examples of protocols which fall under them are given in the following sections.

3.1.1 Prepare and Measure (P& M) Schemes

In P & M schemes, Alice prepare the qubits according to her basis of choice. Each qubit is assigned a bit value. She randomly and independently selects the qubits from her basis and send them to Bob over the quantum channel. Bob receives the noisy qubits and executes measurement on them according to his choice of basis. Alice and Bob then discuss over the classical channels their preparation and measurement basis. They discard all states where

they measured using incompatible basis. Due to possibility of noise in the quantum channel or the presence of Eve, the sequence of bits shared by Alice and Bob may not be identical but rather have some fraction of errors. Eve may also have gained some information about the bits shared by Alice and Bob. The remaining steps is to perform an error correction and privacy amplification to distill a secure key [44]. Under this scheme, there is BB84 [13], SARG04 [20] and six state [46] protocols. Below we describe these protocols.

BB84 Protocol

The protocol was proposed by Charles H. Bennet and Gilles Brassard, hence the name BB84 [13]. The protocol is based on the Heisenberg uncertainty principle [47]. This protocol uses the photon polarization states to send the information. Alice and Bob are linked by a quantum channel which is used to transmit polarised photons between the users. The classical channel is used to discuss the results and detect any eavesdropping. If there is no eavesdropping the shared secret key is used to encrypt and decrypt the message using one time pad. If there is any eavesdropping the key is discarded and process is repeated again. The procedure for BB84 protocol is shown in Table 3.1 below.

Table 3.1: A BB84 Protocol Implementation

Alice's bit sequence	1	0	1	1	0	1	0	0	0	1
Alice's basis	×	+	+	+	×	+	×	×	+	×
Alice's photon polarization										
Bob's basis	+	+	×	+	+	×	×	+	+	×
Bob's measured polarization										
Bob's sifted measured polarization										
Bob's data sequence		0		1			0		0	1

Communication through the quantum channel Alice randomly chooses the polarised photons and send them to Bob. Photons are polarised using conjugate bases, which are either a rectilinear basis (vertical/horizontal polarisations) or a diagonal basis (45° and 135° polarisations). Each polarisation is generated by a basis and is allocated the value 0 or 1 bits of information and these encodings are agreed between Alice and Bob before they start to exchange quantum states. For each photon, Bob randomly chooses one of the two measurement bases (rectilinear and diagonal) to perform a measurement. Bob records his measurement bases and results. He either measures in the same basis as Alice and get the

correct result or measures on a different basis and gets uncorrelated results. Bob publicly acknowledges his receipt of signals.

Public Channel communication In this channel Alice and Bob announces the bases of their measurements. In particular, any photons which were processed using non correlating bases are discarded. Because they both randomly chose the bases, they obtain mismatching and matching results with equal probability. The remaining key is called the sifted key. To check for any eavesdropping Alice and Bob randomly select a fraction, p of the sifted key as the test events. The test events are used to compute the error rate. If the error rate is greater than the prescribed threshold value of 11% they abort, otherwise, they proceed to the next step. The 11% lower bound for the error rate is valid for a sufficiently well built equipment that conforms to the idealised model, and for a true single photon source [48]. A large error rate may occur due to two main reasons: technical imperfections in the set up and the potential eavesdropper.

SARG04 Protocol

In SARG04 protocol Alice creates one of four states from two orthogonal bases; $|\uparrow\rangle \equiv |0\rangle$, $|\downarrow\rangle \equiv |1\rangle$, $|\nearrow\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\swarrow\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. She then sends the qubit signal to Bob who measures in the σ_z or σ_x direction. The basis $\{\uparrow, \downarrow\}$ is assigned the bit value 0 whilst the other basis $\{\nearrow, \swarrow\}$ is given bit value 1. Thus the two bases are selected randomly with equal probability.

In the public discussion phase, Alice does not announce the basis she used, instead she discloses a pair of states from different bases including the state she sent. The four key sifting sets are: $\{\uparrow, \nearrow\}$, $\{\uparrow, \swarrow\}$, $\{\downarrow, \nearrow\}$ and $\{\downarrow, \swarrow\}$. For each of the qubit received, Bob compares his measurement result to the pair of states announced by Alice. If his measurement result is conjugate to one of states in the set, then he concludes that the other state has been sent, which is a conclusive result. Otherwise if the measurement result is non-orthogonal to either of the states in the set, the result is inconclusive [49].

Six State Protocol

The six state is similar to BB84 protocol except that there is an additional basis. In this protocol the three bases are $\{|0\rangle, |1\rangle\}$, $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, $\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$. Alice randomly selects one of states from the three bases and sends it to Bob who measures it either in the σ_x or σ_z direction. Thus a prior probability that Alice and Bob uses the same basis is $1/3$. The scheme has a higher symmetry as compared to BB84 protocol and this

simplifies the security analysis considering symmetric eavesdropping strategies [46].

3.1.2 Entanglement Based (EB) Schemes

The EB schemes uses entangled pairs of photons. These can be produced by a source at Alice's side, or Bob's side, or by an external source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair. The pairs of entangled signals are then measured in certain bases chosen by Alice and Bob separately. Contrary to P& M schemes, EB schemes are basis independent. Entangled based qubit protocols use the nonlocal correlations to achieve security. They rely on the fact that if any local variable exists which can predict the state of an entangled qubit pair, then nonlocal correlations are not observed. The first EB scheme was proposed by Ekert in 1991 [19] by using entangled quantum states explored in the EPR thought experiment. This protocol uses the Bell's inequality to detect the presence or absence of Eve [39].

Ekert Protocol

In Ekert protocol the source emits the pairs of spin-1/2 particles in singlets states:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle).$$

Both Alice and Bob randomly select one of three coplanar axes in which to measure the incoming particles. These three bases can be mathematically represented by defining the vectors $a_i (i = 1, 2, 3)$ (for Alice) and $b_j (j = 1, 2, 3)$ (for Bob). If the particles are moving along the z direction, the vectors a_i and b_j are in the $x - y$ plane (perpendicular to the trajectory of the particles). By using the vertical x axis from which to measure the angles, the vectors a_i and b_j can be described by $|\psi\rangle_1^a = 0^\circ$, $|\psi\rangle_2^a = 45^\circ$, $|\psi\rangle_3^a = 90^\circ$ and $|\psi\rangle_1^b = 45^\circ$, $|\psi\rangle_2^b = 90^\circ$, $|\psi\rangle_3^b = 135^\circ$. The a and b superscripts describe the orientation of Alice and Bob's analyser's respectively. Figure 3.1 shows a representation of the bases described above.

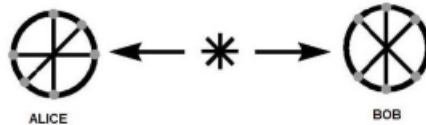


Figure 3.1: Poincare sphere representation of Ekert's protocol

If Alice and Bob choose compatible bases, they will have anti-correlated outcomes, which implies that Bob's particle will have spin up, and Alice's will have spin down, and vice versa.

Alice and Bob then publicly announces the measurement basis they used to measure their particles. They discard the results obtained using incompatible basis and this reduces the key to 30% of its original size, leaving them with a sifted key. Within the sifted key, the spin up and spin down states of the particles correspond to bit values 1 and 0 respectively. The second subsequence, called rejected key, consists of all remaining bit which serves to detect Eves presence.

The correlation coefficient of Alice's (a_i) and Bob's (b_j) measurements below is used to detect the presence of an eavesdropper.

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) + P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j)$$

where $P_{\pm}$ is the probability of obtaining ± 1 along a_i and ± 1 along b_j . The quantity S , which is the sum of all correlation coefficients where Alice and Bob measured using incompatible basis is given by

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3).$$

Using local realism, Bell [39] proved that the value of S is ≤ 2 . However, quantum mechanics gives that

$$S = 2\sqrt{2}.$$

This means that if the original states were truly entangled states, and defied the rules of local realism, Bell's theorem should be violated. Therefore, Alice and Bob can obtain the value S from the results in which they measured using incompatible basis. If the particles were not tampered with by an eavesdropper, S should equal $2\sqrt{2}$. If Alice and Bob receive their expected value of S , they can be sure that the values they measured in compatible basis are anti-correlated and that their sifted key is secure.

Lo-Chau EB Protocol

This is a P& M scheme which was converted to an EB scheme by Lo et al [50]. The scheme can be described as follows: Alice prepares $2n$ -EPR pairs in the state $|\Psi\rangle_{A_i B_i} = \frac{1}{\sqrt{2}}|00\rangle_{A_i B_i} + |11\rangle_{A_i B_i}$ and randomly performs the Hadamard transform on the system B_i . She then sends the EPR pairs to Bob who then randomly applies the Hadamard operation on the received qubits. They discard the EPR pairs in which they applied different operations. Alice and Bob selects some of the EPR pairs as the check qubits. They measure their pairs in the Z basis and compare the measurement results via classical channels. The random

sampling theorem shows that untested qubits have asymptotically the same bit error rates as check qubits with high probability. Therefore, the phase error rate on the encoded qubits is asymptotically equal to bit error rate on encoded qubits. After estimating the error rates, Alice and Bob computes bit and phase flips error syndromes to obtain nearly perfect EPR pairs. They measure their EPR pairs in the Z basis to obtain a shared secret key [50, 51].

3.1.3 Decoy State QKD

The decoy state protocol was proposed by Hwang in order to improve the key generation rate [52]. The protocol introduces decoy states in the channel which are used for the detection of an eavesdropper. In general, the protocol works as follows; Alice prepares additional sets of decoy states together with the signal states. The decoy states and the signal states have different average photon numbers. Alice sets the amplitude of each pulse according to its states and sends it to Bob through the quantum channel. The key generation rate formula achieved through the combination of the decoy method and the entanglement distillation approach by GLLP (Gottesman, Lo, Lukenhaus and Preskill) [53] is found to be:

$$\begin{aligned} R &\geq q \\ &\geq -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1 [1 - H_2(e_1)], \end{aligned} \tag{3.1}$$

where q depends on the implementation of the protocol; μ is the average number of photons per signal in the signal states; Q_μ and E_μ represent the gain and QBER of the signal states respectively; Q_1 and e_1 are gain and the error rate of the single photon state in the signal state respectively; $f(x)$ is bi-direction error correction efficiency [54] as a function of error rate, $H_2(x)$ is the binary entropy function.

3.1.4 Distributed Phase Reference Protocols

The P& M and the EB protocols generate the key from the discrete signals. Contrary to this, the distributed phase reference protocols are implemented using laser sources which emit continuous train of pulses [45]. The receiver performs joint measurement onto subsequent signals in the form of coherence measurement. Below we give two examples of the protocols under this class.

Differential Phase Shift protocol

One of the distributed phase protocols is the differential phase shift in which Alice creates a sequence of coherent states of the same intensity,

$$|\Psi(S_n)\rangle = \cdots |e^{i\psi_{k-1}}\sqrt{\mu}\rangle |e^{i\psi_k}\sqrt{\mu}\rangle |e^{i\psi_{k+1}}\sqrt{\mu}\rangle \cdots ,$$

where each phase can be set at $\psi = 0$ or π . Bob uses an unbalanced interferometer to measure and discriminate the received pulses. There are three time slots that corresponds to the events recorded on Bob's detector. The first slot represents the bright reference pulse which has taken the short path in both Alice and Bob's interferometers. The second slot is attributed to the attenuated pulse which either take the long path in Bob's interferometer or the bright pulse which take the short path in Bob's interferometer. Lastly the third slot represents the very weak pulse that has been attenuated in both Alice and Bob's interferometers. The non-orthogonality of states condition which provides the security for the protocol is met since coherent pulses has an average photon number of less than one. The information is encoded in the phase between the weak signal pulse and the accompanying reference pulse, for example, phase differences 0 and π are used to encode binary 0 and 1, respectively. If the phases of the interferometers of Alice and Bob are matched, constructive interference occurs and the detector records an event, while in the opposite case destructive interference leads to no detection event. Subsequently, Bob announces the time instances at which he recorded an event. From her modulation data, Alice knows which phase value she has applied, so they share in this way an identical bit string [55].

Coherent One Way (COW) Protocol

The COW protocol use coherent light as the source of photons. Alice sends a sequence of coherent pulses that are either non empty $|\mu\rangle$ or empty pulses $|0\rangle$ (no light). In the COW protocol, the bits are encoded in a sequence of empty and nonempty pulses separated by specified time interval τ [56].

$$|0\rangle_k = |\sqrt{\mu}\rangle_{2k-1} |0\rangle_{2k}, \quad |1\rangle_k = |0\rangle_{2k-1} |\sqrt{\mu}\rangle_{2k}.$$

These bits are clearly discriminated by measuring the time of arrival of the bit sequences. Bob uses a data line detector to unambiguously discriminate the non-orthogonal states $|0\rangle_k$ and $|1\rangle_k$. Since $|\mu\rangle_k$ is small, Bob doesn't always get a click in the data line detector, but if he gets a click in time interval k that corresponds to the first (second) pulse of the pair, he records a zero (one). For security reasons, one checks the coherence between two

successive non-empty pulses which can be produced as a decoy sequence, i.e., $|\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$ or as $|\sqrt{\mu}\rangle_{2k}|\sqrt{\mu}\rangle_{2k+1}$ across bit separation when a sequence of $|1\rangle_k|0\rangle_{k+1}$ is coded. The phase between any two successive pulses must be controlled thus providing a measure on how to detect the PNS attacks [45].

3.2 Key Distillation Process

The QKD protocols described above do not provide Alice and Bob with the perfect identical bits. Realistic quantum systems suffer from unwanted interactions with the environment. This unwanted interaction may be due to imperfections in the devices used by Alice and Bob, losses in the channel or eavesdropping [44]. Such noise processes may be controlled through error correction in order to obtain a secure key. After exchanging and measuring qubit signals Alice and Bob start processing their data via classical channel. They estimate parameters such as error rate in decoding, quantum decoherence detection rates in the quantum channel.

3.2.1 Error Correction

After parameter estimation, Alice and Bob hold a raw key which contains symbols that are partially correlated. To obtain a short secret key from the raw key, one way classical post processing is required. Alice sends her error syndromes to Bob who will then correct his qubits by executing the Z or X operations so that his syndromes match Alice's syndromes [57], that is, Alice performs a measurement which tells her what error (phase or bit flip), if any, occurred on the quantum state. The measurement result is called the error syndrome.

3.2.2 Privacy Amplification

The purpose of this procedure is to eliminate Eve's knowledge of the sifted key. Some valuable information may be obtained by Eve during the information reconciliation [58]. Alice and Bob has to carry out this step to remove Eve's partial information about the key. The fraction to be further removed can therefore be written as $\min(I_{AE}, I_{EB})$, where I_E is Eve's information about the sifted key. The Eve's information is computed differently depending on the eavesdropping strategy. For individual attacks, where Eve measures her probes before classical postprocessing, the information bound is given by Csiszar-Korner bound [59]

$$I_{AE} = \max_{\text{Eve}} I(A : E). \quad (3.2)$$

In case of collective attacks where Eve's measurements are delayed until the end of classical postprocessing, the secret key fraction is achieved using Devetak-Winter bound [60]

$$I_{AE} = \max_{\text{Eve}} \chi(A : E), \quad (3.3)$$

where χ is the Holevo bound.

3.3 Implementation of QKD

Practical implementation of QKD has been a great challenge since most QKD schemes are based on the use of single photons. Unfortunately, these states are practically difficult to realize. To date, most protocols are implemented by using the faint laser pulses and entangled photon pairs in which photon and photon pair number distribution obey poisson statistics [45].

3.3.1 Single Photon Sources

Faint Laser Pulses

The laser produces coherent states with a low average number of photon μ which gives approximation of single photon Fock states [44]. The coherent state is defined as,

$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (3.4)$$

The phase factor $e^{i\theta}$ is accessible if a reference for the phase is available, otherwise the produced state is instead described by the mixture

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi} |\alpha\rangle \langle \alpha| = \sum_n P(n|\mu) |n\rangle \langle n|. \quad (3.5)$$

The probability of finding n photons in such coherent state is given by a poisson statistics and is expressed as;

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}, \quad (3.6)$$

where μ is the mean photon number and n is the number of photons.

Sub-Poissonian Sources

A Sub-poissonian source is at times referred to as single photon source due to its closer approximation to single photon source as compared to attenuated laser. It has a very low probability of producing more than one photon. Therefore, quantum signal in each mode is considered to be a photon number diagonal mixture with an insignificant impact from multiphoton terms. The quality of sub-Poissonian source is usually assessed through the second order correlation function [44,61],

$$g_2(\tau) = \frac{\langle : I(t)I(t + \tau) : \rangle}{\langle I(t) \rangle^2}, \quad (3.7)$$

where $I(t)$ is the signal intensity emitted by the source and $: :$ denotes normal ordering of the creation and annihilation operators. Specifically, $g_2(0) \approx 2p(2)/p(1)^2$, where $p(n)$ represent the probability that the source emits n photons. For poisson sources $g_2(0) = 1$. The ideal single photon source becomes achievable with decrease in $g_2(0)$.

Sources of Entangled Photons by Parametric Down-Conversion

Entangled photon pairs can also be generated by spontaneous parametric down-conversion [45,62]. A χ^2 non linear crystal is used to split photons from a pump laser beam into pairs of photons referred to as signal and idler. During this process the total energy and momentum is conserved. The output photon pairs have a lower frequency than the pump which is attributed to non-linear interaction in the optical crystal. The continuous wave pump is the one normally used for QKD. To approximate the output modes, the state behind the crystal can be denoted as;

$$|\psi\rangle_{PDC} = \sqrt{1 - \chi^2} \sum_{n=0}^{\infty} \lambda^n |n_A, n_B\rangle, \quad (3.8)$$

where $\lambda = \tanh \xi$ with ξ proportional to the pump amplitude and $|n_A, n_B\rangle$ is the state with n photons in the mode to be sent to Alice and n photons in the other mode targeted to Bob. The photons can be correlated in any of degree of freedom such as polarisation or in frequencies.

3.3.2 Quantum Channels

The single photon sources and the detectors are linked by a quantum channel. The main quantum channels used are optical fibers and free space. The channel is used to transmit

information that is encoded in the individual quantum systems. The quantum systems are two level systems referred to as qubits. The qubits need to be robust against the environment noise. The effect of decoherence depends strongly on the degree of freedom that is employed. For example, if polarisation encoding is used, the coupling between polarisation and the optical frequency has to be mastered [44].

3.3.3 Detectors

The QKD process is completed by the detection of signals on Bob's side. In general, this is accomplished through various methods, for instance, through the use of photomultipliers or avalanche diodes. The performance of the detector is determined by a number of conditions such as quantum detection efficiency, signal to noise ratio and the recovery time [44].

Avalanche Photodiodes (APDs)

APDs are the most widely used photon counters in the field of cryptography. The counters are designed from silicon, germanium, indium gallium arsenide with choice of material determined by the wavelength to be detected.

The APD are operated on the Geiger gated mode for the QKD applications [44, 45]. In this mode the APD is kept below the breakdown voltage and biased above the breakdown momentarily when the signal photon is expected to arrive. A single photon can then produce an avalanche consisting of millions of electrons and create a macroscopic current pulse. After detection event, avalanche is stopped and gated to decrease dark counts and prepare APD for the next count.

Homodyne Detection

Homodyne detection forms the most suitable method for measuring quadrature properties of light in continuous variable QKD [44]. In this scheme, a signal field is combined with a highly stable local oscillator through a symmetric beam-splitter. The superimposed beams are directed towards the proportional photodetectors (see Figure 3.2). The intensity of light is measured, and the difference between the number of photoelectrons emitted is recorded. The differential current, which vary with phase difference between signal and local oscillator provide us with quantum information of the signal field which is used to determine the quantum state of the signal field [63]. To maintain consistency on the phase difference, the signal and the local oscillator are emitted from the same source and sent through the same channel.

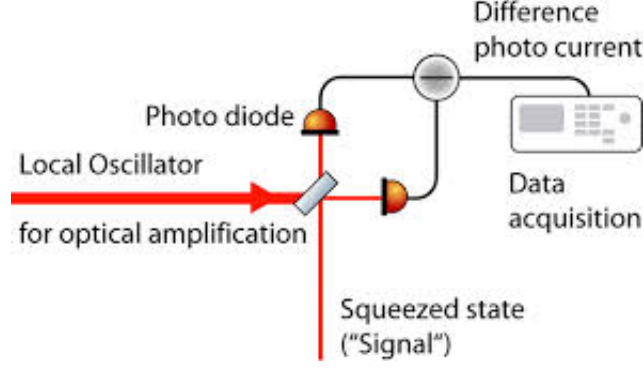


Figure 3.2: Homodyne detection scheme showing the high intensity local oscillator and the signal beam passing through a beamsplitter. Photodiodes make up the proportional detectors which produces photoelectrons. The difference in current is shown in the display and provide us with quantum information about the signal state [1].

3.4 Security of QKD

The security of QKD protocols relies on the fact that an eavesdropper who is trying to acquire information about the exchanged qubits introduces some errors due to the laws of quantum mechanics. Nevertheless, the exchange of qubits takes place under the presence of an inevitable noise in the quantum channel which may be due to imperfections in the measuring devices. But to ensure that the protocol is secure, all of the noise is attributed to the eavesdropper who is assumed to have unlimited computing power [64]. The security proofs have been developed for specific QKD protocols by using various approaches and based on the attacks that may be performed by Eve [64–66]. The security proofs provide bounds for errors for which the protocol may be deemed secure.

The No Cloning Theorem

The no cloning theorem states that it is impossible to make a copy of an unknown quantum state with perfect fidelity [67]. It can be shown as follows: Suppose there exist a quantum copying machine that can copy an unknown state. Then, considering the unitary evolution of a composite system with two orthogonal states $|0\rangle$ and $|1\rangle$ respectively as input, one finds that

$$|0\rangle \otimes |u\rangle \longrightarrow |0\rangle \otimes |0\rangle \otimes |v_0\rangle, \quad (3.9)$$

$$|1\rangle \otimes |u\rangle \longrightarrow |1\rangle \otimes |1\rangle \otimes |v_1\rangle, \quad (3.10)$$

where $|u\rangle$ is the initial state of the copying machine, $|v_0\rangle$ and $|v_1\rangle$ are the final states of the system not including the original and the duplicate. The state $|u\rangle$ is independent of the input state ($|0\rangle$ and $|1\rangle$) as the copying machine is assumed to have no prior knowledge of the state. But the problem arises when the machine tries to copy the linear superposition $a|0\rangle + b|1\rangle$, ($a, b \neq 0$) of the two orthogonal states. Then by the linearity of quantum mechanics, one obtains from Equations (3.9) and (3.10) that

$$a|0\rangle + b|1\rangle \otimes |u\rangle \longrightarrow a|0\rangle \otimes |0\rangle \otimes |v_0\rangle + b|1\rangle \otimes |1\rangle \otimes |v_1\rangle. \quad (3.11)$$

But based on the definition of quantum cloning one should obtain the following outcome; $(a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \otimes |v'\rangle$, instead. Since

$$a|0\rangle \otimes |0\rangle \otimes |v_0\rangle + b|1\rangle \otimes |1\rangle \otimes |v_1\rangle \neq (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \otimes |v'\rangle,$$

whenever, $a, b \neq 0$ which can be verified by considering a simple example, say $a = b = \frac{1}{\sqrt{2}}$, one can conclude that an unknown quantum state cannot be cloned.

Heisenberg Uncertainty Principle

Heisenberg uncertainty principle states that in a quantum system only one property from a pair of conjugate properties can be measured with certainty [68]. For example, if position and momentum properties of a particle are to be measured, then measurement of any of the two properties would disturb the other. Both cannot be measured at the same time with accuracy. This principle can be briefly stated as follows: For any two quantum mechanical observables A and B , if the corresponding operators $\hat{A}$ and $\hat{B}$ satisfy

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A},$$

then

$$\langle \Delta A \rangle \langle \Delta B \rangle \geq \frac{1}{2} \| \langle [A, B] \rangle \|,$$

where $\langle \Delta A \rangle$ and $\langle \Delta B \rangle$ are the average values of operators $\langle \Delta \hat{A} \rangle$ and $\langle \Delta \hat{B} \rangle$ respectively, and they are defined as:

$$\langle \Delta \hat{A} \rangle = \hat{A} - \langle A \rangle \text{ and } \langle \Delta \hat{B} \rangle = \hat{B} - \langle B \rangle$$

Thus $\langle \Delta A \rangle$ and $\langle \Delta B \rangle$ are the variances which measure the uncertainty of the observables A and B . For incompatible observables, i.e., for observables A and B such that $[A, B] \neq 0$, reducing the uncertainty $\langle \Delta A \rangle$, of A forces the uncertainty $\langle \Delta B \rangle$, of B to increase, and vice versa. Thus, the observables A and B cannot be simultaneously measured to arbitrary precision. Measuring one of the observables interferes with the measurement of the other.

3.4.1 Eavesdropping Strategies

Though QKD protocols seems to provide us the unconditional security, but there are various attacking strategies that have been proposed which require serious consideration. The ultimate goal of security proofs is to produce the cryptographic key extracted by error correction and privacy amplification. This key is guaranteed secure against any attack allowed by quantum physics that an eavesdropper may have implemented that is compatible with some given observed error rate. Some of the attacks that may be performed by an eavesdropper that are considered when devising the security proofs for QKD protocols are presented below. For most cases, the security analysis is restricted to an individually and identically distributed (i.d.d) problem, in that the adversary is assumed to intercept each state transmitted from Alice to Bob separately and in exactly the same way.

Individual Attacks

In an individual attack, Eve has a quantum memory to store her ancillae. She intercepts each state sent by Alice separately and applies a unitary operation with the intent of partially cloning it. She does so after sifting has occurred but before error correction takes place [61].

Security against Individual Attacks An example of individual attack model is the Fuchs-Peres entangling-probe (FPEP) attack discovered by Fuchs et al [44, 69]. As already mentioned in this attack Eve allows her probe to interact with the signal system sent by Alice. The joint unitary evolution leaves the two systems in an entangled quantum state. The signal is then passed on to Bob, whilst the probe remains in possession of Eve and awaits the information reconciliation process to be completed before measuring the probe. Entanglement between the system and the probe introduces some correlation between Eve and Bob's measurements, giving Eve partial knowledge on the key.

Let $\mathcal{H}_{\text{Eve}}$ and $\mathbb{C}^2 \otimes \mathcal{H}_{\text{Eve}}$ be the Hilbert spaces of Eve's probe and of the total qubit and probe system, respectively. If $|\vec{m}\rangle$, $|0\rangle$ and U represent the qubit and the probe's initial states and the unitary interaction, respectively, then the state of the qubit received by Bob

is described by the density matrix obtained by tracing out Eve's probe,

$$\rho_{\text{Bob}}(\vec{m}) = \text{Tr}_{\mathcal{H}_{\text{Eve}}}(U|\vec{m}, 0\rangle\langle\vec{m}, 0|U^\dagger). \quad (3.12)$$

Due to the symmetry of the BB84 protocol, we assume that Bob's state is related to Alice's $|\vec{m}\rangle$ by a simple shrinking factor $\eta \in [0, 1]$:

$$\rho_{\text{Bob}}(\vec{m}) = \frac{1 + \eta\vec{m}\vec{\sigma}}{2}. \quad (3.13)$$

Since the qubit state has two dimensional state space, the unitary operator is wholly expressed by its action on the two states. For example, the $|\uparrow\rangle$ and $|\downarrow\rangle$ states. After the unitary interaction, the states can be appropriately written in the Schmidt form as;

$$U|\uparrow, 0\rangle = |\uparrow\rangle \otimes |\phi_\uparrow\rangle + |\downarrow\rangle \otimes |\theta_\uparrow\rangle, \quad (3.14)$$

$$U|\downarrow, 0\rangle = |\downarrow\rangle \otimes |\phi_\downarrow\rangle + |\uparrow\rangle \otimes |\theta_\downarrow\rangle, \quad (3.15)$$

where the four states $|\phi_\uparrow\rangle, |\theta_\uparrow\rangle, |\phi_\downarrow\rangle$ and $|\theta_\downarrow\rangle$ reside in the Hilbert space of Eve's probe $\mathcal{H}_{\text{Eve}}$ and satisfy $|\phi_\uparrow\rangle \perp |\theta_\uparrow\rangle$ and $|\phi_\downarrow\rangle \perp |\theta_\downarrow\rangle$. Symmetry implies $||\phi_\uparrow\rangle|^2 = ||\phi_\downarrow\rangle|^2 \equiv \mathcal{F}$ and $||\theta_\uparrow\rangle|^2 = ||\theta_\downarrow\rangle|^2 \equiv \mathcal{D}$. $\mathcal{F} + \mathcal{D} = 1$ and

$$\langle\phi_\uparrow|\theta_\downarrow\rangle + \langle\phi_\downarrow|\theta_\uparrow\rangle = 0, \quad (3.16)$$

which satisfies the unitary condition. The ϕ 's are associated with Eve's state when Bob receives the qubit uninterrupted, while the θ 's are Eve's state when the qubit is interrupted. This can be highlighted as the most general unitary interaction satisfying Eq. (3.13). One can conclude that the shrinking factor is given by $\eta = \mathcal{F} - \mathcal{D}$. Consequently, if Alice sends $|\uparrow\rangle$ and Bob measures it in the compatible basis, then $\langle\uparrow|\rho_{\text{Bob}}(\vec{m})|\uparrow\rangle = \mathcal{F}$ is the probability that Bob gets the correct result. Hence $\mathcal{F}$ is the fidelity and $\mathcal{D}$ the QBER.

It can be noticed that only four states span Eve's relevant state space and as result Eve's effective Hilbert space is at most four dimensional, regardless of her devious attacking strategies. This significantly simplifies the analysis. Due to symmetry, the attack on the

other basis satisfies;

$$U|\nearrow, 0\rangle = \frac{1}{\sqrt{2}}(|\uparrow, 0\rangle + |\downarrow, 0\rangle) \quad (3.17)$$

$$= \frac{1}{\sqrt{2}}(|\uparrow\rangle \otimes |\phi_\uparrow\rangle + |\downarrow\rangle \otimes |\theta_\uparrow\rangle + |\downarrow\rangle \otimes |\phi_\downarrow\rangle + |\uparrow\rangle \otimes |\theta_\downarrow\rangle) \quad (3.18)$$

$$= |\nearrow\rangle \otimes \phi_\nearrow + |\swarrow\rangle \otimes \theta_\nearrow, \quad (3.19)$$

where

$$\phi_\nearrow = \frac{1}{2}(\phi_\uparrow + \theta_\uparrow + \phi_\downarrow + \theta_\downarrow), \quad (3.20)$$

$$\theta_\nearrow = \frac{1}{2}(\phi_\uparrow - \theta_\uparrow - \phi_\downarrow + \theta_\downarrow), \quad (3.21)$$

$$\phi_\swarrow = \frac{1}{2}(\phi_\uparrow - \theta_\uparrow + \phi_\downarrow - \theta_\downarrow), \quad (3.22)$$

$$\theta_\swarrow = \frac{1}{2}(\phi_\uparrow + \theta_\uparrow - \phi_\downarrow - \theta_\downarrow). \quad (3.23)$$

Condition (3.13) for the $\{|\nearrow\rangle, |\swarrow\rangle\}$ infers that $\theta_\nearrow \perp \phi_\nearrow$ and $\theta_\swarrow \perp \phi_\swarrow$. With a good selection of phases, $\langle\phi_\uparrow|\theta_\downarrow\rangle$ can be made real and $\langle\theta_\uparrow|\phi_\downarrow\rangle$ is also attested to be real by the condition (3.16). Symmetry imposes that $\langle\theta_\nearrow|\phi_\swarrow\rangle \in \mathbf{Re}$. A straightforward computation concludes that all scalar products among Eve's states are real and that the ϕ 's generate a subspace orthogonal to the θ 's:

$$\langle\phi_\uparrow|\theta_\downarrow\rangle = \langle\theta_\uparrow|\phi_\downarrow\rangle = 0. \quad (3.24)$$

The fact that $|\phi_\nearrow|^2 = \mathcal{F}$ implies that the shrinking is the same for all states, and leads to the relation below between the probe states' overlap and the fidelity:

$$\mathcal{F} = \frac{1 + \langle\hat{\theta}_\uparrow|\hat{\theta}_\downarrow\rangle}{2 - \langle\hat{\phi}_\uparrow|\hat{\phi}_\downarrow\rangle + \langle\hat{\theta}_\uparrow|\hat{\theta}_\downarrow\rangle}, \quad (3.25)$$

where the hats denote normalized states, e.g $\hat{\phi}_\uparrow = \phi_\uparrow \mathcal{D}^{-\frac{1}{2}}$. Subsequently, the class of symmetric individual attacks wholly depends only on two real parameters: $\cos(x) = \langle\hat{\phi}_\uparrow|\hat{\phi}_\downarrow\rangle$ and $\cos(y) = \langle\hat{\theta}_\uparrow|\hat{\theta}_\downarrow\rangle$. Due to the symmetry, we can confidently analyse this scenario for the case

when Alice sends the $|\uparrow\rangle$ state and Bob measures in the $\{\uparrow, \downarrow\}$ basis (if not, Alice, Bob, and Eve discard the data). Since Eve knows the basis, she knows that her probe is in one of the following two mixed states

$$\rho_{\text{Eve}}(\uparrow) = \mathcal{F}P(\phi_{\uparrow}) + \mathcal{D}P(\theta_{\uparrow}), \quad (3.26)$$

$$\rho_{\text{Eve}}(\downarrow) = \mathcal{F}P(\phi_{\downarrow}) + \mathcal{D}P(\theta_{\downarrow}). \quad (3.27)$$

An optimum measurement strategy for Eve to differentiate between $\rho_{\text{Eve}}(\uparrow)$ and $\rho_{\text{Eve}}(\downarrow)$ requires to examine if her state is in the subspace created by $\phi_{\uparrow}$ and $\phi_{\downarrow}$ or the one created by $\theta_{\uparrow}$ and $\theta_{\downarrow}$. This is possible, since the two subspaces are mutually orthogonal. Eve now has the task of differentiating between two pure states with an overlap of either $\cos x$ or $\cos y$. The first option occurs with probability $\mathcal{F}$, the second with probability $\mathcal{D}$. The optimal measurement distinguishing two states with an overlap $\cos x$ is the one that gives Eve the correct prediction with probability $\frac{[1+\sin x]}{2}$. Eve's maximal Shannon information, obtained when she executes the optimal measurements, is thus given by

$$I(\alpha, \epsilon) = \mathcal{F} \left[1 - h \left(\frac{[1 + \sin x]}{2} \right) \right] + \mathcal{D} \left[1 - h \left(\frac{1 + \sin x}{2} \right) \right], \quad (3.28)$$

where $h(x)$ is binary entropy. For a given error rate $\mathcal{D}$, this information attains maximum value when $x = y$. Consequently, for $\mathcal{D} = [1 - \cos(x)]/2$ one obtains:

$$I^{\max}(\alpha, \epsilon) = \left[1 - h \left(\frac{[1 + \sin x]}{2} \right) \right]. \quad (3.29)$$

This provides the explicit and analytic optimum eavesdropping strategy. For $x = 0$ the QBER (i.e., $\mathcal{D}$) and the information gain are both zero. For $x = \pi/2$ the QBER is 1/2 and the information gain 1. For small QBER's, the information gain grows linearly:

$$I^{\max}(\alpha, \epsilon) = \frac{2}{\ln 2} \mathcal{D} + \mathcal{O}(\mathcal{D})^2 \approx 2.9 \mathcal{D}. \quad (3.30)$$

Once Alice, Bob, and Eve have measured their quantum systems, they are left with classical random variables α , β and ϵ respectively. Secret-key agreement between Alice and Bob can be achieved using error correction and privacy amplification, if and only if Alice-Bob mutual Shannon information $I(\alpha, \beta)$ is greater than Alice-Eve or Bob-Eve mutual information: $I(\alpha, \beta) > I(\alpha, \epsilon)$ or $I(\alpha, \beta) > I(\beta, \epsilon)$. It is thus interesting to compare Eve's maximal information [Eq 3.30] with Bob's Shannon information. The latter depends only on the error

rate $\mathcal{D}$:

$$I(\alpha, \beta) = 1 - h(\mathcal{D}). \quad (3.31)$$

3.4.2 Collective Attacks

In a collective attack, Eve keeps her ancilla in a quantum memory until classical postprocessing and may perform any joint measurement on the full collection of intercepted states [70]. For collective attacks, the asymptotic secret key rate r in the limit of a key of infinite size under one-way classical postprocessing is lower-bounded by the Devetak-Winter rate [60]

$$r = I(A : B) - \max_{\text{Eve}} \chi(A : E), \quad (3.32)$$

where $I(A : B)$ is the mutual information between Alice and Bob and it is given by

$$I(A : B) = 1 - h(Q), \quad (3.33)$$

where h is the binary entropy. The $\chi(A : E)$ is the Holevo Bound [43] defined as below:

$$\chi(A : E) = S(\rho_E) - \sum_x p(x) S(\rho_{E|x}), \quad (3.34)$$

where S is the Von Neumann entropy, x is a symbol of Alice's alphabet distributed with the probability $p(x)$, $\rho_{E|x}$ is the corresponding state of Eve's ancilla, and $\rho_E = \sum_x p(x) \rho_{E|x}$ is Eve's partial state.

3.4.3 Joint Attacks

This strategy constitutes the most general class of attacks on the quantum channel. In a joint attack, no presumptions are made about Eve's attack. She may entangle the signal systems from Alice to Bob and attach her probe to the combined system instead of interacting with each signal independently [71]. She then waits for the end of classical postprocessing before deciding on which measurement to perform on her ancilla. With collective and joint attacks, Eve performs her measurements after reconciliation and privacy amplification have been completed. For all of these attacks it is assumed that Eve attacks the QKD protocol but nothing prevents her from waiting for Alice and Bob to use the key.

3.4.4 QKD attacks

Photon Number Splitting(PNS) Attack

Practical QKD schemes use coherent laser sources which obey the Poisson distribution. The source emits probabilistically more than one photon signal. This opens a room for Eve to perform some sophisticated attacks such as PNS attack. The attack can be described as follows; Eve performs a quantum non demolition measurement on the photon number of each signal. She blocks all the single photon signals from Alice and splits the multiphoton signals received from Alice. She keeps a copy of the qubit in her quantum memory and sends the other copy to Bob. Eve waits until Alice announces the basis for each qubit and measures her qubits accordingly [72].

Large Pulse Attack

In this attack Eve launches a bright light pulse into the transmission line towards Alice or Bob's set up. Some parts of this pulse will be reflected back from different optical components inside the set up, because any real component has a non-zero reflection coefficient. On its way, a pulse can pass internal modulators and be modulated one or more times. Measuring the characteristics of reflected pulses, Eve can make some conclusions on the modulator's settings and if not learn the transmitted bits directly then at least know transmitted quantum states unambiguously [73].

High Power Damage Attack

Eve can cause harm or modifications to the components of the set ups used by Alice and Bob by bombarding it with high power laser. This affects the device's normal operation conditions and hence Eve can obtain information about the signals sent by Alice. For example, the high power laser can affect the detector sensitivity or damage the valuable attenuator resulting in reduced attenuation of the light. This makes the scheme insecure as the average number of photons per signal will increase making the PNS attack possible [74].

Faked State Attack

Faked state attack on quantum cryptosystem is an intercept and resend attack where Eve does not try to reconstruct the original states, but generates instead light pulses that get detected by legitimate parties in a way controlled by her while not getting detected. The attack exploits the weakness in the apparatus of QKD systems, namely the APD detectors. The APD has a recovery time of roughly $1\mu s$. Under normal operating conditions this does

not raise any concern as weak laser signals will be sent infrequently enough for the recovery of the detector. However, if APD detector is exposed to continuous light it does not recharge and is reduced to a classical photodiode. Eve can therefore by manipulating the continuous light make the detector click when she wants or can blind the detector from seeing valid input. Eve will intercept the photon from Alice and prepare a faked state to send to Bob. The prepared faked state is in opposite base with opposite bit as the state Eve intercept from Alice. For example, if Eve detects 0 in the X base, she will prepare a 1 in the Z basis for Bob. At the same time Eve will blind Bob's 1 bit detectors. Thus, if Bob measures in the X basis he has 50% chance of detecting a 0 or nothing at all and if measures in the Z basis he detects nothing at all. This leads to Bob only detecting the same bit in the same basis as Eve [75].

3.5 Security Proofs of QKD Schemes

The security of QKD can be unconditionally guaranteed if an eavesdropper is given unlimited computing power. The possibility of achieving unconditional security in QKD relies on the laws of quantum physics. However, the unconditional security does not refer to absolute security which is not practically possible. Therefore, there are some conditions which must be satisfied to attain unconditional security [45];

1. Eve does not have physical access to Bob and Alice's devices.
2. Alice and Bob must believe that their measuring devices are operating normally e.g the random number generator that selects the state to be sent.
3. The classical channel is authenticated with unconditionally secure protocols.
4. Eve's attacks is only limited by the laws of quantum physics.

QKD security proofs that exists are obtained using various methods and depends mainly on the kinds of attacks and schemes. The proofs use a wide range of information tools such as Shannon entropy and quantum error correcting codes to attain the security for the QKD schemes.

3.6 Approaches to Security Proofs

3.6.1 Twisted Pair Approach

It has been shown that maximally entangled states are not necessarily prerequisite for creation of a secure key in QKD. Private states can also be employed for generation of the secret key [76]. These are made up of completely correlated systems A and B containing a uniformly distributed key with the shield systems A' and B' alongside. These states are deemed private due to the fact that a bit of secure key can be produced from them even if Eve hold a purification of the state.

The private state δ is defined as d -dimensional private state if one of the unitaries $\mathcal{U}^{(j)}$ and a twisting operator of the form,

$$\mathcal{U}_{\text{twist}} = \sum |jj\rangle\langle jj|_{AB} \otimes \mathcal{U}_{A'B'}, \quad (3.35)$$

such that

$$\delta = \mathcal{U}_{\text{twist}}(|\Phi_d\rangle\langle\Phi_d|_{AB} \otimes \rho_{A'B'})\mathcal{U}_{\text{twist}}^\dagger, \quad (3.36)$$

for some $\rho_{A'B'}$, where $|\Phi_d\rangle = \sum_i^d |ii\rangle/\sqrt{d}$ [77]. The operation is referred to as twisting. Let $\rho_{AA'BB'}$ be the state held by Alice and Bob. Together with its purification the total state can be written in its decomposition form as;

$$\psi_{ABA'B'E} = a|00\rangle_{AB}|\psi_{00}\rangle_{A'B'E} + b|01\rangle_{AB}|\psi_{01}\rangle_{A'B'E} + c|10\rangle_{AB}|\psi_{10}\rangle_{A'B'E} + d|11\rangle_{AB}|\psi_{11}\rangle_{A'B'E}. \quad (3.37)$$

Since the key is perfectly correlated and unbiased it suffices that $b = c = 0$ and $|a|^2 = |d|^2 = \frac{1}{2}$. From the two states that generates the key $|00\rangle$ and $|11\rangle$, Eve holds the states

$$\begin{aligned} \rho_0 &= \text{tr}_{A'B'}[|\psi_{00}\rangle\langle\psi_{00}|], \\ \rho_1 &= \text{tr}_{A'B'}[|\psi_{11}\rangle\langle\psi_{11}|]. \end{aligned} \quad (3.38)$$

Perfect security imposes that $\rho_0 = \rho_1$. Thus, there exists unitaries $\mathcal{U}_{00}$ and $\mathcal{U}_{11}$ on $A'B'$ such that

$$|\psi_{00}\rangle = \sum_i \sqrt{p_i} |\mathcal{U}_0 \phi_i^{A'B'}\rangle |\varphi_i^E\rangle,$$

$$|\psi_{11}\rangle = \sum_i \sqrt{p_i} |\mathcal{U}_1 \phi_i^{A'B'}\rangle |\varphi_i^E\rangle.$$

Tracing out E leads to a state of the form

$$\rho_{A'B'} = \sum_i \sqrt{p_i} |\varphi_i\rangle \langle \varphi_i|. \quad (3.39)$$

Alice and Bob are in control of additional shield systems A' and B' , thus Eve hold a purification of $\rho_{AA'BB'}$ but not of ρ_{AB} . Since it is assumed that Eve has no access to the shield part, she is further limited in her ability to eavesdrop. Therefore, Alice and Bob can derive a higher key generation rate than in the case when Eve does have access to the shield part.

3.6.2 Complimentary Principle

The security of QKD is achieved by considering a pair of protocols; the primary and the secondary protocols between which Alice and Bob can choose to execute [78]. In the primary protocol the communication is over the classical channel, Alice measures a $(\log d)$ bit local observable Z , while Bob tries to guess its outcome. In the secondary protocol Bob assist Alice prepare an eigenstate in the complementary X basis with the help of extra channel. The prepared eigenstate is given by $|0\rangle_A \equiv d^{-1/2} \sum_i |i\rangle_A$ and produce a random results when measured in the Z basis. A detailed description of the complimentary principle is found in [78].

3.6.3 Entanglement Distillation

The main aim of entanglement distillation protocol (EDP) is to obtain nearly perfect entangled states from noisy ones initially shared between distant parties, Alice and Bob. Alice and Bob apply local operations and classical communications(LOCCs) to distil from the N noisy pairs a smaller number, say M of almost perfect pairs i.e. a state close to $|\sigma\rangle_{AB}^M$ [51].

3.7 Composability of the Key

The security of a key S can be parametrized by its deviation Q from a perfect key. A key that deviates by Q from the perfect key is called a Q secure. The main property that guarantees the security is the composability. Composability asserts that the whole protocol must be $Q + Q'$ secure if Q -secure key is to be used for Q' -secure task [79].

A composable definition of security is the one based on the trace norm

$$\frac{1}{2}\|\rho_{SE} - \tau_S \otimes \rho_E\|_1 \leq Q, \quad (3.40)$$

where ρ_{SE} as the actual state which hold some correlations between the final key and Eve, τ_S is the completely mixed state on the set Q of possible final keys, and ρ_E is any state of Eve.

Chapter 4

Secret Sharing

Secret sharing is an information processing protocol for managing secret information over multiple parties or systems [2]. It can be extensively applied to joint checking account, electronic votes, online auctions and missile launching codes. Secret sharing distribute a secret to players in a way that some subsets of players can collaborate to recover the secret fully, but all other subsets gain no information on the secret even with unlimited computing power. The subsets of players that are able to reconstruct the secret are called authorized sets or the access structure, and the subsets of players that are totally denied the secret are called unauthorized sets or the adversary structure [18]. The first secret sharing scheme was proposed by Liu in the late 1960's to address the following problem; he considered a case where a group of 11 scientists working on a secret project had to conceal their results on a vault such that none of them have individual access to the vault. The secret document can only be recovered when majority of them are present [80]. Shamir and Blakley used Liu's idea and independently proposed (k, n) threshold secret sharing scheme in 1979 [16, 81].

A $(k; n)$ threshold scheme is defined as secret sharing with an access structure [82],

$$\mathcal{A} = \{\Gamma \subseteq P; |\Gamma| \geq k\}, \quad (4.1)$$

and adversary structure

$$\mathcal{A} = \{\Gamma \subseteq P; |\Gamma| \leq k - 1\}, \quad (4.2)$$

where $P = \{P_1, P_2, \dots, P_n\}$ is the entire set of n players and Γ is some subset of the participants. If secret sharing is described by a certain threshold number k , its access structure will be called a general access structure. Every access structure must be monotone,

$$(\Gamma \in \mathcal{A} \text{ and } \Gamma \subseteq \Gamma') \Rightarrow \Gamma' \in \mathcal{A}, \quad (4.3)$$

that is, if a subset is authorized to recover the secret, all subsets containing it must recover the secret as well.

Secret sharing schemes can be categorised into three areas of study depending on the type of information that is being distributed and the channels used. Classification is based on whether a secret is a bit string or an arbitrary quantum state, or whether a secret is distributed over private or public channels [83]. All existing secret sharing schemes fall into one of these cases:

- Classical secret sharing with private channels between the dealer and each player and private classical channels shared between each pair of players.
- Classical secret sharing with public channels between the dealer and each player and either quantum or classical channels shared between each pair of players.
- Quantum secret sharing wherein the dealer shares quantum channels with each player, and these channels can be private or public, and the players share either quantum or classical private channels between each other.

4.1 Classical Secret Sharing

Classical secret sharing schemes are devised such that for all positive values of k and n , where $k \leq n$, access structures are monotone and no information can be obtained from fewer than k shares. Threshold schemes are the primitive secret sharing schemes that were constructed by Shamir [16] and Blakley [81] using polynomial interpolation and projective spaces respectively.

4.1.1 Shamir (k, n) Threshold Scheme

Shamir's (k, n) -threshold scheme is based on polynomial interpolation and provides a very simple and efficient way to share a secret among any k of the n participants [16]. Consider k points on a 2-dimensional cartesian plane $\{(x_1, y_1), \dots, (x_k, y_k)\}$. If x values are distinct, define a polynomial $P(x)$ of degree $k - 1$,

$$P(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}.$$

Without loss of generality, if we assume the secret K is a number, it can be divided into parts K_i where

$$a_0 = K, K_1 = P(1), \dots, K_i = P(i), \dots, K_n = P(n).$$

Given any subset of k of these K_i values (together with their identifying indices), we can find the coefficients of $P(x)$ by interpolation, and then evaluate $K = P(0)$. Nevertheless, the knowledge of just $k - 1$ of these values, is not enough to give us the value K (see Figure 4.1). To justify this argument we can rather employ the modular arithmetic which works as follows. If p is a prime number greater than K and n , then a secret key K can be obtained from interpolation of set of integers modulo a prime number p ,

$$P(x) = K + \sum_{i=1}^{k-1} a_i x^i \bmod p.$$

The coefficients $a_0, \dots, a_{k-1}$ in $P(x)$ are randomly chosen from a uniform distribution over the integers in $[0, p)$, and the values $K_1, \dots, K_n$ are computed modulo p . Let consider a case where $k - 1$ participants are trying to learn the secret key K . For each candidate value K' in $[0, p)$ they can construct one and only one polynomial $P'(x)$ of degree $k - 1$ such that $P'(0) = K'$ and $P'(i) = K_i$ for the $k - 1$ given arguments. By construction, these p possible polynomials are equally likely, and thus there is absolutely nothing that these $k - 1$ participants can deduce about the real value of K .

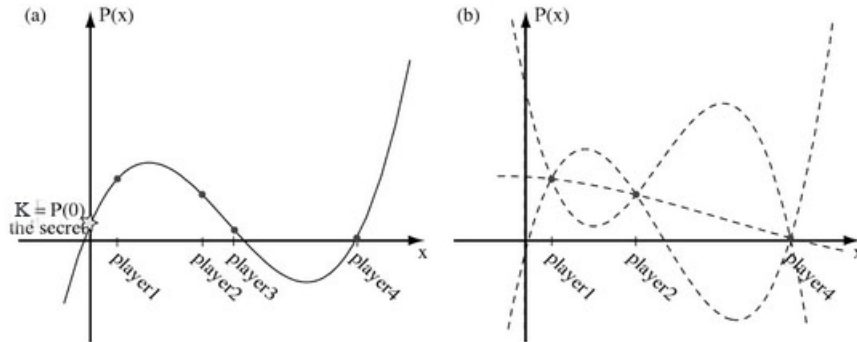


Figure 4.1: Shamir $(4, n)$ threshold secret sharing scheme. (a) Four player can collaborate to recover the original third degree polynomial $P(x)$. (b) Three players can get infinitely many solutions of the polynomial hence cannot retrieve the secret [2].

4.1.2 Blakley Scheme

Blakley's approach to reconstruct the secret key was based on hyperplane geometry [81]. To carry out a (k, n) threshold scheme, the dealer distributes k dimensional hyperplane equations over a finite field to n participants. Each participant is in possession of a $k - 1$ -dimension subspace that passes through the secret key point. The key can be reconstructed from the intersection of k or more hyperplanes whilst the intersection of $k - 1$ or less hyperplanes provides no information about the key as shown in Figure 4.2.

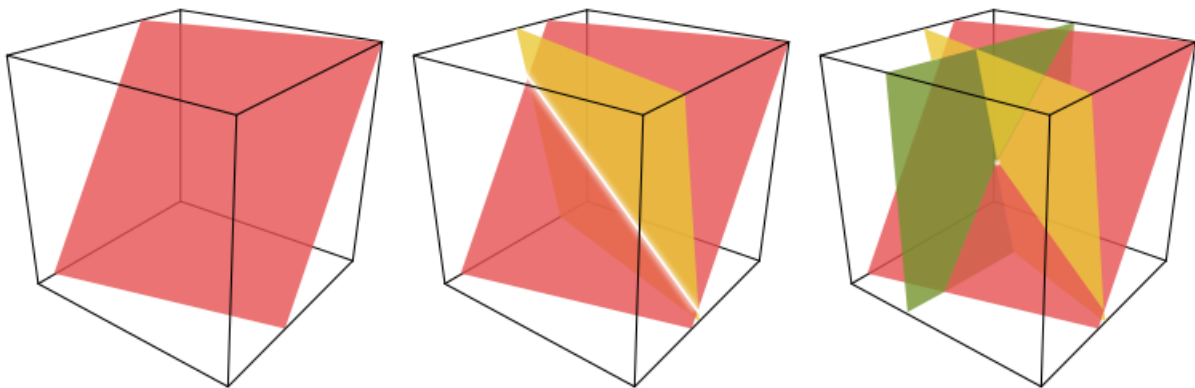


Figure 4.2: Blakley's scheme in three dimensions: each share is a plane, and the secret is the point at which three shares intersect. Two shares are insufficient to determine the secret, although they do provide enough information to narrow it down to the line where both planes intersect [3].

Secret sharing as depicted by the mathematical methods of Shamir and Blakley's schemes does not only preserve the resources required for its implementation but offer other several advantages. It can be noticed the size of the information distributed to participants does not exceed the secret and secondly the number of participants can be increased or reduced without affecting the secret and access structure. Moreover, the schemes are flexible in the sense that new shares can be redeveloped without altering the secret when it needs be. The only alteration is from formation of new polynomials and hyperplanes in the projective spaces. This dynamicity has led to the development of some new schemes with different approaches and applications. Among those are the proactive and verifiable schemes.

4.1.3 Proactive Secret Sharing (PSS)

The information security provided by secret sharing schemes may become inadequate in case the secret is stored for a long time. For example, protection of long lived information such as legal documents or cryptographic master keys. Storing the secret for longer period

provide the adversary with enough time to attack the shareholders and obtain the secret. This situation can be dealt with using PSS in which shares are refreshed periodically without compromising the secrecy of the shares. The main advantages of PSS are that shares are constantly renewed such that even if the adversary can learn the information about the old shares the secret is still remain unaffected. Lost or corrupted shares can be recovered without compromising the secrecy of the shares [84].

In general the proactive secret sharing works as follows; the lifetime of secret is split in specific time periods e.g a week or a month. The share generation protocol is employed to obtain a new shares. Each shareholder is engaged in an interactive update protocol, after which they hold completely new shares of the same secret. The old shares are no longer valid and can be discarded. Consequently, in the case of a $(k + 1, n)$ proactive threshold scheme, the adversary needs to at least obtain information from $(k + 1)$ shareholders during a reduced time period, as opposed to incrementally colluding with $(k + 1)$ shareholder over the entire secret life-time. Similarly, the destruction of the secret requires the adversary to corrupt $n - k$ shares in a single time period.

4.1.4 Verifiable Secret Sharing (VSS)

VSS is an important element of distributed secret sharing protocols involving untrusted participants because the protocols essentially involve each server acting as a semi-trusted dealer to all of the others [85]. The objective of VSS is to detect any dishonest participant in cases such as;

- a dealer sending incorrect shares to some or all of the participants, or
- participants submitting incorrect shares during the reconstruction protocol.

Consider a VSS protocol among n players $P = \{P_1, P_2, \dots, P_n\}$, with a selected player $D \in P$ working as a dealer. The protocol consists of two stages: a sharing stage and a reconstruction stage. Initially, D holds an input S , denoting the secret, and each player P_i may hold an independent random input r_i . The sharing stage may involves several rounds of interaction between players. At the end of the sharing stage, each honest player P_i holds a share s_i that may be required to reconstruct the dealer's secret. To reconstruct the secret, each player P_i publishes its entire share s_i from the sharing stage, and a reconstruction function $Rec(s_1, \dots, s_n)$ is applied and is taken as the protocol's output. A (k, n) VSS protocol satisfy the following conditions;

- If D is honest then the adversary's view during the sharing stage reveals no information about S . In particular, the adversary's view is identically distributed for all different

values of S .

- If D is honest then the honest players output the secret S at the end of the reconstruction stage.
- If D is dishonest, then at the end of the sharing stage there exists a value $S^* \in F_p$, such that at the end of the reconstruction stage all honest players output S^* . The F_p is the field in which secret S lies [86].

4.1.5 Applications of Secret Sharing

Secure Access to Corporate Funding

The restricted access to secret information makes secret sharing suitable for applications in securing corporate funds. For instance, if a financial organisation wants to secure money in one of its accounts, it can use the threshold secret sharing scheme to share account access code among authorised employees. Certain number of employees have to collaborate to access the funds and this reduces the chances of money being stolen by a particular individual or small group of individuals [2].

Electronic Voting

The privacy of electronic voting can be accomplished through secret sharing. The protocol can be explained as follows; Initially the voters needs to split their vote into k shares and distribute them to tallying authorities. Upon receiving the shares, the tallying authorities have verify the identity and the distinctiveness of the voter and no tallying authority can obtain the information about who has been voted. These tallying authorities have to count their partial votes independently and send their results to the central authority. The central authority will then combine the shares to get the results for the votes [87, 88].

Distributed Signatures

The (t, n) threshold secret sharing can be adopted for signing of a message by many co-signers, where t corresponds to the access structure. The signing key is distributed among the co-signers and no single participant know the complete signing key but needs to collaborate with at least $t - 1$ co-signers [89]. More details on threshold signatures is given in [90].

4.2 Quantum Secret Sharing

As already indicated in the previous sections, secret sharing serves vital role in securing classical information. Therefore, the principles used in classical schemes can be inherited in the realm of quantum computation to secure quantum information. A perfect quantum secret sharing (QSS) scheme has the access structure or an authorized set, which comprises of the participants holding all the shares required for reconstructing the original secret, and an unauthorized set, made up of participants who cannot acquire information at all about the secret quantum state (that is, the density matrix of an unauthorized set is the same for all encoded states) [91]. The properties of classical schemes still hold for QSS schemes. For instance, any secret sharing scheme must be monotonic. This means if we increase the size of a set, it cannot switch from authorized to unauthorized. The only other property that needs to be satisfied in QSS schemes is the no-cloning theorem [67]. It prohibits us from making two copies of an unknown quantum state. Therefore, we cannot distribute the shares of QSS scheme into two disjoint authorized sets (each of which could produce a copy of the original state). Since every set is either authorized or unauthorized, this implies the complement of an authorized set is always an unauthorized set. This imposes the limitation $n/2 < k < n$ on threshold QSS and as a result more participants have to collude to reconstruct the secret.

In quantum information processing, the information is distributed in the form of quantum states to agents, hence it is referred to as quantum state sharing (QSTS). Various protocols of QSTS have been realized both experimentally and theoretically. These protocols exploit various quantum resources such as entangled states to distribute an arbitrary single particle, two particle and multiple particle state. The mainly used entangled states are the Bell states and the GHZ states. The first work in quantum state sharing was proposed by Hilery et al [17] who used three and four particle GHZ states to distribute private message to two and three agents respectively. Since then, there has been noticeable progress in researches on QSTS [92–100] .

4.2.1 Applications of QSTS

Quantum Information Networks

Quantum information networks which are analogy to internet comprises of atomic nodes where quantum states are stored and processed. The optical channels are used for transmission of the quantum information between the nodes. Quantum state sharing allows many nodes to cooperate on a specific computing problem as in distributed computing [106]. A problem is divided into many tasks each of which is solved by one or more nodes in the

network. For instance, if the Shor's algorithm is used to crack a code, this can be achieved through distribution of the partial results of the algorithm to each node where they are processed. The access structure can reunite, and with less computing power complete the Shor's algorithm to crack the code [2].

Quantum Error Correction

Quantum states are shared by multiple nodes in quantum information networks. These networks are vulnerable to loss or destruction of quantum states caused by de-coherence or atomic nodes and channel failures. The state is thus robust against any errors that may occur to some shares in the channel as it can be reconstructed from the remaining shares [107].

Chapter 5

Reference Frame Independent QKD Protocol

In this chapter the security proof for a three party QKD protocol is derived. The same procedures used for security proofs of BB84 protocol against the collective attacks in [23, 108, 109] are used in the analysis. In particular, we derive the lower bound on the bit error rate for the rfi scheme under one way classical post-processing.

5.1 Reference Frame Independent Protocol

In QKD, a qubit of information can be encoded in the polarization degrees of freedom, and the linear superpositions required by QKD can be easily produced with polarization rotators. However, QKD protocols using photon polarization requires the alignment of reference frames between communicating parties. This should be considered an extra resource required by the protocol in cases where either Alice or Bob (or both) are based on a moving station such as a satellite [110, 111]. In this case they must continually monitor and control this alignment.

It has been shown that classical and quantum information can be transmitted without a shared reference frame using entangled states of photons. However, these photons are very difficult to generate and are very sensitive to losses [112]. Another implementation of QKD is obtained through phase coding. Though the alignment between the sender and the receiver is not requirement, the complexity in the analysis of this protocol lies in the fact that a photon contribute to more than one bits. Moreover, the protocol requires interferometric stability, which deems it not suitable for ground to satellite implementations where the optical path between sender and receiver will be affected by the satellite movement and by atmospheric variations. Reference frame independent(rfi) QKD protocols addresses all these above problems such as the alignment limitations in standard protocols as it can be

implemented without any alignment between the sender and the receiver. The rfi QKD protocol has applications, for example, in path encoded chip to chip QKD [113, 114] and earth to satellite QKD [115, 116].

The rfi QKD protocols have been proposed using two qubit sources where the key is generated between the two parties. In this chapter, we propose a novel rfi QKD protocol for three qubit source. In this protocol Alice and her communicating parties Bob and Charlie share a common aligned measurement basis $Z = Z_a = Z_b = Z_c$ whilst other measurements basis X and Y are allowed to slowly vary by an arbitrary angle β . The X, Y, Z stands for Pauli matrices. The other measurements basis are given by

$$X_B = \cos \beta X_A + \sin \beta Y_A,$$

$$X_C = \cos \beta X_A + \sin \beta Y_A,$$

$$Y_B = \cos \beta Y_A + \sin \beta X_A,$$

$$Y_C = \cos \beta Y_A + \sin \beta X_A.$$

5.1.1 Operation of the Protocol

We start by describing the entanglement based protocol which is equivalent to prepare and measure protocols. In our protocol Alice prepares N GHZ states $|\phi\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{A_i B_i C_i}$ and randomly perform the Hadamard transform on the system B_i and C_i . She then sends the GHZ states to Bob and Charlie who then randomly apply the Hadamard operation on the received qubits. The density matrix describing their system is three qubit state, ρ_{ABC} . Alice, Bob and Charlie selects some of the GHZ states as the check qubits. They measure their qubits in the Z basis and compare the measurement results via classical channels. The random sampling theorem shows that untested qubits have asymptotically the same bit error rates as check qubits with high probability. Therefore the phase error rate on the encoded qubits is asymptotically equal to bit flip error rate on encoded qubits. After estimating the error rates, Alice, Bob and Charlie computes bit and phase flips error syndromes to obtain nearly perfect GHZ states. Finally, Alice, Bob and Charlie randomly chooses one of the three directions to measure their particles. At the end of qubits exchange procedure they reveal their bases. The raw key is extracted from the cases where they both measured in the Z direction. Hence the quantum bit error rate is given by

$$Q = \frac{1 - \langle Z_A Z_B Z_C \rangle}{2}. \quad (5.1)$$

The other measurement results are used to estimate the information that has leaked to Eve. The quantity, C is used to estimate the bound on Eve's knowledge of the key. It is given by

$$C = \langle X_A X_B X_C \rangle^2 + \langle X_A Y_B X_C \rangle^2 + \langle X_A X_B Y_C \rangle^2 + \langle Y_A X_B X_C \rangle^2 + \langle Y_A Y_B X_C \rangle^2 + \langle Y_A X_B Y_C \rangle^2 + \langle Y_A Y_B Y_C \rangle^2 + \langle X_A Y_B Y_C \rangle^2. \quad (5.2)$$

It can be easily shown that C is independent of the value β when substituting the relations X_B , Y_B and X_C , Y_C in Equation 5.2. However, in order to get accurate estimate of C , the angle β is assumed to be vary slowly in time short enough to allow for exchange of key. For maximal entangled states, C can attain the maximal value of 2, the case where $Q = 0$.

5.1.2 Security Analysis

To compute the error bound, we consider collective attacks where Eve applies the same attack to each system of Alice, Bob and Charlie. The state shared by Alice, Bob and Charlie is Bell diagonal for those attacks and is written as

$$\rho_{ABC} = \mu_1 |\phi^+\rangle\langle\phi^+| + \mu_2 |\phi^-\rangle\langle\phi^-| + \mu_3 |\psi^+\rangle\langle\psi^+| + \mu_4 |\psi^-\rangle\langle\psi^-| + \mu_5 |\Phi^+\rangle\langle\Phi^+| + \mu_6 |\Phi^-\rangle\langle\Phi^-| + \mu_7 |\Psi^+\rangle\langle\Psi^+| + \mu_8 |\Psi^-\rangle\langle\Psi^-|. \quad (5.3)$$

Based on the fact that C is invariant under the following transformations $X_A \rightarrow -X_A$, $X_B \rightarrow -X_B$, $X_C \rightarrow -X_C$, $Y_A \rightarrow -Y_A$, $Y_B \rightarrow -Y_B$, $Y_C \rightarrow -Y_C$ and as a result the state ρ_{ABC} can be written as a mixture. ρ_{ABC} remains unchanged if we apply Z rotations on it. This implies that it can be written as

$$\tilde{\rho} = \frac{1}{2}(\rho + Z_A Z_B Z_C \rho Z_A Z_B Z_C). \quad (5.4)$$

This can be explicitly written as

$$\begin{aligned} \rho_{ABC} = & \mu_1 |\phi^+\rangle\langle\phi^+| + \mu_2 |\phi^-\rangle\langle\phi^-| + \left(\frac{a}{2} |\phi^-\rangle\langle\phi^+| + H.c\right) + \mu_3 |\psi^+\rangle\langle\psi^+| + \mu_4 |\psi^-\rangle\langle\psi^-| + \\ & \left(\frac{b}{2} |\psi^-\rangle\langle\psi^+| + H.c\right) + \mu_5 |\Phi^+\rangle\langle\Phi^+| + \mu_6 |\Phi^-\rangle\langle\Phi^-| + \left(\frac{c}{2} |\Phi^-\rangle\langle\Phi^+| + H.c\right) + \mu_7 |\Psi^+\rangle\langle\Psi^+| + \\ & \mu_8 |\Psi^-\rangle\langle\Psi^-| + \left(\frac{d}{2} |\Psi^-\rangle\langle\Psi^+| + H.c\right). \end{aligned} \quad (5.5)$$

For ease of notation, let us denote this state as $\tilde{\rho}(a, b, c)$. This yields $C = 2[(\mu_1 - \mu_2)^2 + (\mu_3 - \mu_4)^2 + (\mu_5 - \mu_6)^2 + (\mu_7 - \mu_8)^2 + Im(a)^2 + Im(b)^2 + Im(c)^2 + Im(d)^2]$. This results are also attained for $\rho(-a^*, -b^*, -c^*)$. By using the same logic, we can intuitively analyse the

mixture of $\rho' = \frac{1}{2}[\tilde{\rho}(a, b, c) + \tilde{\rho}(-a^*, -b^*, -c^*)]$ to obtain the value of C . The state ρ' can be express as;

$$\rho' = \sum_{n=1}^8 \lambda_n |\Phi\rangle \langle \Phi_n|, \quad (5.6)$$

where $|\Phi_{1,2}\rangle = \frac{1}{2\sqrt{2}}(\exp i\chi|000\rangle \pm \exp -i\chi|111\rangle)$, $|\Phi_{3,4}\rangle = \frac{1}{2\sqrt{2}}(\exp i\chi|001\rangle \pm \exp -i\chi|100\rangle)$, $|\Phi_{5,6}\rangle = \frac{1}{2\sqrt{2}}(\exp i\chi|010\rangle \pm \exp -i\chi|101\rangle)$ and $|\Phi_{7,8}\rangle = \frac{1}{2\sqrt{2}}(\exp i\chi|011\rangle \pm \exp -i\chi|100\rangle)$. The parameters are related as follows; let $A' = \sqrt{(\mu_1 - \mu_2)^2 + A^2}$: $\lambda_{1,2} = \frac{1}{8}(\mu_1 + \mu_2 \pm A')$, $B' = \sqrt{(\mu_1 - \mu_2)^2 + B^2}$, $\lambda_{3,4} = \frac{1}{8}(\mu_3 + \mu_4 \pm B')$. The expressions for other eigenvalues and imaginary parts are calculated in similar manner. This yields the value of C given by;

$$C = 2[(\lambda_1 - \lambda_2)^2 + (\lambda_3 - \lambda_4)^2 + (\lambda_5 - \lambda_6)^2 + (\lambda_7 - \lambda_8)^2]. \quad (5.7)$$

For collective attacks the secret key rate is given by

$$r = 1 - h(Q) - I_E(Q, C). \quad (5.8)$$

To estimate Eve's information, I_E , the coefficients λ_i have to satisfy the condition: $\sum \lambda_i = 1$ and yield the measured values Q and C . Since the states are measured in the computational basis this implies

$$\begin{aligned} \lambda_1 + \lambda_2 &= 1 - Q, \\ \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 &= Q. \end{aligned}$$

The following parametrization is chosen so as to satisfies the above conditions.

$$\begin{aligned}
\lambda_1 &= (1 - Q) \left(\frac{1 + u}{2} \right), \\
\lambda_2 &= (1 - Q) \left(\frac{1 - u}{2} \right), \\
\lambda_3 &= \frac{1}{3} Q \left(\frac{1 + v}{2} \right), \\
\lambda_4 &= \frac{1}{3} Q \left(\frac{1 - v}{2} \right), \\
\lambda_5 &= \frac{1}{3} Q \left(\frac{1 + v}{2} \right), \\
\lambda_6 &= \frac{1}{3} Q \left(\frac{1 - v}{2} \right), \\
\lambda_7 &= \frac{1}{3} Q \left(\frac{1 + v}{2} \right), \\
\lambda_8 &= \frac{1}{3} Q \left(\frac{1 - v}{2} \right),
\end{aligned}$$

where $u, v \in [0, 1]$ are subject to the additional constraint

$$(1 - \varepsilon_z)u + \varepsilon_z v = \varepsilon_x + \varepsilon_y. \quad (5.9)$$

The ε_z , ε_x and ε_y are the quantum bit error rates (QBER) associated with the measurements on the Z basis, X basis and Y basis respectively. Under the assumption of the depolarizing channel, $\varepsilon_z = \varepsilon_x = \varepsilon_y = Q$, this becomes

$$(1 - Q)\frac{u}{2} + Q\frac{v}{2} = Q \quad (5.10)$$

Under this parametrization,

$$H(\underline{\lambda}) = h(Q) + (1 - Q)h(u) + Qh(v)$$

The parameter C is calculated as below:

$$\begin{aligned}
C &= \left[2(1-Q) \left(\frac{1+u}{2} - \frac{1-u}{2} \right) \right]^2 + \left[\frac{2}{3}Q \left(\frac{1+v}{2} - \frac{1-v}{2} \right) \right]^2 \\
&\quad + \left[\frac{2}{3}Q \left(\frac{1+v}{2} - \frac{1-v}{2} \right) \right]^2 + \left[\frac{2}{3}Q \left(\frac{1+v}{2} - \frac{1-v}{2} \right) \right]^2 \\
&= 2 \left[(1-Q)^2 u^2 + \frac{1}{3}Q^2 v^2 \right]. \tag{5.11}
\end{aligned}$$

Eve's information, I_E , is given by the Holevo Bound, $I_E = S(\rho_E) - \frac{1}{2}S(\rho_{E|0}) - \frac{1}{2}S(\rho_{E|1})$. Eve hold purification of the state shared by Alice, Bob and Charlie, therefore this implies $S(\rho_E) = S(\rho_{ABC}) = H(\underline{\lambda})$. To compute $S(\rho_{E|b})$, $b \in [0, 1]$ we trace out Bob and Charlie from the state $|\Psi\rangle_{ABCE}$ and project Alice on $|+z\rangle$ for $b = 0$ and on $|-z\rangle$ for $b = 1$. Since both

$S(\rho_{E|0})$ and $S(\rho_{E|1})$ can occur with equal probability we obtain $S(\rho_{E|0}) = S(\rho_{E|1}) = h(Q)$.

$$\begin{aligned}
H(\lambda) = & (1-Q) \left(\frac{1+u}{2} \right) \log(1-Q) \left(\frac{1+u}{2} \right) + (1-Q) \left(\frac{1-u}{2} \right) \log(1-Q) \left(\frac{1-u}{2} \right) \\
& + \frac{Q}{3} \left(\frac{1+v}{2} \right) \log \frac{Q}{3} \left(\frac{1+v}{2} \right) + \frac{Q}{3} \left(\frac{1-v}{2} \right) \log \frac{Q}{3} \left(\frac{1-v}{2} \right) + \frac{Q}{3} \left(\frac{1+v}{2} \right) \log \frac{Q}{3} \left(\frac{1+v}{2} \right) \\
& + \frac{Q}{3} \left(\frac{1-v}{2} \right) \log \frac{Q}{3} \left(\frac{1-v}{2} \right) + \frac{Q}{3} \left(\frac{1+v}{2} \right) \log \frac{Q}{3} \left(\frac{1+v}{2} \right) + \frac{Q}{3} \left(\frac{1-v}{2} \right) \log \frac{Q}{3} \left(\frac{1-v}{2} \right)
\end{aligned} \tag{5.12}$$

$$\begin{aligned}
= & (1-Q) \left[\left(\frac{1+u}{2} \right) \log \left(\frac{1+u}{2} \right) + \left(\frac{1-u}{2} \right) \log \left(\frac{1-u}{2} \right) \right] \\
& + \log(1-Q) \left[(1-Q) \left(\frac{1+u}{2} \right) + (1-Q) \left(\frac{1-u}{2} \right) \right] \\
& + \log \left(\frac{Q}{3} \right) \left[\frac{Q}{3} \left(\frac{1+v}{2} \right) + \frac{Q}{3} \left(\frac{1-v}{2} \right) \right] \\
& + \frac{Q}{3} \left[\left(\frac{1+v}{2} \right) \log \left(\frac{1+v}{2} \right) + \left(\frac{1-v}{2} \right) \log \left(\frac{1-v}{2} \right) \right] \\
& + \log \left(\frac{Q}{3} \right) \left[\frac{Q}{3} \left(\frac{1+v}{2} \right) + \frac{Q}{3} \left(\frac{1-v}{2} \right) \right] + \frac{Q}{3} \left(\frac{1+v}{2} \right) \\
& + \frac{Q}{3} \left[\left(\frac{1-v}{2} \right) \log \left(\frac{1-v}{2} \right) + \left(\frac{1+v}{2} \right) \log \left(\frac{1+v}{2} \right) \right] \\
& + \log \left(\frac{Q}{3} \right) \left[\frac{Q}{3} \left(\frac{1-v}{2} \right) + \frac{Q}{3} \left(\frac{1+v}{2} \right) \right] \\
& + \frac{Q}{3} \left[\left(\frac{1-v}{2} \right) \log \left(\frac{1-v}{2} \right) + \left(\frac{1+v}{2} \right) \log \left(\frac{1+v}{2} \right) \right]
\end{aligned} \tag{5.13}$$

$$\begin{aligned}
= & (1-Q) \left[\left(\frac{1+u}{2} \right) \log \left(\frac{1+u}{2} \right) + \left(\frac{1-u}{2} \right) \log \left(\frac{1-u}{2} \right) \right] \\
& + Q \left[\left(\frac{1+v}{2} \right) \log \left(\frac{1+v}{2} \right) + \left(\frac{1-v}{2} \right) \log \left(\frac{1-v}{2} \right) \right] \\
& + (1-Q) \left[\left(\frac{1+u}{2} \right) \log(1-Q) + \left(\frac{1-u}{2} \right) \log(1-Q) \right] \\
& + Q \left[\left(\frac{1+v}{2} \right) \log \frac{Q}{3} + \left(\frac{1-v}{2} \right) \log \frac{Q}{3} \right]
\end{aligned} \tag{5.14}$$

$$= h(Q) + (1-Q)h \left(\frac{1+u}{2} \right) + Qh \left(\frac{1+v}{2} \right) - Q \log 3, \tag{5.15}$$

where $h(x)$ is the Shannon entropy function. This yields the following results for Eve's

information bound.

$$\begin{aligned}
I_E(Q, u, v) &= S(\rho_E) - \frac{1}{2}S(\rho_{E|0} - \frac{1}{2}(\rho_{E|1}) \\
&= h(Q) + (1-Q)h\left(\frac{1+u}{2}\right) + Qh\left(\frac{1+v}{2}\right) - Q\log 3 - h(Q) \\
&= (1-Q)h\left(\frac{1+u}{2}\right) + Qh\left(\frac{1+v}{2}\right) - Q\log 3.
\end{aligned} \tag{5.16}$$

To compute

$$I_E(Q, C) = \max_C I_E(Q, u, v), \tag{5.17}$$

we consider the fact that $C = 2[(1-Q)^2u^2 + \frac{1}{3}Q^2v^2]$, $u_{\min} = \frac{\sqrt{(C/2 - \frac{1}{3}Q^2)}}{1-Q}$, $u_{\max} = \frac{\sqrt{C/2}}{1-Q}$ and when $Q \leq 15.9\%$, Eve's information is bounded by

$$I_E(Q, C) = I_E(Q, u_{\max}, v(u_{\max})). \tag{5.18}$$

To compute the secret key rate we consider the case of depolarising channel which gives rise to Werner states [117]. For Werner states $C = (1-2Q)^2$ which gives;

$$I_E(Q) = (1-Q)h\left(\frac{1-3Q/2}{1-Q}\right) + Q - Q\log 3. \tag{5.19}$$

The corresponding secret key rate is therefore derived to be;

$$r = 1 - h(Q) - (1-Q)h\left(\frac{1-3Q/2}{1-Q}\right) - Q + Q\log 3. \tag{5.20}$$

The highest tolerable error rate Q can be obtained for the worst case value of the key generation rate r and hence given by the solution to the equation;

$$1 - h(Q) - (1-Q)h\left(\frac{1-3Q/2}{1-Q}\right) - Q + Q\log 3 = 0. \tag{5.21}$$

By making use of the definition of binary entropy, we get

$$\begin{aligned}
&1 + Q\log Q + (1-Q)\log(1-Q) - (1-Q)\left(-\left(\frac{1-3Q/2}{1-Q}\right)\log\left(\frac{1-3Q/2}{1-Q}\right)\right) \\
&- \left(\frac{Q/2}{1-Q}\right)\log\left(\frac{Q/2}{1-Q}\right) - Q + Q\log 3 = 0.
\end{aligned} \tag{5.22}$$

By solving this equation yields $Q \approx 0.18$ which is the lower bound on the bit error rate for

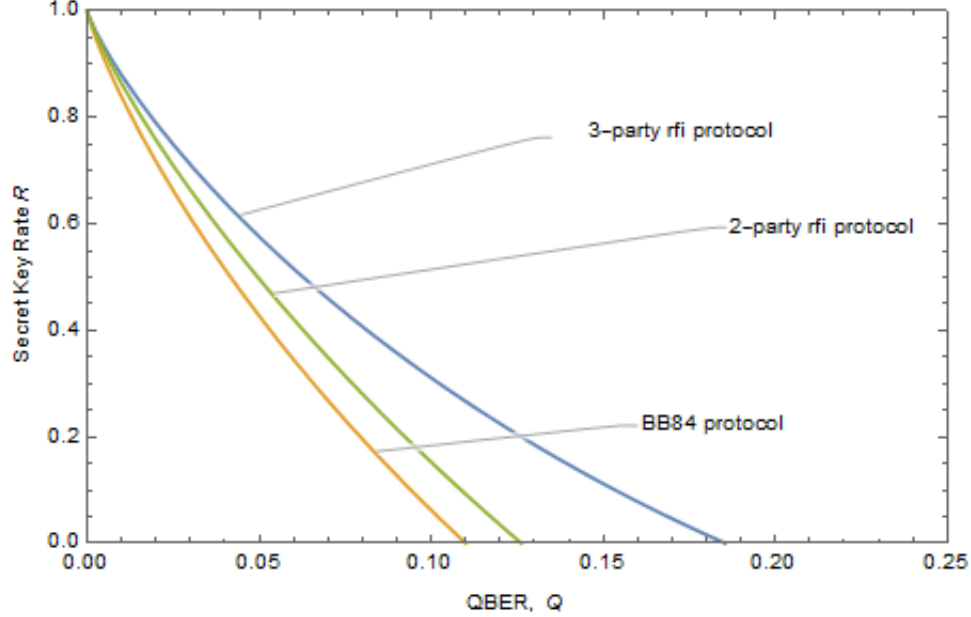


Figure 5.1: Comparison between the secret key rate of the BB84 protocol [48], 2-party rfi protocol [23] and our proposed 3-party rfi protocol.

the reference frame independent scheme under one-way classical postprocessing. Alice, Bob and Charlie cannot generate a key if the error rate, Q exceeds this value. The communicating parties will have to restart the key distribution procedure again until they obtain an error rate less than this bound, where Eve's information is considered to be negligible to obtain full knowledge of the key. In this work for the first time, we attempted to increase the number of communicating parties to three, and the obtained QBER shows a degradation as compared with existing error bounds obtained from two party protocols. For instance, an error bound of 12.62% was obtained for the security proof of QKD with BB84 by Laing et al [23] and the well known error bound of 11.0% BB84 protocol was obtained by Shor et al [48] for the defined reference frames. The secret key rate of BB84 protocol by Shor et al was achieved using the Calderbank-Shor-Steane (CSS) quantum error correcting codes and entanglement purification protocol. Our proposed protocol uses similar operations and methods as the Laing et al protocol but only differ in the number of communicating parties involved. The secret key rate for our protocol was derived using entanglement based protocol under one way classical post-processing. The key was extracted only from measurements in the Z basis and Eve's information was given by the Holevo Bound. The results of these three protocols are shown in figure 5.1. Though the protocol is not efficient enough to reduce the amount of information available to Eve, there is still a potential that a better key rate can be obtained from communication involving three parties if other approaches are employed. Our

protocol was based on the case where the quantum signal is a single qubit and on perfect devices used by communicating parties which is not practical in realization. However, high performing two party rfi protocols have been obtained taking into account the imperfections in the quantum channel.

Chapter 6

Security Proof of a Generic Three Party QKD Protocol

We present a security proof for a three party generic QKD protocol which makes use of the GHZ states. The protocol requires only single particle measurements by communicating parties and uses one-way information reconciliation and privacy amplification to obtain a secret key. We use the tools and techniques used recently by Christandl et al [31] to calculate the error bound for our protocol.

6.1 Operation of the Protocol

In our protocol Alice prepares N GHZ states $|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}$ and send the other particles to Bob and Charlie. The density matrix describing their system is a three qubit state, ρ . The three parties choose some of the GHZ states as the test qubits. They carry out measurements on their particles using either standard basis or Hadamard basis. The $\langle 001|\rho|001\rangle$ denotes the probability that Alice results is 0, Bob's result is 0 and Charlie's results is 1 when they measured on the standard basis. Similarly, $|+\rangle$ represent the result 0 and $|-\rangle$ represent the result 1. The communicating parties publicly announces their results. Their bases are compared and any photon which were processed using non correlating bases are discarded.

6.2 Security Analysis

In this section we begin by describing some vital information aspects involved in the QKD. A key measure of information is entropy, which is usually expressed by the average number

of bits needed to store or communicate one symbol in a message. Entropy quantifies the uncertainty involved in predicting the value of a random variable [32]. Shannon defined the entropy of a discrete random variable $\{X\}$, which we denote by $H(X)$ as

$$H(X) = E[\log_2(p(X))] = - \sum_x p(x) \log_2 p(x), \quad (6.1)$$

where X is a discrete random variable, whose possible values x are drawn from the probability distribution $p(x)$. Another Shannon's entropy quantity is the mutual information which measures the how much information is contained in both variables,

$$I(X : Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = I(Y : X). \quad (6.2)$$

Suppose Alice, Bob and Charlie's qubit systems are described by three random variables X , Y and Z respectively. The mutual information gives the degree of correlations between the bit strings shared between the parties,

$$I(X : Y : Z) = I(X : Y) - I(X : Y|Z) \quad (6.3)$$

$$= H(X) - H(X|Y) - [H(X|Z) - H(X|Y, Z)]. \quad (6.4)$$

The strings of Alice, Bob and Charlie can be made almost identical through information reconciliation. Alice has to announce in public $H(X|Y, Z)$ bits about her strings so that Bob and Charlie who holds Y and Z can guess Alice's string correctly.

The entropy for Alice's strings X is $H(X) = 1$ and the conditional entropies represent the amount of information that leaked to Eve and is given by $H(X|Y) - [H(X|Z) - H(X|Y, Z)] = h(\epsilon)$. The $h(\epsilon)$ is the binary entropy given by $h(\epsilon) = -\epsilon \log \epsilon - (1 - \epsilon) \log(1 - \epsilon)$, where ϵ is the average bit error rate.

Let describe the outcomes of all projective measurements on ρ with random variable V . The von Neumann entropy can be approximated by $H(V) \geq S(\rho)$. One can compute the unconditional security bound by restricting consideration to all collective attacks such that the final state of Alice, Bob and Charlie is Bell diagonal,

$$\begin{aligned} \rho_{ABC} = & \lambda_1 |\phi^+\rangle \langle \phi^+| + \lambda_2 |\phi^-\rangle \langle \phi^-| + \lambda_3 |\psi^+\rangle \langle \psi^+| + \lambda_4 |\psi^-\rangle \langle \psi^-| + \lambda_5 |\Phi^+\rangle \langle \Phi^+| + \lambda_6 |\Phi^-\rangle \langle \Phi^-| \\ & + \lambda_7 |\Psi^+\rangle \langle \Psi^+| + \lambda_8 |\Psi^-\rangle \langle \Psi^-|, \end{aligned} \quad (6.5)$$

where the GHZ states are defined as

$$\begin{aligned}
|\psi^+\rangle_1 &= \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \\
|\psi^+\rangle_1 &= \frac{1}{4}(|+++\rangle + |+-\rangle + |-+-\rangle + |--+\rangle) \\
|\psi^-\rangle_2 &= \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \\
|\psi^-\rangle_2 &= \frac{1}{4}(|-++\rangle - |+-\rangle - |+-\rangle + |--\rangle) \\
|\Psi^+\rangle_3 &= \frac{1}{2\sqrt{2}}(|011\rangle + |100\rangle) \\
|\Psi^+\rangle_3 &= \frac{1}{4}(|+++\rangle + |+-\rangle - |-+-\rangle - |--+\rangle) \\
|\Psi^-\rangle_4 &= \frac{1}{2\sqrt{2}}(|011\rangle - |100\rangle) \\
|\Psi^-\rangle_4 &= \frac{1}{4}(|-++\rangle - |+-\rangle - |+-\rangle + |--\rangle) \\
|\phi^+\rangle_5 &= \frac{1}{2\sqrt{2}}(|101\rangle + |010\rangle) \\
|\phi^+\rangle_5 &= \frac{1}{4}(|+++\rangle - |+-\rangle + |-+-\rangle - |--+\rangle) \\
|\phi^+\rangle_6 &= \frac{1}{2\sqrt{2}}(|101\rangle - |010\rangle) \\
|\phi^-\rangle_6 &= \frac{1}{4}(|+-\rangle - |+-\rangle - |-+-\rangle + |--\rangle) \\
|\varphi^+\rangle_7 &= \frac{1}{2\sqrt{2}}(|001\rangle + |110\rangle) \\
|\varphi^+\rangle_7 &= \frac{1}{4}(|+++\rangle - |+-\rangle - |-+-\rangle + |--+\rangle) \\
|\varphi^-\rangle_8 &= \frac{1}{2\sqrt{2}}(|001\rangle - |110\rangle) \\
|\varphi^-\rangle_8 &= \frac{1}{4}(|+-\rangle - |+-\rangle + |-+-\rangle - |--\rangle). \tag{6.6}
\end{aligned}$$

The probabilities of V as denoted by λ_i in terms of the probabilities of measurement in the basis one and basis two are:

$$\begin{aligned}
\lambda_1 &= \langle\psi^+|\rho|\psi^+\rangle = \langle+++\rho|+++\rangle + \langle+-\rho|+-\rangle + \langle-+-\rho|-+-\rangle + \langle--+\rho|--+\rangle \\
&\quad - 15\langle\phi^+|\rho|\phi^+\rangle \tag{6.7}
\end{aligned}$$

$$\lambda_2 = \langle \psi^- | \rho | \psi^- \rangle = \frac{1}{8} \langle ++- | \rho | +- \rangle + \langle +-+ | \rho | -+ \rangle + \langle -++ | \rho | -++ \rangle + \langle --- | \rho | --- \rangle \quad (6.8)$$

$$\lambda_3 = \langle \Psi^+ | \rho | \Psi^+ \rangle = \langle 001 | \rho | 001 \rangle + \langle 110 | \rho | 110 \rangle + \langle 100 | \rho | 100 \rangle + \langle 010 | \rho | 010 \rangle + \langle 101 | \rho | 101 \rangle - \langle \phi^+ | \rho | \phi^+ \rangle - \langle \Phi^+ | \rho | \Phi^+ \rangle \quad (6.9)$$

$$\lambda_4 = \langle \Psi^- | \rho | \Psi^- \rangle = \frac{1}{16} \langle +-+ | \rho | +- \rangle + \langle +- - | \rho | -- \rangle + \langle -++ | \rho | -++ \rangle + \langle -+- | \rho | -+- \rangle \quad (6.10)$$

$$\lambda_5 = \langle \phi^+ | \rho | \phi^+ \rangle = \frac{1}{16} \langle +++ | \rho | +++ \rangle + \langle +- - | \rho | -- \rangle + \langle -+- | \rho | -+- \rangle + \langle - - + | \rho | - - + \rangle \quad (6.11)$$

$$\lambda_6 = \langle \phi^- | \rho | \phi^- \rangle = \frac{1}{16} \langle ++- | \rho | +- \rangle + \langle +-+ | \rho | -+ \rangle + \langle -++ | \rho | -++ \rangle + \langle --- | \rho | --- \rangle \quad (6.12)$$

$$\lambda_7 = \langle \varphi^+ | \rho | \varphi^+ \rangle = \langle +++ | \rho | +++ \rangle + \langle +- - | \rho | -- \rangle + \langle -+- | \rho | -+- \rangle + \langle - - + | \rho | - - + \rangle - 15 \langle \phi^+ | \rho | \phi^+ \rangle \quad (6.13)$$

$$\lambda_8 = \langle \varphi^- | \rho | \varphi^- \rangle = \frac{1}{16} \langle ++- | \rho | +- \rangle + \langle +-+ | \rho | -+ \rangle + \langle -++ | \rho | -++ \rangle + \langle --- | \rho | --- \rangle \quad (6.14)$$

The symmetry error probability ϵ produces

$$\langle 000 | \rho | 000 \rangle + \langle 111 | \rho | 111 \rangle = 1 - \epsilon \quad (6.15)$$

$$\langle +++ | \rho | +++ \rangle + \langle +- - | \rho | -- \rangle + \langle -+- | \rho | -+- \rangle + \langle - - + | \rho | - - + \rangle = 1 - \epsilon \quad (6.16)$$

$$\begin{aligned} & \langle 001 | \rho | 001 \rangle + \langle 010 | \rho | 010 \rangle + \langle 100 | \rho | 100 \rangle + \langle 011 | \rho | 011 \rangle + \langle 101 | \rho | 101 \rangle \\ & + \langle 110 | \rho | 110 \rangle = \epsilon \end{aligned} \quad (6.17)$$

and inserting them into the above equations we obtain

$$\lambda_1 = (1 - \epsilon) - 15\lambda_5 \quad (6.18)$$

$$\lambda_3 + \lambda_4 = \frac{1}{16}\mathbf{I},$$

where $\mathbf{I}$ is the identity matrix, which implies;

$$\lambda_3 + \lambda_4 = \frac{1}{16}$$

Thus,

$$\lambda_1 + \lambda_2 + \lambda_5 + \lambda_6 + \lambda_7 + \lambda_8 = \frac{15}{16}$$

$$\lambda_1 = \lambda_7$$

$$\lambda_2 = \lambda_6 = \lambda_8$$

Substituting into equation 6.11 then we have

$$2\lambda_1 + 3\lambda_2 = \frac{15}{16}$$

$$\lambda_2 = \frac{15}{48} + \frac{\lambda_5}{3} - \frac{2\lambda_1}{3}$$

$$\lambda_2 = \frac{2}{3}\epsilon - \frac{17}{48} + \frac{29}{3}\lambda_5 \quad (6.19)$$

From equation 6.9 we can show that

$$\lambda_3 + \lambda_5 + \lambda_7 = \epsilon$$

Hence

$$\lambda_3 = \epsilon - \lambda_5 - \lambda_7$$

$$\lambda_3 = 2\epsilon - 14\lambda_5 - 1 \quad (6.20)$$

Then using equation 6.10 we get

$$\lambda_4 = \frac{17}{16} - 2\epsilon + 14\lambda_5 \quad (6.21)$$

$$\lambda_6 = \frac{2}{3}\epsilon - \frac{17}{48} + \frac{29}{3}\lambda_5 \quad (6.22)$$

$$\lambda_7 = (1 - \epsilon) - 15\lambda_5 \quad (6.23)$$

$$\lambda_8 = \frac{2}{3}\epsilon - \frac{17}{48} + \frac{29}{3}\lambda_5 \quad (6.24)$$

The lower bound on the secret key rate can be achieved by maximising $S(\rho)$ over all possible density operators ρ . Then it remains to find the value of free parameter λ_5 such that $H(V)$ is maximised. This is the case for $\lambda_5 = \frac{2}{15}\epsilon^2$.

The rate R of the protocol is given by

$$R = H(X) - H(X|Y) - [H(X|Z) - H(X|Y, Z)] - H(V). \quad (6.25)$$

$H(V)$ is given by $S(\rho) = -\sum \lambda_i \log \lambda_i$ and its explicit evaluation yields $H(V) = 4h(\epsilon)$. The security threshold is the highest value of ϵ such that the rate R is positive and therefore the solution to the equation $1 - 5h(\epsilon) = 0$. But $h(\epsilon)$ is the binary entropy hence,

$$\frac{1}{5} = -\epsilon \log_2 \epsilon - (1 - \epsilon) \log_2 (1 - \epsilon), \quad (6.26)$$

$$\frac{1}{5} \ln 2 = -\epsilon \ln \epsilon - (1 - \epsilon) \ln (1 - \epsilon). \quad (6.27)$$

By using approximation of $\epsilon = \frac{1}{8}$, we find that $\ln \epsilon = 8\epsilon - (1 + \ln \epsilon)$ and $\ln(1 - \epsilon) = -\frac{8}{7}\epsilon + (\frac{1}{7} - \ln \frac{8}{7})$.

We can simplify by using

$$\begin{aligned}\epsilon(a\epsilon + b) + c &= -(1 - \epsilon)[d\epsilon + \epsilon] \\ (a - d)\epsilon^2 + (b + d + \epsilon)\epsilon + c + \epsilon &= 0.\end{aligned}\tag{6.28}$$

By substitution yields

$$8\epsilon^2 - \epsilon(1 + \ln 8) + \frac{1}{5} \ln 2 = [-\frac{8}{7}\epsilon + (\frac{1}{7} - \ln \frac{8}{7})] + \frac{8}{7}\epsilon^2 - \epsilon(\frac{1}{7} - \ln \frac{8}{7}).\tag{6.29}$$

Solving the above equation we obtain $\epsilon \approx 0.031$ which corresponds to a 3.1% bit error rate. This is the upper bound of the quantum bit error rate (QBER) for which the key can be established. The bound obtained is better than the well known bound of 11% for the two party BB84 protocol [48] which implies the improvement in the security of the QKD.

Chapter 7

Multiparty QSTS of an Arbitrary Unknown Three Particle State with GHZ State Measurements

In this chapter, we propose a scheme for sharing an unknown three-particle quantum state to n agents by using Greenberger-Horne-Zeilinger (GHZ) states. Firstly, we introduce the five party quantum state sharing scheme of arbitrary three particle unknown quantum state, where Alice starts by sharing four GHZ entangled states with her four agents, and performs three GHZ state measurements on her particles followed by two single particle measurements on the Hadamard basis. One of the agents, Bob1, performs single measurement on her particle and the three other agents, each perform unitary transformations on their particles to recover the unknown state. Subsequently, we propose the generalized multiparty quantum state sharing scheme for an arbitrary three particle state.

7.1 Five Party QSTS of an Arbitrary Three Particle Unknown State using GHZ States

In our proposed scheme, Alice shares an arbitrary three particle of an unknown quantum state with four agents referred to as Bob1, Bob2, Bob3 and Bob4 as shown in the steps in Figure 7.1. Bob4 acts as the controller whilst the remaining three parties act as receivers of the unknown state. They each have to perform a unitary transformation to their particle to recover the state. The unknown quantum state is expressed as;

$$|\Psi\rangle_{x,y,z} = (a|000\rangle + b|011\rangle + c|101\rangle + d|001\rangle + e|110\rangle + f|010\rangle + g|100\rangle + h|111\rangle)_{xyz}, \quad (7.1)$$

where x, y and z are three particles in the state $|\Psi\rangle$ and a, b, c, d, e, f, g and h are complex numbers that satisfy the normalization condition

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 + |e|^2 + |f|^2 + |g|^2 + |h|^2 = 1. \quad (7.2)$$

For sharing an arbitrary three qubit state, Alice first shares four three-particle GHZ states with her four agents as indicated on the first block in Figure 7.1. Three particle GHZ states can be generalized as follows:

$$\begin{aligned} |\phi^\pm\rangle_{1,2} &= \frac{1}{2\sqrt{2}}(|000\rangle \pm |111\rangle) \\ |\varphi^\pm\rangle_{3,4} &= \frac{1}{2\sqrt{2}}(|011\rangle \pm |100\rangle) \\ |\Psi^\pm\rangle_{5,6} &= \frac{1}{2\sqrt{2}}(|101\rangle \pm |010\rangle) \\ |\Phi^\pm\rangle_{7,8} &= \frac{1}{2\sqrt{2}}(|001\rangle \pm |110\rangle). \end{aligned} \quad (7.3)$$

Without loss of generality, if we assume that all three-particle GHZ states prepared by Alice are

$$|\phi^+\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle), \quad (7.4)$$

then the whole system of 15 particles can be written as;

$$\begin{aligned} |\Phi\rangle_{xyz123456789101112} &= |\psi\rangle_{xyz} \otimes |\phi^+\rangle_{123} \otimes |\phi^+\rangle_{456} \otimes |\phi^+\rangle_{789} \otimes |\phi^+\rangle_{101112} \\ &= |\psi\rangle_{xyz} (a|000\rangle + b|011\rangle + c|101\rangle + d|001\rangle + e|110\rangle + f|010\rangle + g|100\rangle \\ &\quad + h|111\rangle)_{xyz} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{123} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{456} \\ &\quad \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{789} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{101112}. \end{aligned} \quad (7.5)$$

After Alice shares the four GHZ states with Bob1, Bob2, Bob3 and Bob4, they are in possession of particle 3, 6, 9 and 12 respectively whilst Alice retains other particles. She then applies the CNOT gate operation on four particles $x, y, 10$ and 11 . In this proposed scheme, x and y acts as control particles whilst 10 and 11 are target particles. We can write

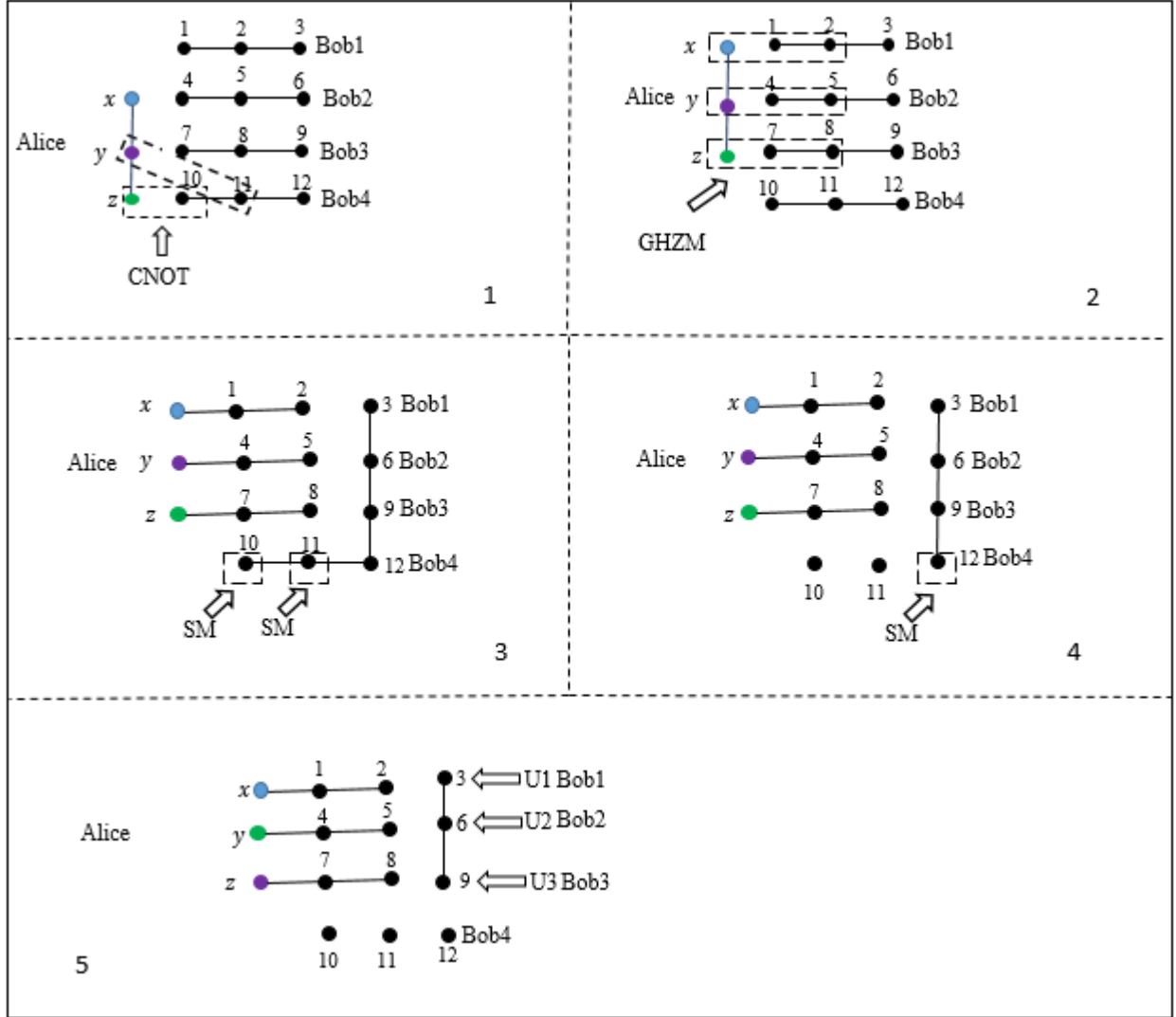


Figure 7.1: The steps for the proposed five party QSTS of unknown three particle quantum state. In 1 Alice starts by sharing 4 GHZ states with Bob1, Bob2, Bob3 and Bob4 and then performs a Controlled Not gate operation (CNOT) on particles $(y, 11)$, $(z, 10)$. In 2 Alice then carries out GHZ state measurement (GHZM) on particles $(x, 1, 2)$, $(y, 4, 5)$ and $(z, 7, 8)$. In 3 Alice executes single particle measurements (SM) on particle 10 and 11. In 4 Bob4 perform single particle measurement (SM) on particle 12. Finally, in 5 Bob1, Bob2 and Bob3 perform unitary operations (U_1 , U_2 and U_3) on their particles.

down the state of the whole 15 particle system as

$$\begin{aligned}
|\Psi\rangle = & (a|000000000000000\rangle + a|000000000000111\rangle + a|000000000111000\rangle + a|000000000111111\rangle \\
& + a|000000111000000\rangle + a|000000111000111\rangle + a|000000111111000\rangle + a|000000111111111\rangle \\
& + a|000111000000000\rangle + a|000111000000111\rangle + a|000111000111000\rangle + a|000111000111111\rangle \\
& + a|000111111000000\rangle + a|000111111000111\rangle + a|000111111111000\rangle + a|000111111111111\rangle \\
& + b|011000000000110\rangle + b|011000000000001\rangle + b|011000000111110\rangle + b|011000000111001\rangle \\
& + b|011000111000110\rangle + b|011000111000001\rangle + b|011000111111110\rangle + b|011000111111001\rangle \\
& + b|011111000000110\rangle + b|011111000000001\rangle + b|011111000111110\rangle + b|011111000111001\rangle \\
& + b|011111111000110\rangle + b|011111111000001\rangle + b|011111111111110\rangle + b|011111111111001\rangle \\
& + c|101000000000010\rangle + c|101000000000101\rangle + c|101000000111010\rangle + c|101000000111101\rangle \\
& + c|101000111000010\rangle + c|101000111000101\rangle + c|101000111111010\rangle + c|101000111111101\rangle \\
& + c|101111000000010\rangle + c|101111000000101\rangle + c|101111000111010\rangle + c|101111000111101\rangle \\
& + c|101111111000010\rangle + c|101111111000101\rangle + c|101111111111010\rangle + c|101111111111101\rangle \\
& + d|001000000000010\rangle + d|001000000000101\rangle + d|001000000111010\rangle + d|001000000111101\rangle \\
& + d|001000111000010\rangle + d|001000111000101\rangle + d|001000111111010\rangle + d|001000111111101\rangle \\
& + d|001111000000010\rangle + d|001111000000101\rangle + d|001111000111010\rangle + d|001111000111101\rangle \\
& + d|001111111000010\rangle + d|001111111000101\rangle + d|001111111111010\rangle + d|001111111111101\rangle \\
& + e|110000000000010\rangle + e|110000000000011\rangle + e|110000000111100\rangle + e|110000000111011\rangle \\
& + e|110000111000100\rangle + e|110000111000011\rangle + e|110000111111100\rangle + e|110000111111011\rangle \\
& + e|110111000000100\rangle + e|110111000000011\rangle + e|110111000111100\rangle + e|110111000111011\rangle \\
& + e|110111111000100\rangle + e|110111111000011\rangle + e|110111111111100\rangle + e|110111111111011\rangle \\
& + f|010000000000100\rangle + f|010000000000011\rangle + f|010000000111100\rangle + f|010000000111011\rangle \\
& + f|010000111000100\rangle + f|010000111000011\rangle + f|010000111111100\rangle + f|010000111111011\rangle \\
& + f|010111000000100\rangle + f|010111000000011\rangle + f|010111000111100\rangle + f|010111000111011\rangle \\
& + f|010111111000100\rangle + f|010111111000011\rangle + f|010111111111100\rangle + f|010111111111011\rangle \\
& + g|100000000000000\rangle + g|100000000000011\rangle + g|100000000111000\rangle + g|100000000111111\rangle \\
& + g|100000111000000\rangle + g|100000111000111\rangle + g|100000111111000\rangle + g|100000111111111\rangle \\
& + g|100111000000000\rangle + g|100111000000111\rangle + g|100111000111000\rangle + g|100111000111111\rangle \\
& + g|100111111000000\rangle + g|100111111000111\rangle + g|100111111111000\rangle + g|100111111111111\rangle \\
& + h|111000000000110\rangle + h|111000000000001\rangle + h|111000000111110\rangle + h|111000000111001\rangle \\
& + h|111000111000110\rangle + h|111000111000001\rangle + h|111000111111110\rangle + h|111000111111001\rangle \\
& + h|111111000000110\rangle + h|111111000000001\rangle + h|111111000111110\rangle + h|111111000111001\rangle \\
& + h|111111111000110\rangle + h|111111111000001\rangle + h|111111111111110\rangle + h|111111111111001\rangle.
\end{aligned}$$

Thereafter, Alice carries out three GHZ state measurements on the particles $(x, 1, 2)$, $(y, 4, 5)$ and $(z, 7, 8)$ respectively as illustrated in second block of Figure 7.1. This GHZ state measurement projects onto any of the GHZ states. For instance, if Alice's measurements results are $|\phi\rangle^+$ then the collapsed state of the remaining particles can be written as

$$\begin{aligned} |\Psi\rangle_{369101112} &= {}_{x12}\langle\phi^+| \otimes {}_{y45}\langle\phi^+| \otimes {}_{x78}\langle\phi|\Psi\rangle_{123456789101112} \\ &= (a|000000\rangle + a|000111\rangle + b|011110\rangle + b|011001\rangle + c|101101\rangle + c|101010\rangle \\ &\quad + d|001010\rangle + d|001101\rangle + e|110100\rangle + e|110011\rangle + f|010100\rangle + f|010011\rangle \\ &\quad + g|100000\rangle + g|100111\rangle + h|111110\rangle + h|111001\rangle. \end{aligned} \quad (7.7)$$

Alice then executes two single measurements on particles 10 and 11 with the basis $X\{|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ (block 3 of Figure 7.1). If she obtains $|+x\rangle$ as her measurement result, then the collapsed state becomes

$$\begin{aligned} |\Phi\rangle_{36912} &= {}_{10}\langle+x| {}_{11}\langle+x|\Phi\rangle_{369101112} \\ &= (a|0000\rangle + a|0001\rangle + b|0110\rangle + b|0111\rangle + c|1011\rangle + c|1010\rangle + c|0010\rangle + d|0011\rangle \\ &\quad + e|1100\rangle + e|1101\rangle + f|0100\rangle + f|0101\rangle + g|1000\rangle + g|1001\rangle + h|1110\rangle + h|1111\rangle. \end{aligned} \quad (7.8)$$

Alice reveals her measurement results to her agents through a classical channel. To reconstruct the original state, Bob4 performs a single measurement on the standard basis and informs Bob1, Bob2 and Bob3 about his results as shown in block 4 in Figure 7.1. Bob1, Bob2 and Bob3 then collaborate to recover the unknown state by performing unitary transformations on their particles. This is depicted in block 5 in Figure 7.1. The required unitary operators are $(\sigma_z, \sigma_x, \mathbf{1})$ where $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $\mathbf{1} = |0\rangle\langle 0| + |1\rangle\langle 1|$.

For instance, if Alice's measurement results are $|\phi^+\rangle_{x12}, |\phi^+\rangle_{y45}, |\phi^+\rangle_{x78}, |-x\rangle_{10}, |+x\rangle_{11}$ and Bob's results are $|1\rangle_{12}$, then the collapsed state can be described as

$$|\Phi\rangle_{369} = (-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369}. \quad (7.9)$$

To recover the original state then Bob1, Bob2 and Bob3 have to perform the following unitary operations, $(\mathbf{1} \otimes \sigma_z \sigma_x \otimes \mathbf{1})$, that is, Bob1 and Bob3 have to do nothing on their particle whilst Bob2 has to do the phase flip operation followed by the bit flip on his particle. This can be explicitly shown as;

Bob1's operation:

$$(|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369}$$

This yields;

$$(-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369}.$$

Bob2 has to carry out the phase flip and bit flip on his particle,

$$(|0\rangle\langle 1| - |1\rangle\langle 0|) \otimes (-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369},$$

which gives,

$$|\Phi\rangle_{369} = (a|010\rangle + b|101\rangle + c|111\rangle + d|011\rangle + e|100\rangle + f|000\rangle + g|110\rangle + h|101\rangle)_{369},$$

which is the original states sent by Alice to her agents.

7.2 The Generalized Scheme for Multi-Party QSTS of an Arbitrary Three Particle State with GHZ States Measurements

Our proposed scheme can be generalized to the case of n agents. Firstly, Alice prepares and shares n three-particle GHZ states with Bob1, Bob2,..., Bob n , where $n > 3$. Each agent Bob i is in possession of his $3i$ particle whilst Alice holds the particles 1, 2, 4, 5, $3n - 1$. Alice then performs the CNOT gate operations, with the particles x, y or z are acting as control particles and 10, 11, 13, 14, ..., $3n - 1$ as the target particles. After that, Alice carries out three GHZ state measurement on particles $(x, 1, 2)$, $(y, 4, 5)$ and $(z, 7, 8)$ followed by $2(n - 3)$ single particle measurements on her particles 10, 11, ..., $(3n - 1)$ with basis $X\{|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. She eventually publishes her results to the agents via the classical channel. The agents who act as controllers will perform single particle measurements on the standard basis on their respective particles and reveal their results to Bob1, Bob2 and Bob3 who acts as recoverers. The trio collaborate to recover the original state by performing local unitary operations on their particles depending on Alice and controllers' results.

7.3 QSTS of an Arbitrary m -Particle State with n Agents

Subsequently, this three-particle scheme can be generalised to the case of sharing m -particle state with n agents (as shown in Figure 7.2). Alice start by sharing n GHZ states with Bobi ($i = 1, , n$) and hence the whole system can be written as

$$|\Psi\rangle \equiv \left(\sum_{ij\dots k} \alpha_{ij\dots k} \underbrace{|ij\dots k\rangle}_m \right)_{x_1 x_2 \dots x_m} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{123} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{456} \otimes \dots \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{n-2, n-1, n}, \quad (7.10)$$

where $i, j, \dots, k \in \{0, 1\}$ and $x_1, x_2, \dots$ and x_m are the m particles in the unknown state.

Alice then carries out $2(n - m)$ CNOT operations and performs m GHZ state measurements followed by $2(n - m)$ single particle measurements on her particles. Consequently, the unknown state is transferred into the particles in the possession of her agents. The controllers then executes $(n - m)$ single particle measurements in the standard basis and publishes their results. The m agents collaborate to recover the unknown state by performing the unitary operations to their particles(see Figure 7.2).

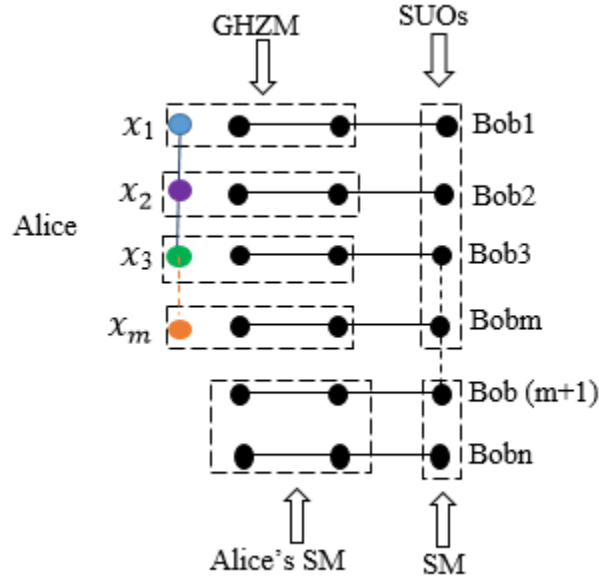


Figure 7.2: The principles of our QSTS scheme of an arbitrary m -particle state. Alice perform m GHZ state measurements (GHZM) and $2(n - m)$ single particle measurements (SM). Controllers carries out $(n - m)$ single particle measurements and other agents performs single particle unitary operations (SUOs) to recover the unknown state.

Table 7.1: The comparison between our scheme and the other previous schemes for sharing three particle state and two particle state with five parties. QR-quantum resources, NO-necessary operations, CR-Classical resources, GHZM-GHZ state joint measurement, BM-Bell state measurement, SM- single particle measurement, Single particle unitary operation, η_t -total efficiency

Schemes	QR	NO	CR	η_t
Sheng et al [119]	6 GHZ States	3 GHZM, 9SMs and 3SUOs	15 bits	1/6
Deng et al. [93]	8 EPR pairs	10 GHZM, 6SMs and 2SUOs	10 bits	1/13
Deng et al [118]	5 EPR pairs	5 BMs and 3SUOs	10 bits	1/10
Our scheme	4 GHZ States	3 GHZM, 3SMs and 3SUOs	12 bits	1/8

In our scheme, the quantum channel is set up using the decoy-photon technique. The proportion of the decoy photons is so negligible that the intrinsic efficiency of qubits in our scheme approaches 100% as given by the formula;

$$\eta_q \equiv \frac{q_u}{q_t}, \quad (7.11)$$

where q_u is the number of useful qubits in the QSTS and q_t is the number of transmitted qubits. The total efficiency of QSTS scheme is defined as

$$\eta_t = \frac{q_s}{q_u + b_t}, \quad (7.12)$$

where q_s is the number of qubits that consists of the quantum information to be shared, q_u is the number of useful qubits in the QSTS and b_t is the number of classical bits transmitted. In our scheme $q_u = 3n$, $q_s = 3$ and $b_t = 3n$ which gives the total efficiency, η_t , as $1/2n$. This is equivalent to $1/8$ for a five party QSTS. This efficiency greater than that in the QSTS by Deng et al [93,118] as depicted in table 7.1. Though these schemes in reference [93,118] uses EPR pairs which are easier to prepare practically as compared to GHZ states in our scheme, they involve a lot operations performed by the parties which increases the difficulty of the schemes. For instance, Alice needs to perform 10 joint GHZ states measurements in reference [93] which is practically difficult to implement in the present moment. The scheme by Sheng et al in ref [119] has better efficiency as compared to our scheme. However, considering the fact that 6 GHZ states are needed to be prepared, our scheme is more convenient in terms of resource consumption as only 4 GHZ states are required.

Moreover, there are other existing schemes which uses non maximally entangled states

which are robust against environmental effects and easier to implement [99, 120]. However, these schemes are asymmetric, therefore only one agent can retrieve the unknown state as compared to our scheme in which any of the agents can act as a receiver. The symmetry created by maximally entangled states allows any of the agents to act as a receiver of the unknown state with the help of other agents.

Chapter 8

QSTS of an Arbitrary 3-Particle State using Einstein-Podolsky-Rosen Pairs and GHZ State Measurements

We present another scheme which is more efficient in terms of resource consumption and operation complexity. The scheme uses the EPR pairs which are easier to prepare as compared to the more-partite entangled states such as GHZ states hence making it practically realizable. More importantly, the scheme can be extended to multi-partite QSTS without compromising the efficiency of the scheme.

8.1 Operation of the Scheme

Our scheme can be described as follows; suppose Alice want to share an arbitrary three-particle state with her two agents Bob1 and Bob2. An arbitrary three particle state in possession of Alice is supposed to be in this form,

$$|\Phi\rangle_{xyz} = \alpha|000\rangle + \beta|011\rangle + \gamma|101\rangle + \delta|001\rangle + \tau|110\rangle + \lambda|010\rangle + \mu|100\rangle + \eta|111\rangle. \quad (8.1)$$

As shown in Figure 8.1, Alice starts by sharing 6 EPR pairs a_1b_1, c_1d_1, e_1f_1 and a_2b_2, c_2d_2, e_2f_2 with Bob1 and Bob2 respectively. After that, each one of the agents has 3 particles in his possession. The a_1 and b_1 represents the particles in an EPR pair and similarly for other notations. An EPR pair is in one of the Bell states which can be expressed as

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad (8.2)$$

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle). \quad (8.3)$$

Without loss of generality, we assume that all EPR pairs shared by Alice are

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (8.4)$$

The whole system can then be written as

$$|\Psi\rangle = |\Phi\rangle_{xyz} |\phi^+\rangle_{a1b1} |\phi^+\rangle_{c1d1} |\phi\rangle_{e1f1} |\phi^+\rangle_{a2b2} |\phi^+\rangle_{c2d2} |\phi^+\rangle_{e2f2}. \quad (8.5)$$

Alice executes three joint three-particle GHZ measurements on particles (x, a_1, a_2) , (y, c_1, c_2) and (z, e_1, e_2) .

The three-particle GHZ state can be generalised as

$$\begin{aligned} |\varphi^\pm\rangle &= \frac{1}{2\sqrt{2}}(|000\rangle \pm |111\rangle), \\ |\psi^\pm\rangle &= \frac{1}{2\sqrt{2}}(|011\rangle \pm |100\rangle), \\ |\Psi^\pm\rangle &= \frac{1}{2\sqrt{2}}(|101\rangle \pm |010\rangle), \\ |\Phi^\pm\rangle &= \frac{1}{2\sqrt{2}}(|001\rangle \pm |110\rangle). \end{aligned} \quad (8.6)$$

Suppose Alice's GHZ state measurement results are $|\varphi^+\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)$, then the system collapses to subsystem of the particles initially distributed between the agents. To restore the original state one of the agents has to carry out product measurement $\sigma_x \otimes \sigma_x \otimes \sigma_x$ on his three particles and the other performs three unitary operations according to the results provided by the other party. The rearranged subsystem can be expressed as follows, with $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ representing two eigenstates of measuring in basis σ_x .

$$\begin{aligned} |\Psi\rangle_{sub} = & |+x\rangle|+x\rangle|+x\rangle(\alpha|000\rangle + \beta|011\rangle + \gamma|101\rangle + \delta|001\rangle + \tau|110\rangle + \lambda|010\rangle + \mu|100\rangle + \eta|111\rangle) \\ & + |+x\rangle|+x\rangle|-x\rangle(\alpha|000\rangle - \beta|011\rangle - \gamma|101\rangle - \delta|001\rangle + \tau|110\rangle + \lambda|010\rangle + \mu|100\rangle - \eta|111\rangle) \\ & + |-x\rangle|+x\rangle|+x\rangle(\alpha|000\rangle + \beta|011\rangle - \gamma|101\rangle + \delta|001\rangle - \tau|110\rangle + \lambda|010\rangle + \mu|100\rangle - \eta|111\rangle) \\ & + |-x\rangle|+x\rangle|-x\rangle(\alpha|000\rangle - \beta|011\rangle + \gamma|101\rangle - \delta|001\rangle - \tau|110\rangle + \lambda|010\rangle - \mu|100\rangle + \eta|111\rangle) \\ & + |+x\rangle|-x\rangle|+x\rangle(\alpha|000\rangle - \beta|011\rangle + \gamma|101\rangle + \delta|001\rangle - \tau|110\rangle - \lambda|010\rangle + \mu|100\rangle - \eta|111\rangle) \\ & + |+x\rangle|-x\rangle|-x\rangle(\alpha|000\rangle + \beta|011\rangle - \gamma|101\rangle - \delta|001\rangle - \tau|110\rangle - \lambda|010\rangle + \mu|100\rangle + \eta|111\rangle) \\ & + |-x\rangle|-x\rangle|+x\rangle(\alpha|000\rangle - \beta|011\rangle - \gamma|101\rangle + \delta|001\rangle + \tau|110\rangle - \lambda|010\rangle - \mu|100\rangle + \eta|111\rangle) \\ & + |-x\rangle|-x\rangle|-x\rangle(\alpha|000\rangle + \beta|011\rangle + \gamma|101\rangle - \delta|001\rangle + \tau|110\rangle - \lambda|010\rangle - \mu|100\rangle - \eta|111\rangle). \end{aligned} \quad (8.7)$$

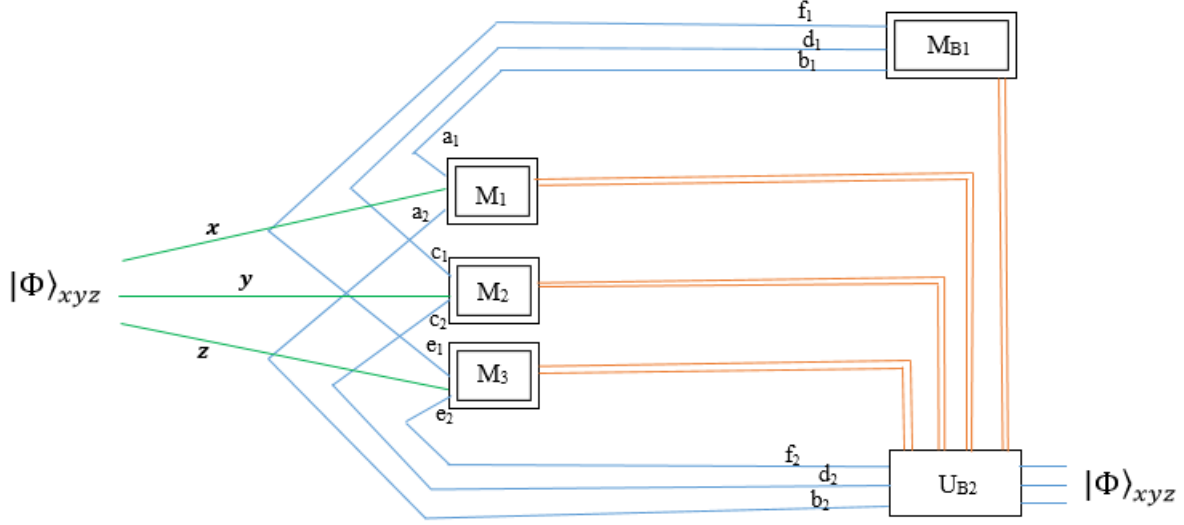


Figure 8.1: QSTS of arbitrary three-particle quantum state with two parties. Alice starts by sharing two EPR pairs with Bob1 and Bob2. Alice then carries out GHZ state measurement (M_1, M_2 and M_3) on particles $(x, a_1, a_2), (y, c_1, c_2)$ and (z, e_1, e_2) . Bob1 executes product measurement (M_{B1}) on his particles and Bob2 performs unitary operations (U_{B2}) on his particles .

If Bob1 collaborate with Bob2, Bob2 can recover the original state by performing the unitary operations $U_0 \otimes U_0 \otimes U_0$, $U_0 \otimes U_1 \otimes U_0$, $U_0 \otimes U_0 \otimes U_1$, $U_1 \otimes U_0 \otimes U_0$, $U_1 \otimes U_0 \otimes U_1$, $U_0 \otimes U_1 \otimes U_1$, $U_1 \otimes U_1 \otimes U_0$ and $U_1 \otimes U_1 \otimes U_1$ if Bob1 obtained the following results $|+x\rangle|+x\rangle|+x\rangle, |+x\rangle|-x\rangle|+x\rangle, |+x\rangle|+x\rangle|-x\rangle, |-x\rangle|+x\rangle|+x\rangle, |-x\rangle|+x\rangle|-x\rangle, |+x\rangle|-x\rangle|-x\rangle, |-x\rangle|-x\rangle|+x\rangle$ and $|-x\rangle|-x\rangle|-x\rangle$ respectively. Here

$$U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad U_2 = |1\rangle\langle 0| + |0\rangle\langle 1|, \quad U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|. \quad (8.8)$$

For other results obtained by Bob1, the local unitary operations with which Bob2 uses to reconstruct the unknown state is shown in Table 8.2-8.5.

Table 8.1: The comparison between our scheme and the other previous schemes for sharing three particle state and two particle state. QR-quantum resources, NO-necessary operations, CR-Classical resources, GHZM-GHZ state joint measurement, BM-Bell state measurement, SM- single particle measurement, Single particle unitary operation, η_t -total efficiency

Schemes	QR	NO	CR	η_t
Li et al [100]	2 GHZ States	2 BMs, 2 SMs and 2SUOs	6 bits	3/7
Peng et al. [121]	3 GHZ States	3BMs 3SMs and 3SUOs	4 bits	1/5
Our scheme	6 EPR pairs	3GHZMs, 3SMs and 3SUOs	9 bits	1/7

The V_{xa1a2} , V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2$, $yc1c2$ and $ze1e2$ respectively, that is,

$$V_{|G_{ij\pm}\rangle} = j, \quad P_{|G_{ij\pm}\rangle} = \pm, \quad P_{|\pm x\rangle} = \pm, \quad (8.9)$$

where $|G_{ij\pm}\rangle = \frac{1}{\sqrt{2}}(|0ij\rangle \pm |1\bar{i}\bar{j}\rangle)$ is the notation for the GHZ states with $i, j \in \{0, 1\}$, $\bar{i} = 1 - i$ and $\bar{j} = 1 - j$.

8.2 QSTS of an Arbitrary 3 Particle State to N Agents

It is straight forward to generalise this scheme to a case of n agents. Alice has to share $3N$ EPR pairs ($|\phi^\pm\rangle_{a_i b_i}$, $|\phi^\pm\rangle_{c_i d_i}$, $|\phi^\pm\rangle_{e_i f_i}$ with her agents and hence the whole system of the particles becomes

$$|\Psi\rangle_S = |\Phi\rangle_{xyz} \prod_{i=1}^N \otimes (|\phi^+\rangle_{a_i b_i} \otimes |\phi^+\rangle_{c_i d_i} \otimes |\phi^+\rangle_{e_i f_i}). \quad (8.10)$$

Alice executes $3(N+1)$ -GHZ state joint measurements on particles $x, a_1, \dots, a_N, y, c_1, \dots, c_N$ and $y, e_1, \dots, e_N$. The GHZ states can be defined as

$$|G_{\underbrace{ij\dots k}_N+}\rangle = \frac{1}{\sqrt{2}}(|\underbrace{0ij\dots k}_N\rangle + |\underbrace{1\bar{i}\bar{j}\dots \bar{k}}_N\rangle), \quad (8.11)$$

$$|G_{\underbrace{ij\dots k}_N-}\rangle = \frac{1}{\sqrt{2}}(|0\underbrace{ij\dots k}_N\rangle - |1\underbrace{\bar{i}\bar{j}\dots\bar{k}}_N\rangle), \quad (8.12)$$

where $i, j, k \in \{0, 1\}$, $\bar{i} = 1 - i$, $\bar{j} = 1 - j$, $k = 1 - k$. Given that, $\psi_{xa_1, \dots, a_N}$, $\psi_{\bar{x}a_1, \dots, a_N} \in \{|\underbrace{G_{ij\dots k}}_N+\rangle, |\underbrace{G_{ij\dots k}}_N-\rangle\}$, then the whole system can be rearranged as follows

[illegible]

where $|i\rangle = \frac{1}{\sqrt{2}}[|+x\rangle + (-1)^i |-x\rangle]$, $\{i, j, \dots, k, m, n, \dots, l, r, s, \dots, t\} \in \{0, 1\}$ and $\bar{m} = 1 - m$, $\bar{r} = 1 - r$. To recover the original state each of the controllers carries out product measurement $\sigma_x \otimes \sigma_x \otimes \sigma_x$ on his particles. Because of symmetry, the measurements performed by the controllers can be expressed by the operation M ,

$$M = [(\langle +x|)^{N-1-t}(\langle -x|)^t]_1 \otimes [(\langle +x|)^{N-1-q}(\langle -x|)^q]_2 \otimes [(\langle +x|)^{N-1-r}(\langle -x|)^r]_3, \quad (8.14)$$

where $[(\langle +x|)^{N-1-t}(\langle -x|)^t]_1$ is the measurement operation related to the particles in possession of the controllers and t, q and r are the numbers that, the controllers obtained $|-x\rangle$, when they measured their particles. After measurements by the controllers the whole system collapses to

$$\begin{aligned} |\Psi\rangle_{sub} = & \sum_{\substack{i,k\dots k \\ m,n,\dots,l \\ r,s,\dots,t}} |G_{i,j\dots,k+}\rangle |G_{m,n\dots,l+}\rangle |G_{r,s\dots,t+}\rangle (\alpha |klt\rangle \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \\ & \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \pm \eta |\bar{k}\bar{l}t\rangle) + |G_{i,j\dots,k+}\rangle |G_{m,n\dots,l+}\rangle |G_{r,s\dots,t-}\rangle \\ & (\alpha |klt\rangle \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \pm \eta |\bar{k}\bar{l}t\rangle) + |G_{i,j\dots,k-}\rangle \\ & |G_{m,n\dots,l+}\rangle |G_{r,s\dots,t-}\rangle (\alpha |klt\rangle \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \\ & \pm \eta |\bar{k}\bar{l}t\rangle) + |G_{i,j\dots,k-}\rangle |G_{m,n\dots,l-}\rangle |G_{r,s\dots,t-}\rangle (\alpha |klt\rangle \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \\ & \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \pm \eta |\bar{k}\bar{l}t\rangle) + |G_{i,j\dots,k+}\rangle |G_{m,n\dots,l-}\rangle |G_{r,s\dots,t+}\rangle (\alpha |klt\rangle \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \\ & \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \pm \eta |\bar{k}\bar{l}t\rangle) + |G_{i,j\dots,k+}\rangle |G_{m,n\dots,l-}\rangle |G_{r,s\dots,t-}\rangle (\alpha |klt\rangle \\ & \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \pm \eta |\bar{k}\bar{l}t\rangle) + |G_{i,j\dots,k-}\rangle |G_{m,n\dots,l-}\rangle \\ & |G_{r,s\dots,t-}\rangle (\alpha |klt\rangle \pm \beta |\bar{k}\bar{l}\bar{t}\rangle \pm \gamma |\bar{k}\bar{l}t\rangle \pm \delta |k\bar{l}\bar{t}\rangle \pm \tau |\bar{k}lt\rangle \pm \lambda |\bar{k}\bar{l}t\rangle \pm \mu |\bar{k}lt\rangle \pm \eta |\bar{k}\bar{l}t\rangle). \end{aligned} \quad (8.15)$$

The sign of the eigenvalues depends on the measurement results of the controllers. Finally, BobN has to perform local unitary operations on his particles to recover the original state. The scheme can be easily generalised to sharing m -particle state with N agents. Alice starts by sharing mN EPR pairs with her agents. The composite system can be expressed as

$$|\Psi\rangle \equiv \left(\sum_{i,j\dots k} \alpha_{i,j\dots k} \underbrace{|i,j\dots k\rangle}_m \right)_{x_1 x_2, \dots, x_m} \otimes \prod_{i=1}^m \frac{1}{\sqrt{2}} \left(\prod_{i=1}^N |00\rangle + \prod_{i=1}^N |11\rangle \right), \quad (8.16)$$

where $i, j, \dots, k \in \{0, 1\}$ and $x_1, x_2, \dots, x_m$ and x_m are the m particles in the unknown state. The unknown state is then transferred to the agents when Alice executes $m(N+1)$ GHZ state measurements. Each of controllers performs product measurement $\sigma_x^1 \otimes \sigma_x^2 \otimes \dots \otimes \sigma_x^m$

on their m particles. Bob N then recovers the original state by performing local unitary operations on his m particles.

Our scheme can be easily implemented experimentally since EPR pairs are not difficult to prepare compared to other entangled states such as GHZ states and five particle entangled states that have been used in other schemes [121,122]. Alice can also deter eavesdropping on her particles by her agents as she can privately set up a quantum channel with each of the agents beforehand. In order to set up the secure quantum channel with all agents, Alice can use the decoy-photon technique. However, the proportion of the decoy photon is so small and does not affect the efficiency of the scheme. The intrinsic efficiency of qubits in our scheme approaches 100% as given by the formula,

$$\eta_q \equiv \frac{q_u}{q_t}, \quad (8.17)$$

where q_u is the number of useful qubits in the QSTS and q_t is the number of transmitted qubits. The total efficiency of QSTS scheme is defined as

$$\eta_t = \frac{q_s}{q_u + b_t}, \quad (8.18)$$

where q_s is the number of qubits that consists of the quantum information to be shared, q_u is the number of useful qubits in the QSTS and b_t is the number of classical bits transmitted. In our scheme $q_u = mN$, $q_s = m$ and $b_t = mN$ which gives η_t as $1/N$. Recently, Li et al [100] proposed a scheme that uses a 2 GHZ states to share an arbitrary two particle state. The scheme requires Alice to execute 2 Bell basis measurements on her particles and her agents, Bob and Charlie to carry out 2 single particle measurements and 2 unitary operations respectively. Moreover, in another scheme proposed by Peng et al [121], Alice performs 3 Bell measurements followed 3 single particle measurement by Bob and 3 single unitary operations executed by Charlie to recover the unknown state. These schemes are similar to our scheme in terms of the required operations. The efficiency obtained from the schemes are much better than our scheme as depicted in table 8.1. However, our scheme requires the use of EPR pairs which has been experimentally realised as compared to the GHZ states used in these schemes. Therefore, our scheme is feasible according to the present experimental technology.

Table 8.2: The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2} , V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2$, $yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}$, $P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.

V_{xa1a2}	V_{yc1c2}	V_{ze1e2}	$P_{xa1a2} \otimes P_{b1}$	$P_{yc1c2} \otimes P_{d1}$	$P_{ze1e2} \otimes P_{f1}$	$ \Phi\rangle_{b2d2f2}$	U_{B2}
0	0	0	+	+	+	$\alpha 000\rangle + \beta 011\rangle + \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle + \lambda 010\rangle + \mu 100\rangle + \eta 111\rangle$	$U_0 \otimes U_0 \otimes U_0$
0	0	0	+	-	+	$\alpha 000\rangle - \beta 011\rangle + \gamma 101\rangle + \delta 001\rangle$ $- \tau 110\rangle - \lambda 010\rangle + \mu 100\rangle - \eta 111\rangle$	$U_0 \otimes U_1 \otimes U_0$
0	0	0	+	+	-	$\alpha 000\rangle - \beta 011\rangle - \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle + \lambda 010\rangle + \mu 100\rangle - \eta 111\rangle$	$U_0 \otimes U_0 \otimes U_1$
0	0	0	-	+	+	$\alpha 000\rangle + \beta 011\rangle - \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle + \lambda 010\rangle - \mu 100\rangle - \eta 111\rangle$	$U_1 \otimes U_0 \otimes U_0$
0	0	0	-	+	-	$\alpha 000\rangle - \beta 011\rangle + \gamma 101\rangle - \delta 001\rangle$ $+ \tau 110\rangle + \lambda 010\rangle - \mu 100\rangle + \eta 111\rangle$	$U_1 \otimes U_0 \otimes U_1$
0	0	0	+	-	-	$\alpha 000\rangle + \beta 011\rangle - \gamma 101\rangle - \delta 001\rangle$ $- \tau 110\rangle - \lambda 010\rangle + \mu 100\rangle + \eta 111\rangle$	$U_0 \otimes U_1 \otimes U_1$
0	0	0	-	-	+	$\alpha 000\rangle - \beta 011\rangle - \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle - \lambda 010\rangle + \mu 100\rangle + \eta 111\rangle$	$U_1 \otimes U_1 \otimes U_0$
0	0	0	-	-	-	$\alpha 000\rangle + \beta 011\rangle + \gamma 101\rangle - \delta 001\rangle$ $+ \tau 110\rangle - \lambda 010\rangle - \mu 100\rangle + \eta 111\rangle$	$U_1 \otimes U_1 \otimes U_1$
0	1	1	+	+	+	$\alpha 000\rangle + \beta 011\rangle + \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle + \lambda 010\rangle + \mu 100\rangle + \eta 111\rangle$	$U_0 \otimes U_2 \otimes U_2$
0	1	1	+	-	+	$\alpha 000\rangle + \beta 011\rangle + \gamma 101\rangle + \delta 001\rangle$ $- \tau 110\rangle - \lambda 010\rangle + \mu 100\rangle - \eta 111\rangle$	$U_0 \otimes U_3 \otimes U_0$
0	1	1	+	+	-	$\alpha 000\rangle - \beta 011\rangle - \gamma 101\rangle - \delta 001\rangle$ $+ \tau 110\rangle + \lambda 010\rangle + \mu 100\rangle - \eta 111\rangle$	$U_3 \otimes U_0 \otimes U_1$
0	1	1	-	+	+	$\alpha 000\rangle + \beta 011\rangle - \gamma 101\rangle + \delta 001\rangle$ $- \tau 110\rangle + \lambda 010\rangle - \mu 100\rangle - \eta 111\rangle$	$U_1 \otimes U_0 \otimes U_0$
0	1	1	-	+	-	$\alpha 000\rangle - \beta 011\rangle + \gamma 101\rangle - \delta 001\rangle$ $- \tau 110\rangle + \lambda 010\rangle - \mu 100\rangle + \eta 111\rangle$	$U_1 \otimes U_3 \otimes U_1$
0	1	1	+	-	-	$\alpha 000\rangle + \beta 011\rangle - \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle - \lambda 010\rangle - \mu 100\rangle + \eta 111\rangle$	$U_0 \otimes U_1 \otimes U_1$
0	1	1	-	-	+	$\alpha 000\rangle - \beta 011\rangle - \gamma 101\rangle + \delta 001\rangle$ $+ \tau 110\rangle - \lambda 010\rangle - \mu 100\rangle + \eta 111\rangle$	$U_3 \otimes U_1 \otimes U_0$
0	1	1	-	-	-	$\alpha 000\rangle + \beta 011\rangle + \gamma 101\rangle - \delta 001\rangle$ $+ \tau 110\rangle - \lambda 010\rangle - \mu 100\rangle - \eta 111\rangle$	$U_1 \otimes U_1 \otimes U_1$

Table 8.3: The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2} , V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2$, $yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}$, $P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.

V_{xa1a2}	V_{yc1c2}	V_{ze1e2}	$P_{xa1a2} \otimes P_{b1}$	$P_{yc1c2} \otimes P_{d1}$	$P_{ze1e2} \otimes P_{f1}$	$ \Phi\rangle_{b2d2f2}$	U_{B2}
1	0	1	+	+	+	$\alpha 101\rangle + \beta 110\rangle + \gamma 000\rangle + \delta 100\rangle$ $+ \tau 011\rangle + \lambda 111\rangle + \mu 001\rangle + \eta 010\rangle$	$U_2 \otimes U_0 \otimes U_2$
1	0	1	+	-	+	$\alpha 101\rangle - \beta 110\rangle + \gamma 000\rangle + \delta 100\rangle$ $- \tau 011\rangle - \lambda 111\rangle + \mu 001\rangle - \eta 010\rangle$	$U_0 \otimes U_1 \otimes U_0$
1	0	1	+	+	-	$\alpha 101\rangle - \beta 110\rangle - \gamma 000\rangle - \delta 100\rangle$ $+ \tau 011\rangle + \lambda 111\rangle + \mu 001\rangle - \eta 010\rangle$	$U_2 \otimes U_0 \otimes U_3$
1	0	1	-	+	+	$\alpha 101\rangle + \beta 110\rangle - \gamma 000\rangle + \delta 100\rangle$ $- \tau 011\rangle + \lambda 111\rangle - \mu 001\rangle - \eta 010\rangle$	$U_3 \otimes U_0 \otimes U_2$
1	0	1	-	+	-	$\alpha 101\rangle - \beta 110\rangle + \gamma 000\rangle - \delta 100\rangle$ $+ \tau 011\rangle + \lambda 111\rangle - \mu 001\rangle + \eta 010\rangle$	$U_1 \otimes U_0 \otimes U_1$
1	0	1	+	-	-	$\alpha 101\rangle + \beta 110\rangle - \gamma 000\rangle - \delta 100\rangle$ $- \tau 011\rangle - \lambda 111\rangle + \mu 001\rangle + \eta 010\rangle$	$U_0 \otimes U_3 \otimes U_1$
1	0	1	-	-	+	$\alpha 101\rangle - \beta 110\rangle - \gamma 000\rangle + \delta 100\rangle$ $+ \tau 011\rangle - \lambda 111\rangle - \mu 001\rangle + \eta 010\rangle$	$U_3 \otimes U_1 \otimes U_0$
1	0	1	-	-	-	$\alpha 101\rangle + \beta 110\rangle + \gamma 000\rangle - \delta 100\rangle$ $+ \tau 011\rangle - \lambda 111\rangle - \mu 001\rangle - \eta 010\rangle$	$U_1 \otimes U_1 \otimes U_1$
0	0	1	+	+	+	$\alpha 001\rangle + \beta 010\rangle + \gamma 100\rangle + \delta 000\rangle$ $+ \tau 111\rangle + \lambda 011\rangle + \mu 101\rangle + \eta 110\rangle$	$U_0 \otimes U_0 \otimes U_1$
0	0	1	+	-	+	$\alpha 001\rangle - \beta 010\rangle + \gamma 100\rangle + \delta 000\rangle$ $- \tau 111\rangle - \lambda 011\rangle + \mu 101\rangle - \eta 110\rangle$	$U_0 \otimes U_1 \otimes U_0$
0	0	1	+	+	-	$\alpha 001\rangle - \beta 010\rangle - \gamma 100\rangle - \delta 000\rangle$ $+ \tau 111\rangle + \lambda 011\rangle + \mu 101\rangle - \eta 110\rangle$	$U_0 \otimes U_0 \otimes U_3$
0	0	1	-	+	+	$\alpha 001\rangle + \beta 010\rangle - \gamma 100\rangle + \delta 000\rangle$ $- \tau 111\rangle + \lambda 011\rangle - \mu 101\rangle - \eta 110\rangle$	$U_1 \otimes U_0 \otimes U_0$
0	0	1	-	+	-	$\alpha 001\rangle - \beta 010\rangle + \gamma 100\rangle - \delta 000\rangle$ $- \tau 111\rangle + \lambda 011\rangle - \mu 101\rangle + \eta 110\rangle$	$U_3 \otimes U_0 \otimes U_1$
0	1	1	+	-	-	$\alpha 001\rangle + \beta 010\rangle - \gamma 100\rangle - \delta 000\rangle$ $- \tau 111\rangle - \lambda 011\rangle + \mu 101\rangle + \eta 110\rangle$	$U_0 \otimes U_3 \otimes U_1$
0	0	1	-	-	+	$\alpha 001\rangle - \beta 010\rangle - \gamma 100\rangle + \delta 000\rangle$ $+ \tau 111\rangle - \lambda 011\rangle - \mu 101\rangle + \eta 110\rangle$	$U_3 \otimes U_3 \otimes U_0$
0	0	1	-	-	-	$\alpha 001\rangle + \beta 010\rangle + \gamma 100\rangle - \delta 000\rangle$ $+ \tau 111\rangle - \lambda 011\rangle - \mu 101\rangle - \eta 110\rangle$	$U_3 \otimes U_3 \otimes U_3$

Table 8.4: The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2} , V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2$, $yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}$, $P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.

V_{xa1a2}	V_{yc1c2}	V_{ze1e2}	$P_{xa1a2} \otimes P_{b1}$	$P_{yc1c2} \otimes P_{d1}$	$P_{ze1e2} \otimes P_{f1}$	$ \Phi\rangle_{b2d2f2}$	U_{B2}
1	1	0	+	+	+	$\alpha 110\rangle + \beta 101\rangle + \gamma 011\rangle + \delta 111\rangle$ $+ \tau 000\rangle + \lambda 100\rangle + \mu 010\rangle + \eta 001\rangle$	$U_2 \otimes U_2 \otimes U_0$
1	1	0	+	-	+	$\alpha 110\rangle - \beta 101\rangle + \gamma 011\rangle + \delta 111\rangle$ $- \tau 110\rangle - \lambda 100\rangle + \mu 010\rangle - \eta 001\rangle$	$U_0 \otimes U_3 \otimes U_0$
1	1	0	+	+	-	$\alpha 110\rangle - \beta 101\rangle - \gamma 011\rangle - \delta 111\rangle$ $+ \tau 000\rangle + \lambda 100\rangle + \mu 010\rangle - \eta 001\rangle$	$U_0 \otimes U_0 \otimes U_1$
1	1	0	-	+	+	$\alpha 110\rangle + \beta 101\rangle - \gamma 011\rangle + \delta 111\rangle$ $- \tau 000\rangle + \lambda 100\rangle - \mu 010\rangle - \eta 001\rangle$	$U_3 \otimes U_0 \otimes U_0$
1	1	0	-	+	-	$\alpha 110\rangle - \beta 101\rangle + \gamma 011\rangle - \delta 111\rangle$ $- \tau 000\rangle + \lambda 100\rangle - \mu 010\rangle + \eta 001\rangle$	$U_3 \otimes U_0 \otimes U_1$
1	1	0	+	-	-	$\alpha 110\rangle + \beta 101\rangle - \gamma 011\rangle - \delta 111\rangle$ $- \tau 000\rangle - \lambda 100\rangle + \mu 010\rangle + \eta 001\rangle$	$U_0 \otimes U_1 \otimes U_3$
1	1	0	-	-	+	$\alpha 110\rangle - \beta 101\rangle - \gamma 011\rangle + \delta 111\rangle$ $+ \tau 000\rangle - \lambda 100\rangle - \mu 010\rangle + \eta 001\rangle$	$U_1 \otimes U_1 \otimes U_0$
1	1	0	-	-	-	$\alpha 110\rangle + \beta 101\rangle + \gamma 011\rangle - \delta 111\rangle$ $+ \tau 000\rangle - \lambda 100\rangle - \mu 010\rangle - \eta 001\rangle$	$U_1 \otimes U_1 \otimes U_1$
0	1	0	+	+	+	$\alpha 110\rangle + \beta 101\rangle + \gamma 011\rangle + \delta 111\rangle$ $+ \tau 000\rangle + \lambda 100\rangle + \mu 010\rangle + \eta 001\rangle$	$U_0 \otimes U_2 \otimes U_0$
0	1	0	+	-	+	$\alpha 010\rangle - \beta 001\rangle + \gamma 111\rangle + \delta 011\rangle$ $- \tau 100\rangle - \lambda 000\rangle + \mu 110\rangle - \eta 101\rangle$	$U_0 \otimes U_3 \otimes U_0$
0	1	0	+	+	-	$\alpha 010\rangle - \beta 001\rangle - \gamma 111\rangle - \delta 011\rangle$ $+ \tau 100\rangle + \lambda 000\rangle + \mu 110\rangle - \eta 101\rangle$	$U_0 \otimes U_0 \otimes U_1$
0	1	0	-	+	+	$\alpha 010\rangle + \beta 001\rangle - \gamma 111\rangle + \delta 011\rangle$ $- \tau 100\rangle + \lambda 000\rangle - \mu 110\rangle - \eta 101\rangle$	$U_1 \otimes U_0 \otimes U_0$
0	1	0	-	+	-	$\alpha 010\rangle - \beta 001\rangle + \gamma 111\rangle - \delta 011\rangle$ $- \tau 100\rangle + \lambda 000\rangle - \mu 110\rangle + \eta 101\rangle$	$U_1 \otimes U_0 \otimes U_1$
0	1	0	+	-	-	$\alpha 010\rangle + \beta 001\rangle - \gamma 111\rangle - \delta 011\rangle$ $- \tau 100\rangle - \lambda 000\rangle + \mu 110\rangle + \eta 101\rangle$	$U_0 \otimes U_3 \otimes U_1$
0	1	0	-	-	+	$\alpha 010\rangle - \beta 001\rangle - \gamma 111\rangle + \delta 011\rangle$ $+ \tau 100\rangle - \lambda 000\rangle - \mu 110\rangle + \eta 101\rangle$	$U_1 \otimes U_3 \otimes U_0$
0	1	0	-	-	-	$\alpha 010\rangle + \beta 001\rangle + \gamma 111\rangle - \delta 011\rangle$ $- \tau 100\rangle - \lambda 010\rangle - \mu 110\rangle - \eta 101\rangle$	$U_1 \otimes U_3 \otimes U_1$

Table 8.5: The relation between the local unitary operations U_{B2} performed by Bob2 and the results obtained by Alice and Bob1. The V_{xa1a2} , V_{yc1c2} , and V_{ze1e2} represents the bit value of the results of the GHZ state joint measurements on $xa1a2$, $yc1c2$ and $ze1e2$ respectively. The $P_{a1a2} \otimes P_{b1}$, $P_{yc1c2} \otimes P_{d1}$ and $P_{ze1e2} \otimes P_{f1}$ represents the parity of Alice and Bob1's results.

V_{xa1a2}	V_{yc1c2}	V_{ze1e2}	$P_{xa1a2} \otimes P_{b1}$	$P_{yc1c2} \otimes P_{d1}$	$P_{ze1e2} \otimes P_{f1}$	$ \Phi\rangle_{b2d2f2}$	U_{B2}
1	0	0	+	+	+	$\alpha 100\rangle + \beta 111\rangle + \gamma 001\rangle + \delta 101\rangle$ $+ \tau 110\rangle + \lambda 110\rangle + \mu 000\rangle + \eta 011\rangle$	$U_2 \otimes U_0 \otimes U_0$
1	0	0	+	-	+	$\alpha 100\rangle - \beta 111\rangle + \gamma 001\rangle + \delta 101\rangle$ $- \tau 010\rangle - \lambda 110\rangle + \mu 000\rangle - \eta 011\rangle$	$U_0 \otimes U_1 \otimes U_0$
1	0	0	+	+	-	$\alpha 100\rangle - \beta 111\rangle - \gamma 001\rangle - \delta 101\rangle$ $+ \tau 010\rangle + \lambda 110\rangle + \mu 000\rangle - \eta 011\rangle$	$U_0 \otimes U_0 \otimes U_1$
1	0	0	-	+	+	$\alpha 100\rangle + \beta 111\rangle - \gamma 001\rangle + \delta 101\rangle$ $- \tau 010\rangle + \lambda 110\rangle - \mu 000\rangle - \eta 011\rangle$	$U_1 \otimes U_0 \otimes U_0$
1	0	0	-	+	-	$\alpha 100\rangle - \beta 111\rangle + \gamma 001\rangle - \delta 101\rangle$ $- \tau 110\rangle + \lambda 110\rangle - \mu 000\rangle + \eta 011\rangle$	$U_3 \otimes U_0 \otimes U_1$
1	0	0	+	-	-	$\alpha 100\rangle - \beta 111\rangle - \gamma 001\rangle - \delta 101\rangle$ $- \tau 010\rangle - \lambda 110\rangle + \mu 000\rangle + \eta 011\rangle$	$U_0 \otimes U_1 \otimes U_1$
1	0	0	-	-	+	$\alpha 100\rangle - \beta 111\rangle - \gamma 001\rangle + \delta 101\rangle$ $+ \tau 010\rangle - \lambda 110\rangle - \mu 000\rangle + \eta 011\rangle$	$U_3 \otimes U_1 \otimes U_0$
1	0	0	-	-	-	$\alpha 100\rangle + \beta 111\rangle + \gamma 001\rangle - \delta 101\rangle$ $+ \tau 010\rangle - \lambda 110\rangle - \mu 000\rangle - \eta 011\rangle$	$U_3 \otimes U_1 \otimes U_1$
1	1	1	+	+	+	$\alpha 111\rangle + \beta 100\rangle + \gamma 010\rangle + \delta 110\rangle$ $+ \tau 001\rangle + \lambda 101\rangle + \mu 011\rangle + \eta 000\rangle$	$U_2 \otimes U_2 \otimes U_2$
1	1	1	+	-	+	$\alpha 111\rangle - \beta 100\rangle + \gamma 010\rangle + \delta 110\rangle$ $- \tau 001\rangle - \lambda 101\rangle + \mu 011\rangle - \eta 000\rangle$	$U_0 \otimes U_3 \otimes U_0$
1	1	1	+	+	-	$\alpha 111\rangle - \beta 100\rangle - \gamma 010\rangle - \delta 110\rangle$ $+ \tau 001\rangle + \lambda 101\rangle + \mu 011\rangle - \eta 000\rangle$	$U_0 \otimes U_0 \otimes U_3$
1	1	1	-	+	+	$\alpha 111\rangle + \beta 100\rangle - \gamma 010\rangle + \delta 110\rangle$ $- \tau 001\rangle + \lambda 101\rangle - \mu 011\rangle - \eta 000\rangle$	$U_3 \otimes U_0 \otimes U_0$
1	1	1	-	+	-	$\alpha 111\rangle - \beta 100\rangle + \gamma 010\rangle - \delta 110\rangle$ $- \tau 001\rangle + \lambda 101\rangle - \mu 011\rangle + \eta 000\rangle$	$U_3 \otimes U_0 \otimes U_3$
1	1	1	+	-	-	$\alpha 111\rangle + \beta 100\rangle - \gamma 010\rangle - \delta 110\rangle$ $- \tau 001\rangle - \lambda 101\rangle + \mu 011\rangle + \eta 000\rangle$	$U_0 \otimes U_3 \otimes U_3$
1	1	1	-	-	+	$\alpha 111\rangle - \beta 100\rangle - \gamma 010\rangle + \delta 110\rangle$ $+ \tau 001\rangle - \lambda 101\rangle - \mu 011\rangle + \eta 000\rangle$	$U_3 \otimes U_3 \otimes U_0$
1	1	1	-	-	-	$\alpha 111\rangle + \beta 100\rangle + \gamma 010\rangle - \delta 110\rangle$ $+ \tau 001\rangle - \lambda 101\rangle - \mu 011\rangle - \eta 000\rangle$	$U_3 \otimes U_3 \otimes U_3$

Chapter 9

Conclusion

This thesis dealt with two important disciplines of quantum information processing, that is, quantum key distribution and quantum secret sharing.

In the first part of the thesis, we reviewed the tools used to analyse the security proofs of the protocols which we later proposed. We also discussed some of the prominent QKD protocols and the processes involved in their practical implementation. Furthermore, we described the fundamental structure of secret sharing and also highlighted the applications of secret sharing.

We presented a three party reference frame independent QKD protocol, which can be implemented without any alignment between the sender and the receiver. In our protocol the key is extracted from the measurement of the GHZ states initially shared between the parties. We proved the security of the protocol against collective attacks. Our results shows that the protocol is very robust against these attacks as we obtained a better error rate threshold of 18.5%.

We also presented a simple security proof for the three party generic QKD protocol using the tools and methods recently used by Christandl [31]. The protocol is implemented using the GHZ states and each party has to perform a single particle measurement either on the computational basis or the Hadamard basis. The security analysis of our protocol was based on the collective attacks and we used one way information reconciliation and privacy amplification to extract the key. Eve's information was conditioned on the random variable V , which provided all the projective measurements on the density operator ρ_{ABC} . The value obtained for the error bound was $\epsilon \approx 0.031$ which is an improvement compared to the BB84 security threshold of 11% obtained in [48].

Furthermore, we proposed a scheme for sharing an arbitrary unknown three particle state to n agents using GHZ states. We showed that the unknown state can be recovered with 100% probability provided that the agents acts honestly. We also obtained a total efficiency

of $1/2n$ for our proposed scheme.

Finally, we proposed another QSTS scheme for an arbitrary unknown three particle state using EPR pairs. We found out that the scheme has a very high intrinsic efficiency and consumes less classical and quantum resources as compared to other schemes in literature [121, 122]. We obtained the total efficiency of $1/N$ for our proposed scheme.

Based on the above, regardless of the challenges that are associated with deriving security bounds for QKD protocols and proving the security of quantum secret sharing, we can conclude that the objectives of this thesis as highlighted on chapters outline we met.

Bibliography

- [1] “Squeezed Light, url=<http://www.squeezed-light.de>,” online; Accessed: 2017-03-20.
- [2] A. V. Sergienko, *Quantum communications and cryptography*. CRC press, 2005.
- [3] Wikipedia, “Secret sharing — wikipedia, the free encyclopedia,” 2017, [Online; accessed 2-March-2017]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Secret_sharing&oldid=764869233
- [4] S. Singh, *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum cryptography*. Delarcote Press, 2002.
- [5] G. V. Assche, *Quantum Cryptography and Secret Key Distillation*. Cambridge University Press, 2006.
- [6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.
- [7] R. J. Hughes, D. M. Alde, P. Dyer, G. Luther, Gabriel, L. Morgan, George, and M. Schauer, “Quantum cryptography,” *Contemporary Physics*, vol. 36, no. 3, pp. 149–163, 1995.
- [8] G. S. Vernam, “Cipher printing telegraph systems: For secret wire and radio telegraphic communications,” *Journal of the AIEE*, vol. 45, no. 2, pp. 109–115, 1926.
- [9] L. Rivest, Ronald, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
- [10] M. Elboukhari, M. Azizi, and A. Azizi, “Quantum key distribution protocols: A survey,” *International Journal of Universal Computer Sciences*, vol. 1, no. 2, pp. 59–67, 2010.

- [11] D. Naik, C. Peterson, A. White, A. Berglund, and P. G. Kwiat, “Entangled state quantum cryptography: Eavesdropping on the ekert protocol,” *Physical Review Letters*, vol. 84, no. 20, p. 4733, 2000.
- [12] H.-K. Lo and Y. Zhao, “Quantum cryptography,” *arXiv:0803.2507v4 [quant-ph]*, 2008.
- [13] C. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.
- [14] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” *Physical Review Letters*, vol. 68, pp. 557–559, 1992.
- [15] M. Musharraf, I. Khan, and M. Sher, “Protocols for secure quantum transmission: a review of recent developments,” *Information Technology Journal*, vol. 2, pp. 265–276, 2003.
- [16] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [17] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.
- [18] N. J. Cerf, G. Leuchs, and E. S. Polzik, *Quantum information with continuous variables of atoms and light*. Imperial College Press, 2007.
- [19] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.
- [20] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Physical Review Letters*, vol. 92, no. 5, p. 057901, 2004.
- [21] H. Bechmann-Pasquinucci and N. Gisin, “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography,” *Physical Review A*, vol. 59, no. 6, p. 4238, 1999.
- [22] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Physical Review Letters*, vol. 68, no. 21, p. 3121, 1992.
- [23] A. Laing, V. Scarani, J. G. Rarity, and J. L. O’Brien, “Reference-frame-independent quantum key distribution,” *Physical Review A*, vol. 82, no. 1, p. 012304, 2010.

- [24] J. Wabnig, D. Bitauld, H. Li, A. Laing, J. O’Brien, and A. Niskanen, “Demonstration of free-space reference frame independent quantum key distribution,” *New Journal of Physics*, vol. 15, no. 7, p. 073001, 2013.
- [25] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. Nock, J. Munns, D. Bonneau, P. Jiang, H. Li *et al.*, “Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client,” *Physical Review Letters*, vol. 112, no. 13, p. 130501, 2014.
- [26] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, 1948.
- [27] E. T. Jaynes, “Information theory and statistical mechanics,” *Physical review*, vol. 106, no. 4, p. 620, 1957.
- [28] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University, 2000.
- [29] F. M. Reza, *An Introduction to Information Theory*. Dover Publications, 1994.
- [30] D. J. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.
- [31] M. Christandl, R. Renner, and A. Ekert, “A generic security proof for quantum key distribution,” *arXiv:0402131v2*, 2004.
- [32] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley and Sons, 1991.
- [33] P. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing*. Oxford University Press, 2007.
- [34] T. F. Jordan, *Linear operators for quantum mechanics*. Courier Corporation, 2012.
- [35] J. Audretsch, *Entangled systems: new directions in quantum physics*. John Wiley & Sons, 2008.
- [36] U. Fano, “Description of states in quantum mechanics by density matrix and operator techniques,” *Reviews of Modern Physics*, vol. 29, no. 1, p. 74, 1957.
- [37] B. Thaller, *Advanced visual quantum mechanics*. Springer Science & Business Media, 2005.

- [38] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?” *Physical Review A*, vol. 47, no. 10, p. 777, 1935.
- [39] J. S. Bell, “On the einstein podolsky rosen paradox,” 1964.
- [40] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Going beyond bells theorem,” in *Bells theorem, quantum theory and conceptions of the universe*. Springer, 1989, pp. 69–72.
- [41] J. Preskill, *Lecture Notes for Ph219/CS219: Quantum Information*. California Institute of Technology, 2015, ch. 10.
- [42] A. Peres, *Quantum theory: concepts and methods*. Springer Science & Business Media, 2006, vol. 57.
- [43] A. S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 3–11, 1973.
- [44] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002.
- [45] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.
- [46] D. Bru, “Optimal eavesdropping in quantum cryptography with six states,” *Physical Review Letters*, vol. 81, pp. 3018–3021, 1998.
- [47] W. Heisenberg, “Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik,” *Zeitschrift für Physik*, vol. 43, no. 3-4, pp. 172–198, 1927.
- [48] P. W. Shor and J. Preskill, “Simple proof of security of the bb84 quantum key distribution protocol,” *Physical Review Letters*, vol. 85, no. 2, p. 441, 2000.
- [49] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” *Physical Review Letters*, vol. 92, p. 057901, Feb 2004.
- [50] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

- [51] P. W. Shor and J. Preskill, “Simple proof of security of the bb84 quantum key distribution protocol,” *Physical Review Letters*, vol. 85, no. quant-ph/0003004. CALT68-2264, pp. 441–444. 5 p, 2000.
- [52] W. Y. Hwan, “Quantum key distribution with high loss: Toward global secure communication,” *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.
- [53] D. Gottesman, H. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” *Quantum Information and Computation*, vol. 4, 2004.
- [54] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” lecture notes in computer science”, vol. 765, pp. 410–423, 1994.
- [55] K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” *Physical Review Letters*, vol. 89, no. 3, p. 037902, 2002.
- [56] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.
- [57] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, “Performance of two quantum-key-distribution protocols,” *Physical Review A*, vol. 73, p. 012337, Jan 2006.
- [58] C. H. Bennett, G. Brassard, and J. M. Robert, “Privacy amplification by public discussion,” *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988.
- [59] Csiszar and J. Korner, “Broadcast channels with condential messages,” *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, 1978.
- [60] I. Devetak and A. Winter, “Distillation of secret key and entanglement from quantum states,” *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, vol. 461, no. 2053, pp. 207–235, 2005.
- [61] E. Waks, A. Zeevi, and Y. Yamamoto, “Security of quantum key distribution with entangled photons against individual attacks,” *Physical Review A*, vol. 65, no. 5, p. 052310, 2002.
- [62] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, “New high-intensity source of polarization-entangled photon pairs,” *Physical Review Letters*, vol. 75, no. 24, p. 4337, 1995.
- [63] U. Leonhardt and H. Paul, “Measuring the quantum state of light,” *Progress in Quantum Electronics*, vol. 19, no. 2, pp. 89–130, 1995.

- [64] B. Kraus, N. Gisin, and R. Renner, “Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication,” *Physical Review Letters*, vol. 95, no. 8, p. 080501, 2005.
- [65] D. Mayers, “Unconditionally secure quantum bit commitment is impossible,” *Physical Review Letters*, vol. 78, no. 17, p. 3414, 1997.
- [66] M. Koashi, “Complementarity, distillable secret key, and distillable entanglement,” *arXiv:0704.3661*, 2007.
- [67] W. Wootters and W. Zurek, “Single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
- [68] W. Heisenberg, *The physical principles of the quantum theory*. Courier Corporation, 1949.
- [69] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, “Security of two quantum cryptography protocols using the same four qubit states,” *Physical Review A*, vol. 72, no. 3, p. 032301, 2005.
- [70] E. Biham and T. Mor, “Security of quantum cryptography against collective attacks,” *Physical Review Letters*, vol. 78, pp. 2256–2259, 1997.
- [71] E. Biham, M. Boyer, G. Brassard, J. Van De Graaf, and T. Mor, “Security of quantum key distribution against all collective attacks,” *arXiv preprint quant-ph/9801022*, 1998.
- [72] A. Gaidash, V. Egorov, and A. Gleim, “Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices,” in *Journal of Physics: Conference Series*, vol. 735, no. 1. IOP Publishing, 2016, p. 012072.
- [73] A. Vakhitov, V. Makarov, and D. R. Hjølme, “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography,” *Journal of modern optics*, vol. 48, pp. 2023–2038, 2001.
- [74] V. Makarov, “Quantum cryptography and quantum cryptanalysis,” Ph.D. dissertation, Norwegian University of Science and Technology, Faculty of Information Technology, Mathematics and Electrical Engineering, Department of Electronics and Telecommunications, 2007.
- [75] V. Makarov* and D. R. Hjølme, “Faked states attack on quantum cryptosystems,” *Journal of Modern Optics*, vol. 52, no. 5, pp. 691–705, 2005.

- [76] H.-K. Lo and Y. Zhao, “Quantum cryptography,” in *Computational Complexity*. Springer, 2012, pp. 2453–2477.
- [77] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, “Secure key from bound entanglement,” *Physical Review Letters*, vol. 94, no. 16, p. 160502, 2005.
- [78] M. Koashi, “Simple security proof of quantum key distribution based on complementarity,” *New Journal of Physics*, vol. 11, no. 4, p. 045018, 2009.
- [79] R. Renner and R. König, “Second theory of cryptography conference tcc,” *Lecture Notes in Computer Science*, vol. 3378, pp. 407–425, 2005.
- [80] C. L. Liu, “Introduction to combinatorial mathematics,” 1968.
- [81] G. R. Blakley, “Safeguarding cryptographic keys,” *Proceedings of the National Computer Conference 1979*, vol. 48, pp. 313–317, 1979.
- [82] A. D. Smith, “Quantum secret sharing for general access structures,” *arXiv preprint quant-ph/0001087*, 2000.
- [83] A. Marin and D. Markham, “Equivalence between sharing quantum and classical secrets and error correction,” *Physical Review A*, vol. 88, no. 4, p. 042332, 2013.
- [84] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung, “Proactive secret sharing or: How to cope with perpetual leakage,” in *Annual International Cryptology Conference*. Springer, 1995, pp. 339–352.
- [85] P. Feldman, “A practical scheme for non-interactive verifiable secret sharing,” in *Foundations of Computer Science, 1987., 28th Annual Symposium*. IEEE, 1987, pp. 427–438.
- [86] M. Backes, A. Kate, and A. Patra, “Computational verifiable secret sharing revisited,” in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2011, pp. 590–609.
- [87] L. Yuan, M. Li, C. Guo, W. Hu, and X. Tan, “A verifiable e-voting scheme with secret sharing,” in *Communication Technology (ICCT), 2015 IEEE 16th International Conference on*. IEEE, 2015, pp. 304–308.
- [88] B. Schoenmakers, “A simple publicly verifiable secret sharing scheme and its application to electronic voting,” in *Annual International Cryptology Conference*. Springer, 1999, pp. 148–164.

- [89] M. Naor and A. Wool, “Access control and signatures via quorum secret sharing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 9, no. 9, pp. 909–922, 1998.
- [90] Y. Desmedt and Y. Frankel, “Shared generation of authenticators and signatures,” in *Annual International Cryptology Conference*. Springer, 1991, pp. 457–469.
- [91] D. Gottesman, “Theory of quantum secret sharing,” *Physical Review A*, vol. 61, no. 4, p. 042311, 2000.
- [92] C. Wang, Y. Zhang, and G. Jin, “Generalized quantum state sharing of the arbitrary two particles state,” *Science China Physics, Mechanics and Astronomy*, vol. 53, no. 11, pp. 2064–2068, 2010.
- [93] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, “Multiparty quantum secret splitting and quantum state sharing,” *Physics Letters A*, vol. 354, no. 3, pp. 190–195, 2006.
- [94] R.-H. Shi, L.-S. Huang, W. Yang, and H. Zhong, “Multi-party quantum state sharing of an arbitrary two-qubit state with bell states,” *Quantum Information Processing*, vol. 10, no. 2, pp. 231–239, 2011.
- [95] C.-Y. Cheung, “Controlled quantum secret sharing,” *Physica Scripta*, vol. 74, no. 4, p. 459, 2006.
- [96] M. Jiang and D. Dong, “Multi-party quantum state sharing via various probabilistic channels,” *Quantum Information Processing*, vol. 12, no. 1, pp. 237–249, 2013.
- [97] M. Nadeem and N. U. Ain, “Secure and authenticated quantum secret sharing,” *arXiv preprint arXiv:1506.08558*, 2015.
- [98] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, “Tripartite quantum state sharing,” *Physical Review Letters*, vol. 92, no. 17, p. 177903, 2004.
- [99] M. Jiang, X. Huang, L. Zhou, Y. Zhou, and J. Zeng, “An efficient scheme for multi-party quantum state sharing via non-maximally entangled states,” *Chinese Science Bulletin*, vol. 57, no. 10, pp. 1089–1094, 2012.
- [100] Y. Li, K. Zhang, and K. Peng, “Multiparty secret sharing of quantum information based on entanglement swapping,” *Physics Letters A*, vol. 324, no. 5, pp. 420–424, 2004.

- [101] H. Yuan, Y.-M. Liu, W. Zhang, and Z.-J. Zhang, “Optimizing resource consumption, operation complexity and efficiency in quantum-state sharing,” *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 41, no. 14, p. 145506, 2008.
- [102] S. Muralidharan and P. K. Panigrahi, “Quantum-information splitting using multipartite cluster states,” *Physical Review A*, vol. 78, no. 6, p. 062333, 2008.
- [103] R. Ursin and R. Hughes, “Quantum information: Sharing quantum secrets,” *Nature*, vol. 501, no. 7465, pp. 37–38, 2013.
- [104] Y. Yu-Guang and W. Qiao-Yan, “Circular threshold quantum secret sharing,” *Chinese Physics B*, vol. 17, no. 2, p. 419, 2008.
- [105] R. Cleve, D. Gottesman, and H.-K. Lo, “How to share a quantum secret,” *Physical Review Letters*, vol. 83, no. 3, p. 648, 1999.
- [106] W. Li, C. Li, and H. Song, “Quantum synchronization and quantum state sharing in irregular complex network,” *arXiv preprint arXiv:1606.08113*, 2016.
- [107] Z. Zu-Rong, L. Wei-Tao, and L. Cheng-Zu, “Quantum secret sharing based on quantum error-correcting codes,” *Chinese Physics B*, vol. 20, no. 5, p. 050309, 2011.
- [108] B. Kraus, N. Gisin, and R. Renner, “Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication,” *Physical Review Letters*, vol. 95, no. 8, p. 080501, 2005.
- [109] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” *Physical Review A*, vol. 72, no. 1, p. 012332, 2005.
- [110] V. D’ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, “Complete experimental toolbox for alignment-free quantum communication,” *Nature communications*, vol. 3, p. 961, 2012.
- [111] X. Fang, C. Wang, Y.-G. Han, Z.-Q. Yin, W. Chen, and Z.-F. Han, “Tomographic approach in reference-frame-independent measurement-device-independent quantum key distribution,” *Communications in Theoretical Physics*, vol. 66, no. 5, p. 496, 2016.
- [112] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. Spekkens, “Robust polarization-based quantum key distribution over a collective-noise channel,” *Physical Review Letters*, vol. 92, no. 1, p. 017901, 2004.

- [113] T. Honjo, K. Inoue, and H. Takahashi, “Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit mach–zehnder interferometer,” *Optics letters*, vol. 29, no. 23, pp. 2797–2799, 2004.
- [114] H. Takesue and K. Inoue, “Generation of 1.5- μ m band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers,” *Physical Review A*, vol. 72, no. 4, p. 041804, 2005.
- [115] F. M. Spedalieri, “Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum,” *Optics communications*, vol. 260, no. 1, pp. 340–346, 2006.
- [116] L. Aolita and S. Walborn, “Quantum communication without alignment using multiple-qubit single-photon states,” *Physical Review Letters*, vol. 98, no. 10, p. 100501, 2007.
- [117] D. W. Lyons, A. M. Skelton, and S. N. Walck, “Werner state structure and entanglement classification,” *Advances in Mathematical Physics*, vol. 2012, 2012.
- [118] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, “Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and bell-state measurements,” *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, vol. 39, no. 3, pp. 459–464, 2006.
- [119] Y.-B. Sheng, F.-G. Deng, and H.-Y. Zhou, “Efficient and economic five-party quantum state sharing of an arbitrary m-qubit state,” *The European Physical Journal D*, vol. 48, no. 2, pp. 279–284, 2008.
- [120] G. Gordon and G. Rigolin, “Generalized quantum-state sharing,” *Physical Review A*, vol. 73, p. 062316, 2006.
- [121] P. Jia-Yin and M. Zhi-Wen, “Several teleportation schemes of an arbitrary unknown multi-particle state via different quantum channels,” *Chinese Physics B*, vol. 22, no. 5, p. 050310, 2013.
- [122] X.-H. Li, P. Zhou, C.-Y. Li, H.-Y. Zhou, and F.-G. Deng, “Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state,” *Journal of Physics B*, vol. 39, no. 8, p. 1975, 2006.

Appendix

Publication

C.Sekga and M.Mafu, Security proof of a three party reference frame independent quantum key distribution(QKD) protocol (2017). *(To be submitted to Physical Review A.)*

Talks Presented

Comfort Sekga and Mhlambululi Mafu, Quantum state sharing of an arbitrary three particle state using Einstein-Podolsky-Rosen pairs and GHZ state measurements, The 61st Annual Conference of the South African Institute of Physics (2016)

Poster Presented

Comfort Sekga and Mhlambululi Mafu, Multiparty Quantum State Sharing of an arbitrary unknown three particle state with GHZ state measurements, The 61st Annual Conference of the South African Institute of Physics (2016)