Non-Local Correlations and Quantum Cryptography

By
Noor Ul Ain
2013-NUST-MS-IS -62790

Supervisor
Dr. Shahzad Saleem
Department of Computing

This thesis is submitted in the partial fulfillment of the requirements for degree of Masters of Science in Information Security (MS IS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(Apr 2017)

Approval

It is certified that the contents of this thesis entitled as "**Non-Local Correlations and Quantum Cryptography"** submitted by Noor Ul Ain has been found satisfactory for the requirements of the degree.

Advisor: Dr. Shahzad Saleem
Signature:

Date:

Committee Member 1: Dr. Sajid Ali
Signature:
Date:

Committee Member 2: Mr. M. Nadeem
Signature:
Date:

Committee Member 3: Mr. Fahad Ahmed Satti
Signature:
Date:

Certificate of Originality

I hereby declare that this thesis is my own work and I have done it to the best of my knowledge. Moreover, it does not contain any material previously published or written by any another person, including the material which has been accepted as a part of any degree or diploma awarded at NUST SEECS or at some other educational institute, where ever the material is used, it has been duly acknowledgement in the thesis. Any contributions made to this research topic by other researchers, with whom I have worked at NUST SEECS or elsewhere, has been explicitly acknowledged in this thesis.

I also declare that the intellectual content of this thesis is my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: Noor Ul Ain

Signature:

Acknowledgments

I would like to thank Allah Almighty (SWT) for giving me strength and courage to successfully conduct this research. His constant support has enabled me to successfully complete all milestones of this journey.

I offer sincere gratitude to my supervisor Respected Dr. Shahzad Saleem, who provided me a great deal of his knowledge and valuable expertise in this research domain. I have to appreciate his full support, motivation and kind guidance that provided me the possibility to complete this research.

I greatly appreciate the help of Respected Teacher Mr. Muhammad Nadeem for helping me in order to refine major goals of my research. He provided me exemplary guidance, constant encouragement and mentorship to develop a valuable skill set for conducting this research along with his constant support that helped me to come this far. I am grateful to him for this amazing cooperation and marvelous support during the period of this research.

I wish to extend my thanks to my committee members Respected Dr Sajid Ali and Mr Fahad Ahmed Satti for their kind support and ideas to improve my research goals.

Finally, I want to thank my lovely parents and my dearest husband M. Danish Hassan for their complete support who encouraged me not to worry and to go my own way. It has been a long journey, but their constant support and love helped me to keep on going, even at times when the things seemed to be very difficult.
Moreover, a kind thanks to my brothers, sister whose motivation and support enabled me to successfully accomplish this goal.

I would also like to thank all my research fellows, student, staff and everyone who directly and indirectly contributed to my research work.

This thesis is dedicated to my lovely parents and my dearest husband

For their endless love, encouragement and support

"The best way to predict the future is to create it."

Peter Drucker

Contents

List of Symbols

$\left|\Phi^{+}\right\rangle = \frac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}}$ **Bell state**

$\left|\Psi^{+}\right\rangle = \frac{\left|01\right\rangle + \left|10\right\rangle}{\sqrt{2}}$ **Bell state**

$\left|\Phi^{-}\right\rangle = \frac{\left|00\right\rangle - \left|11\right\rangle}{\sqrt{2}}$ **Bell state**

$\left|\Psi^{-}\right\rangle = \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}}$ **Bell state**

σ_x **Pauli Operator / X-gate**

σ_y **Pauli Operator / Y-gate**

σ_z **Pauli Operator / Z-gate**

σ_t **Encoding Operator during Teleportation**

H**Hilbert Space**

$\otimes$ **Tensor Product**

$\langle\ |$ **Bra**

$|\ \rangle$ **ket**

$\langle .|.\rangle$ **Inner Product**

$|.\rangle\langle .|$ **Outer Product**

$|\varphi\rangle$ **Original Secret Qubit**

$|\varphi'\rangle$ **Encoded Secret Qubit**

U **Unitary Operator**

BSM **Bell State Measurements**

Abstract

Secret sharing, a building block of multiparty cryptography, ensures secure communication of any secret among a set of parties in a way that secret can only be revealed when all of the intended recipients come together and communicate with each other. Where classical cryptography assures computational security only, quantum cryptography promises information-theoretic security through the rules of quantum mechanics which have no classical counterparts such as uncertainty principle, quantum no-cloning theorem, and quantum entanglement. Based on quantum entanglement and hence non-local correlations generated by quantum teleportation and entanglement swapping, I discuss here unconditionally secure and authenticated (2,2) quantum secret sharing scheme for classical secret. Both secrecy and authenticity is assured by the sender through quantum non-local correlations based on quantum teleportation and entanglement swapping. Our security protocol is proved to be secure against internal and external eavesdropping along with the attacks during sharing and reconstruction of secrets for (2,2) threshold scheme. Another feature of this protocol is that it detects both active and passive eavesdropping strategies.

Chapter 1

Introduction

"A quantum computer, if built, will be to an ordinary computer as a hydrogen bomb is to gunpowder, at least for some types of computations." – [1](PE Black)

1.1 Background

Cryptography is the field of science used to design and implement systems capable of performing encryption and decryption of data. The word cryptography is formed by two Greek words kryptos meaning 'hidden', and graphein meaning 'to write'[2]. The purpose of the cryptosystems is to protect the confidential messages. Cryptosystems use one-way functions, factorization of large prime numbers, discrete logarithmic problems or computationally complex algorithms to encrypt the messages, which makes it computationally hard to invert the message back to original form.[3] The security of classical cryptosystems depends upon the strong computational power i.e. if enough computational power is achieved the security of classical cryptography may be compromised.

Unlike classical cryptosystems, the security of quantum cryptosystems is based on the laws of quantum physics[4] instead of mathematical assumptions. This enables the ways to design unconditionally secure cryptographic systems by depending on inherent secure nature of quantum physics.

Main features of quantum cryptography that make it secure are quantum no cloning theorem and quantum entanglement. Where quantum no cloning theorem states that it is impossible to create identical copy of an unknown quantum state[5] and quantum entanglement refers to a physical phenomenon that occurs when pair or group of particles are generated in a way that the quantum state of each particle cannot be described independently, so those particles are represented by a single state.[6]

Quantum no cloning theorem restricts the interception and cloning of any encrypted message whereas Quantum entanglement refers to the behavior of two non-locally correlated and spatially separated quantum particles. In depth details of quantum no cloning theorem and quantum entanglement along with other necessary building blocks of quantum cryptography are discussed in chapter 3.

1.2 Motivation

The motivation behind choosing quantum cryptography as the field of research in thesis is due to the inherent strength guaranteed by laws of quantum mechanics to ensure that instead of making the computations more complex (the factor which can be superseded, if, we get enough computational power), unconditional secure cryptographic security protocols can be designed that would be able to cope up against active and passive attacks.
Thus, the focus of this thesis will be to develop secure cryptographic protocol with the use of quantum non local correlations in order to ensure a secure and authenticated quantum secret sharing protocol.

1.3 Secret Sharing

Secret sharing allows a sender to share his secret among multiple parties in a way that a specific set or all parties have to collaborate together to extract the secret message. [7]

1.3.1 Classical Secret Sharing

Shamir[7] introduced the idea of classical secret sharing where an encrypted classical message was sent to multiple parties and later on, parties had to collaborate together and apply a predefined decryption function to extract the secret message. Classical secret sharing was distributed into two types. (n,n) threshold scheme and (k,n) threshold scheme. In (n,n) threshold scheme, secret message was divided into n parts and then those parts were sent to n parties. When they wanted to extract the secret all n parties had to collaborate and provide their share to extract the secret message into original form[7]. Whereas, in (k,n) threshold scheme, secret was divided and sent to n parties and if k or more than k parties collaborate together, they will be able to extract the secret message into original form, (here n=2k-1) [8] .This idea was later extended by Hillary to apply secret sharing on qubits (*quantum bit, just like classical bit, but qubit can be both 0 or 1 at the same time.*) in quite the same way as that of classical secret sharing to introduce unconditional secure message communication.

1.3.2 Quantum Secret Sharing

The idea of secret sharing in the field of quantum computing was introduced by Hillary [2]. The key difference between classical secret and quantum secret resides in transformation of secret back to its original shape. In classical cryptography, the sequence of bits is recovered, whereas in quantum cryptosystems, a physical particle (qubit- quantum bit) is brought back to its original state. Quantum cryptosystems follow the laws of quantum mechanics instead of classical cryptosystems schemes.[9]

1.4 Problem Statement

Following problem statement is addressed in this thesis: Suppose a Business man maintains a safe vault to receive confidential documents. He wants to get the recently received confidential file. He wants to avoid tampering and ensure confidentiality of the file. So, instead of revealing the password to a single authority, the password will be revealed to three authorities in parts to avoid misuse of the document. Now if it becomes mandatory to misuse the document three authorities should collectively decide to tamper the document.

In the terminology of cryptography, this issue is termed as "*secret sharing*". The issue works as, if someone wants to share a secret among a group of parties instead of a single person in a way that a specific group can cooperate to recover the secret. This scheme is termed as (k,n) threshold scheme [8]. Another scheme is to share the secret among n parties and all the parties must communicate with each other to extract the secret message. This is termed as (n,n) threshold scheme [7]. These secret sharing schemes have their applications in secret key distribution along with many multi-party protocols.

If we use classical cryptography to share secret between the parties, there is a possibility that someone could actively or passively eavesdrop the information or the attacker has enough computational power to perform brute force attack, the system could be over ruled.[10] In order to avoid such issues, a system is to be designed based on the laws immaterial of computational power. Such system can be designed with the help of Quantum cryptography because of inherent secure nature of quantum physics {no cloning theorem and quantum measurement rule (*whenever a quantum state is measured, it gets converted into classical bit and it cannot be converted back into original qubit before measurement*,[11] *so if somebody tries to measure an unknown qubit, it will be changed into classical bit and eavesdropper will not be able to get the initial qubit state to be used for an attack*)}.

So now, to avoid the attacks possible in classical cryptography, some researchers moved to quantum cryptography. Many schemes have been provided in quantum cryptography to overcome the issues of classical cryptography, but there are some problems in existing quantum secret sharing schemes as well. The main issues in existing schemes include lack of proper authentication of the parties involved in secret sharing scheme along with overhead of qubits. Thus, the aim of this thesis will be to provide a secret sharing scheme in quantum cryptography with proper authentication mechanism and minimum number of qubits will be used to ensure secure and authenticated secret sharing scheme.

1.5 Outline of Thesis

This thesis is organized as follows. Chapter 2 describes the basic mathematical preliminary concepts to understand quantum mechanics. In Chapter 3 basics of quantum cryptography will be presented. Chapter 4 will provide an in depth literature review to discuss the existing quantum

secret sharing schemes and the problems with those scheme to extract our problem statement. In Chapter 5 proposed protocol will be discussed. Finally, in Chapter 6 stepwise security analysis along with conclusions and future work will be presented.

Chapter 2

Quantum Mechanics

In this chapter, underlying structure of quantum mechanics and its postulates are revisited to understand the fundamentals of quantum cryptography. These concepts will help to build a basic idea of how cryptography works in quantum domain.

2.1 Hilbert Space

In quantum physics, possible states of a physical system are described with the help of unit vectors in *Hilbert space*; a complex vector space with inner product[12]. A complex vector space V is a set of vectors $|\psi\rangle, |\psi_1\rangle, |\psi_2\rangle, \ldots\ldots$ together with a set of scalars (ordinary complex numbers) $\alpha, \beta, \ldots\ldots$ bounded by vector addition and scalar multiplication:

2.1.1 Vector Addition

$$|\psi_1\rangle + |\psi_2\rangle = |\psi_3\rangle \tag{2.1}$$

$$|\psi_1\rangle + |\psi_2\rangle = |\psi_2\rangle + |\psi_1\rangle \tag{2.2}$$

$$(|\psi_1\rangle + |\psi_2\rangle) + |\psi_3\rangle = |\psi_1\rangle + (|\psi_2\rangle) + |\psi_3\rangle) \tag{2.3}$$

$$|0\rangle + |\psi_1\rangle = |\psi_1\rangle \tag{2.4}$$

$$|\psi_1\rangle + |-\psi_1\rangle = |0\rangle \tag{2.5}$$

2.1.2 Scalar Multiplication

$$\alpha|\psi_1\rangle = |\psi_2\rangle \tag{2.6}$$

$$\alpha\left(|\psi_1\rangle + |\psi_2\rangle\right) = \alpha|\psi_1\rangle + \alpha|\psi_2\rangle \tag{2.7}$$

$$(\alpha+\beta)|\psi_1\rangle = \alpha|\psi_1\rangle + \beta|\psi_1\rangle \tag{2.8}$$

$$\alpha\left(\beta|\psi_1\rangle\right) = \beta\left(\alpha|\psi_1\rangle\right) = \alpha\beta|\psi_1\rangle \tag{2.9}$$

$$1|\psi_1\rangle = |\psi_1\rangle \tag{2.10}$$

$$|-\psi_1\rangle = (-1)|\psi_1\rangle \tag{2.11}$$

$$0|\psi_1\rangle = |0\rangle \tag{2.12}$$

2.2 Dual Vector Space

Corresponding to every vector $|\psi\rangle$ in a vector space [13], there is a dual vector $\langle\psi|$ in dual vector space bounded by same vector addition and multiplication rules. These rules are described below: Here

$$\langle\psi| = |\psi\rangle^{\dagger} = \left(|\psi\rangle^{T}\right)^{*} \tag{2.13}$$

Where the symbol † is called Hermitian Conjugate.

2.2.1 Vector Addition

$$\langle\psi_1| + \langle\psi_2| = \langle\psi_3| \tag{2.14}$$

$$\langle\psi_1| + \langle\psi_2| = \langle\psi_2| + \langle\psi_1| \tag{2.15}$$

$$\langle\psi_1| + \left(\langle\psi_2| + \langle\psi_3|\right) = \left(\langle\psi_1| + \langle\psi_2|\right) + \langle\psi_3| \tag{2.16}$$

$$\langle\psi_1| + \langle 0| = \langle\psi_1| \tag{2.17}$$

$$\langle\psi_1| + \langle -\psi_1| = |0\rangle \tag{2.18}$$

2.2.2 Scalar Multiplication

$$\alpha\langle\psi_1| = \langle\psi_2| \tag{2.19}$$

$$\alpha\left(\langle\psi_1| + \langle\psi_2|\right) = \alpha\langle\psi_1| + \alpha\langle\psi_2| \tag{2.20}$$

$$(\alpha+\beta)\langle\psi_1| = \alpha\langle\psi_1| + \beta\langle\psi_1| \tag{2.21}$$

$$\alpha(\beta)\langle\psi_1| = \beta\left(\alpha\langle\psi_1|\right) = \alpha\beta\langle\psi_1| \tag{2.22}$$

$$1\langle\psi_1| = \langle\psi_1| \tag{2.23}$$

$$\langle -\psi_1| = (-1)\langle\psi_1| \tag{2.24}$$

$$0\langle\psi_1| = |0\rangle \tag{2.25}$$

2.3 Inner Product

Inner product of two vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ is a complex number and it is written as:

$$\langle\psi_1|\psi_2\rangle \tag{2.26}$$

Inner product has following properties:

$$\langle\psi_1|\psi_2\rangle = \langle\psi_2|\psi_1\rangle^* \tag{2.27}$$

$$\langle\psi_1|\psi_1\rangle \geq 0 \tag{2.28}$$

$$\langle\psi_1|\psi_1\rangle = 0 \Leftrightarrow |\psi_1\rangle = 0 \tag{2.29}$$

$$\langle\psi_1|\left(\alpha|\psi_2\rangle + \beta|\psi_2\rangle\right) = \alpha\langle\psi_1|\psi_2\rangle + \beta\langle\psi_1|\psi_2\rangle \tag{2.30}$$

As inner product of any vector with itself is a nonnegative number, so its square root is real and is called norm of vector.

$$\|\psi_2\| = \sqrt{\langle\psi_2|\psi_2\rangle} \tag{2.31}$$

A vector whose norm is 1, is termed as normalized vector.

$$\|\psi_2\| = \sqrt{\langle\psi_2|\psi_2\rangle} = 1 \tag{2.32}$$

If inner product of two vectors is zero, they are called orthogonal (generalization of notion perpendicular in case of dot product.)

$$\langle\psi_1|\psi_2\rangle = 0 \tag{2.33}$$

2.4 Postulates of Quantum Mechanics

There are four main postulates of quantum mechanics to understand working of quantum world, that are explained in depth here.

2.4.1 First Postulate

"Every quantum system is described completely by a state vector. All properties of the system can be deduced from the state vector."[14]

A quantum system can be represented in this form:

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \alpha_3|\psi_3\rangle + ... = \sum_{i=1}^{N} \alpha_i|\psi_i\rangle \tag{2.34}$$

Where $\psi_1, \psi_2, \psi_3 \ldots$ are the basis and $\alpha_1, \alpha_2, \alpha_3$ are the corresponding weights for these states. Moreover, eq.(2.34) can be expressed in vector form as well:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ . \\ . \\ \alpha_N \end{pmatrix} \tag{2.35}$$

Qubit:

Qubit stands for Quantum Bit. It is generated via electron, photon or any other atom. It is the same as classical bit but it is basically the superposition of $|0\rangle$ and $|1\rangle$.[14] That is:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.36}$$

Moreover, if written in vector form, eq (2.36) can be expressed as:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{2.37}$$

A Qubit can b an atom, electron or photon.
In case of atom, it has 2 states:
Ground state is represented as $|0\rangle$ whereas excited state is represented by $|1\rangle$.
Similarly, in case of electron, the 2 states are:
Spin up, which is represented by $|0\rangle$ and spin down state which is represented by $|1\rangle$.

If we talk about photon, it also has 2 states:
Horizontal polarization represented by $|0\rangle$ and vertical polarization is represented by $|1\rangle$

2.4.2 Second Postulate

"*The probability of a measurement on a quantum system giving a certain result is determined by the weight of the relevant basis state in the state vector. After the measurement, the system is in the state corresponding to the result of the measurement."*[14]

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

When qubits are measured, they give us two possible measurements in general: $|0\rangle$ or $|1\rangle$. Similarly, as described in eq. (2.36) where qubits are in superposition state, if it is wished to find out the probability or likeliness of finding a qubit in a specific state, it can be measured in following way:

$$P(0)= \alpha^*\alpha = |\alpha|^2 \tag{2.38}$$

$$P(1) = \beta^*\beta = |\beta|^2 \tag{2.39}$$

The major rule to be followed in this regard for superposition to hold is:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.40}$$

Now if quantum state was in $|0\rangle$ or $|1\rangle$ and it is wished to measure in $|+\rangle$ or $|-\rangle$ or vice versa, do following:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.41}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.42}$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \tag{2.43}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{2.44}$$

State of Qubit from eq. (2.36) will be found by putting eq.(2.43) and eq.(2.44) in eq.(2.36)

$$|\psi\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{2.45}$$

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \tag{2.46}$$

2.4.2.1 Quantum Measurement Rule

The probability of a measurement on a quantum system giving a certain result is determined by the weight of the relevant basis state in the state vector. After the measurement, the system remains in the state corresponding to the result of the measurement [14].
Measurement of the quantum system has to made with respect to certain basis.
Measurement of the state from eq. (2.36)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.36}$$

w.r.t {+,-} basis can only yield two possible results: |+⟩ or |-⟩ with probability P(+) or P(-) respectively. Whereas:

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

Putting these values in eq. (2.36), we get, (2.47) and (2.48):
In order to find P(+) and P(-), we will use those equations:

$$P(+) = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)^2 \tag{2.47}$$

$$P(-) = \left(\frac{\alpha-\beta}{\sqrt{2}}\right)^2 \tag{2.48}$$

2.4.2.2 Projection Operator for Quantum Measurements

If the state of a quantum system is $|\psi\rangle$ immediately before the measurement, the likeliness that result m occurs is

$$\Pr(m) = \langle\psi|P_m|\psi\rangle \tag{2.49}$$

Where $\langle\psi| = (|\psi\rangle^{\tau})^*$ and

$$P_m|\psi\rangle = |m\rangle\langle m\|\psi\rangle \tag{2.50}$$

Similarly, after the measurement, the system remains in the state corresponding to the result of the measurement.

$$|\psi'\rangle = \frac{P_m|\psi\rangle}{\sqrt{\langle\psi|P_m|\psi\rangle}} \tag{2.51}$$

Measurements are made with respect to any particular basis. In quantum mechanics, the only way to pull the information out of qubit about its state is possible through measurement. And from the

no- cloning theorem when a state is measured it changes permanently and thus any attacker can easily be detected. This feature of quantum mechanics makes quantum cryptography unconditionally secure.

2.4.3 Third Postulate

"The evolution of a closed quantum system is described by a unitary transformation."[14]
For this particular condition to hold, the matrix (gate) deployed must have following properties:

Hermitian:

A square matrix with complex entries, which is equal to its own conjugate transpose. That is,

$$U^{\dagger} = U \tag{2.52}$$

$$U^{\dagger} = (U^{T})^{*} \tag{2.53}$$

Unitary:

A matrix should satisfy following condition:

$$UU^{\dagger} = I \tag{2.54}$$

$$U^{\dagger} = U^{-1} \tag{2.55}$$

The main strength of quantum systems is that the gates used in quantum systems are reversible as compared to the classical gates which are irreversible. Thus any quantum system can determine the inputs to the gates by knowing the outputs.

2.4.3.1 Quantum Gates

Basic quantum gates along with their associated matrix are described here.[15]

Quantum NOT Gate

The operation of quantum not gate is:

$$X|0\rangle = |1\rangle \tag{2.56}$$

$$X|1\rangle = |0\rangle \tag{2.57}$$

The particular transformation matrix for this gate is:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Quantum Phase Flip Gate

The operation of quantum phase flip is:

$$Z|0\rangle = |0\rangle \tag{2.58}$$

$$Z|1\rangle = -|1\rangle \tag{2.59}$$

The particular transformation matrix for this gate is:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Quantum Phase Flip+ NOT Gate

$$Y|0\rangle = -i|1\rangle \tag{2.60}$$

$$Y|1\rangle = i|0\rangle \tag{2.61}$$

The particular transformation matrix for this gate is:

$$\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

Phase Shift Gate

$$P|0\rangle = |0\rangle \tag{2.62}$$

$$P|1\rangle = e^{i\theta}|1\rangle \tag{2.63}$$

The particular transformation matrix for this gate is:

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Hadamard Gate

Hadamard gate transforms classical state into quantum superposition state by following manner:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.64}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.65}$$

The particular transformation matrix for this gate is:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$$

Controlled Not Gate

$$C|0,x\rangle = |0,x\rangle \tag{2.66}$$

$$C|1,x\rangle = |1,1-x\rangle, x \in \{0,1\} \tag{2.67}$$

The particular transformation matrix for this gate is:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2.4.4 Fourth Postulate

"The state space of a composite physical system is the tensor product of the state space of the component systems"[14]
In order to find the tensor product of a composite system, following computation is performed:

$$|\psi_{1,2}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \tag{2.68}$$

$$|\psi_{1,2}\rangle = |\psi_1\rangle|\psi_2\rangle \tag{2.69}$$

$$|\psi_{1,2}\rangle = |\psi_1\psi_2\rangle \tag{2.70}$$

This can be well elaborated by a composite system having two qubits as shown ahead:
Considering two independent qubits:

$$|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{2.71}$$

$$|\psi_2\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{2.72}$$

The tensor product of eq. (2.71) and eq.(2.72) will be eq. (2.76):

$$|\psi_{1,2}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \tag{2.73}$$

$$|\psi_{1,2}\rangle = \left(\alpha_0|0\rangle + \alpha_1|1\rangle\right) \otimes \left(\alpha_0|0\rangle + \alpha_1|1\rangle\right) \tag{2.74}$$

$$|\psi_{1,2}\rangle = \alpha_0\alpha_0|00\rangle + \alpha_0\alpha_1|01\rangle + \alpha_1\alpha_0|10\rangle + \alpha_1\alpha_1|11\rangle \tag{2.75}$$

$$|\psi_{1,2}\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{2.76}$$

Chapter 3

Methods of Quantum Cryptography

This chapter covers the basic and fundamental concepts of quantum cryptography including uncertainty principle, quantum no-cloning theorem, entanglement, quantum teleportation, entanglement swapping, and super dense coding. All these concepts are discussed here to grab the idea that how quantum mechanics lead to secure and authenticated quantum secret sharing schemes to be discussed in chapters 4 and 5.

3.1. Uncertainty Principle

According to Heisenberg uncertainty principle, in quantum world where the particles to be observed are at atomic scale, the more precisely you know the position (i.e., the smaller Δx) the less accurate will be the momentum [16](i.e., the larger Δp) and vice versa. It is therefore impossible to know both the position and momentum exactly, i.e.

$$\Delta x \Delta p \geq \frac{h}{4\pi} \tag{3.1}$$

Remember that the uncertainties in position and momentum are very small at quantum scale and cannot be detected by the observer. Similarly, the value of h (Planck's constant) is also very small so these uncertainties cannot be observed in our everyday life.

The relationship of Heisenberg uncertainty principle can be described in terms of energy and time. The more accurately you know the energy of a body, the lesser accurate you will know that how long the body possessed that energy. In this way the relationship can be expressed as follows:

$$\Delta E \Delta t \geq \frac{h}{4\pi} \tag{3.2}$$

3.2 No-Cloning Theorem

Wootters, Zurek and Dieks in 1982 proposed a theorem that, *" it is impossible to create an identical copy of an arbitrary unknown quantum state".*[5]

Proof

If a quantum state can be cloned, then the following conditions must be satisfied:

$$U|\psi_1\rangle|0\rangle = |\psi_1\rangle|\psi_1\rangle \tag{3.3}$$

$$U|\psi_2\rangle|0\rangle = |\psi_2\rangle|\psi_2\rangle \tag{3.4}$$

Take inner products of left hand sides of both (3.3) and (3.4)

$$\left(\langle\psi_1|\langle 0|U^\dagger\right)\left(U|\psi_2\rangle|0\rangle\right) = \langle\psi_1|\psi_2\rangle\langle 0|0\rangle\right) = \langle\psi_1|\psi_2\rangle \tag{3.5}$$

Now, take inner product of right hand sides of both (3.3) and (3.4)

$$\left(\langle\psi_1|\langle\psi_1|\right)\left(|\psi_2\rangle|\psi_2\rangle\right) = \langle\psi_1|\psi_2\rangle\langle\psi_1|\psi_2\rangle = |\langle\psi_1|\psi_2\rangle|^2 \tag{3.6}$$

Now from (3.5) and (3.6),

$$\langle\psi_1|\psi_2\rangle \neq |\langle\psi_1|\psi_2\rangle|^2 \tag{3.7}$$

From (3.7) it is clear that an unknown quantum state cannot be copied.

3.3 Quantum Entanglement

Quantum entanglement is a physical phenomenon that occurs when pair or group of particles are generated in a way that the quantum state of each particle cannot be described independently.[6] Instead, a quantum state must be described for the system as a whole. That is, if $|\psi\rangle$ represents a maximally entangled state of two quantum particles, then there are no single qubit states $|\alpha\rangle$ and $|\beta\rangle$ such that

$$|\psi\rangle = |\alpha\rangle \otimes |\beta\rangle \tag{3.10}$$

For example, the four maximally entangled Bell states

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.11}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \tag{3.12}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{3.13}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{3.14}$$

3.4. Quantum Teleportation

Quantum teleportation is a process through which quantum information can be sent from one location to another with the help of pre shared entanglement and classical communication.[14] This information transfer is unconditionally secure even if classical communication is sent over public channel. In general, teleportation works as follows:
(1) Alice and Bob share an entangled Pair of particles (e.g.: eq. (3.8))

$$\left|\Phi^{+}\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

where 1st qubit belongs to Alice and 2nd Belongs to Bob.
(2) Alice applies CNOT gate on product of the qubit to be transmitted $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and her particle of EPR.

$$(\alpha|0\rangle + \beta|1\rangle)\otimes\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \tag{3.15}$$

$$\frac{\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle)}{\sqrt{2}} \tag{3.16}$$

$$\frac{\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle)}{\sqrt{2}} \tag{3.17}$$

Or

$$\left(\frac{\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)}{\sqrt{2}}\right) \tag{3.18}$$

(3) Alice applies Hadamard gate on (3.18) where

$$H|0\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \tag{3.19}$$

$$H|1\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{3.20}$$

$$\alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|10\rangle + |01\rangle}{\sqrt{2}}\right) \tag{3.21}$$

$$\left(\frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + (|01\rangle(\alpha|1\rangle + \beta|0\rangle)) + (|10\rangle(\alpha|0\rangle - \beta|1\rangle)) + (|11\rangle(\alpha|1\rangle - \beta|0\rangle))\right) \tag{3.22}$$

(4) Alice measures her pair and gets two classical bits while Bob's particle transforms into one of the four possible states as shown in table below:

Alice Measurement outcome	Bob's EPR half
00	$\alpha\|0\rangle + \beta\|1\rangle$
01	$\alpha\|1\rangle + \beta\|0\rangle$
10	$\alpha\|0\rangle - \beta\|1\rangle$
11	$\alpha\|1\rangle - \beta\|0\rangle$

Tab 3.1: Alice's BSM measurement outcome and corresponding possibilities on Bob's side.

(5) Alice sends her measurement outcome to Bob over public classical channel.
(6) Bob then applies one of the four Pauli operators corresponding to Alice's measurement outcome and gets the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

3.5. Entanglement Swapping

Entanglement swapping, an extension of teleportation, entangles two quantum particles in one of the four Bell states even if they have never been interacted. Entanglement swapping starts with two pairs of EPR, the first shared between Alice and Bob while other shared between Alice and Charlie where Bob and Charlie have never met one another [17]. By performing Bell state measurement (BSM) on particles in her possession, Alice can project Bob's and Charlie's particles into one out of the four Bell states ($\beta_{00}, \beta_{01}, \beta_{10}, \beta_{11}$).

Suppose Alice and Bob share an entangled state $|\beta_{00}\rangle_{ab} = (|0_a 0_b\rangle + |1_a 1_b\rangle)/\sqrt{2}$ whereas Alice and Charlie share an entangled state $|\beta_{00}\rangle_{ac} = (|0_a 0_c\rangle + |1_a 1_c\rangle)/\sqrt{2}$. Their composite system

$$|\beta_{00}\rangle_{ab}|\beta_{00}\rangle_{ac} = \left(\frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}}\right)\left(\frac{|0_a 0_c\rangle + |1_a 1_c\rangle}{\sqrt{2}}\right) \tag{3.24}$$

can be rewritten as

$$|\beta_{00}\rangle_{ab}|\beta_{00}\rangle_{ac} = \frac{1}{2}\left(|0_a 0_b\rangle|0_a 0_c\rangle + |0_a 0_b\rangle|1_a 1_c\rangle + |1_a 1_b\rangle|0_a 0_c\rangle + |1_a 1_b\rangle|1_a 1_c\rangle\right) \tag{3.25}$$

After rearranging the qubits, we can write Alice's qubits together and qubits in possession of Bob and Charlie together as

$$|\beta_{00}\rangle_{ab}|\beta_{00}\rangle_{ac} = \frac{1}{2}\left(|0_a 0_a\rangle|0_b 0_c\rangle + |0_a 1_a\rangle|0_b 1_c\rangle + |1_a 0_a\rangle|1_b 0_c\rangle + |1_a 1_a\rangle|1_b 1_c\rangle\right) \tag{3.26}$$

$$|\beta_{00}\rangle_{ab}|\beta_{00}\rangle_{ac} = \frac{1}{2}\left(|\beta_{00}\rangle_{aa}|\beta_{00}\rangle_{bc} + |\beta_{01}\rangle_{aa}|\beta_{01}\rangle_{bc} + |\beta_{10}\rangle_{aa}|\beta_{10}\rangle_{bc} + |\beta_{11}\rangle_{aa}|\beta_{11}\rangle_{bc}\right) \tag{3.27}$$

If Alice performs BSM on her qubits, Bob's and Charlie's particles get entangled into one of the four Bell states as follows:

If Alice gets $(\beta_{00})_{\mathbf{aa}}$	Bob's and Charlie's particles get entangled into one of the four Bell state $(\beta_{00})_{\mathbf{bc}}$
If Alice gets $(\beta_{01})_{\mathbf{aa}}$	Bob's and Charlie's particles get entangled into one of the four Bell state $(\beta_{01})_{\mathbf{bc}}$
If Alice gets $(\beta_{10})_{\mathbf{aa}}$	Bob's and Charlie's particles get entangled into one of the four Bell state $(\beta_{10})_{\mathbf{bc}}$
If Alice gets $(\beta_{11})_{\mathbf{aa}}$	Bob's and Charlie's particles get entangled into one of the four Bell state $(\beta_{11})_{\mathbf{bc}}$

Tab 3.2: Results of Entanglement Swapping between Alice, Bob and Charlie

3.6. Super Dense Coding

Super dense coding is one of the most promising and simple application of quantum mechanics. It is a perfect illustration of communication tasks to be fulfilled by quantum mechanics [3]. Super dense coding involves two distant parties, let's say 'Alice' and 'Bob'. The purpose is to convey classical information from Alice to Bob, two distant parties who share a pair of qubits in the entangled state:

$$|\beta_{00}\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \tag{3.28}$$

By sending single qubit in her possession to Bob, Alice can communicate two classical bits of with Bob as follows:
(1) if Alice desires to send the bit string '00' to Bob then she does entirely nothing to her qubit and simply transmits the qubit in her possession to Bob.
(2) If Alice wants to send '01' then she applies quantum NOT gate or X to her qubit and transmits to Bob.
(3) If Alice wants to send '10' then she applies the phase flip Z gate to her qubit and transmits to Bob.
(4) If Alice wants to send '11' then applies both NOT gate or X as well as phase flip Z gate to her qubit and transmits to Bob.

After receiving the qubit sent by Alice, Bob measures both qubits in the Bell basis and gets two classical bits sent from Alice. In this way, by transmitting only a single qubit, Alice can communicate two classical bits to Bob.

3.7. Quantum Key Distribution

Quantum key distribution (QKD) applies fundamental laws of quantum physics to guarantee secure communication. It enables two legitimate users to produce a shared secret random bit string to be used as a key in cryptographic applications, such as message encryption and authentication. Unlike conventional cryptography, whose security relies on computational assumptions, QKD promises unconditional security based on the fundamental laws of quantum mechanics (quantum measurement and no cloning theorem).

3.7.1 QKD: BB84 Protocol

BB84 uses three key principles:[13]

1. No-cloning theorem
2. Measurement leads to state collapse.
3. Measurements are irreversible.

Channel Conditions

Suppose sender and receiver share two channels between them:

Quantum channel where active attacks are possible from Eve.

Classical private channel where passive attacks are allowed but active are not allowed:

- Eve can passively listen their communication.
- Eve cannot actively alter their communication.

Protocol Steps

Protocol is divided into three phases. Situation at sender side, Situation at receiver side and key announcement.

1. **Situation at Sender Side:**

Sender generates a random and private classical bit-string s=1011010110. Sender then generates equivalent quantum string $|q\rangle = |011010110\rangle$. After that sender applies Hadamard & identity gates randomly e.g.: HIHIHIHIII

As a result, quantum state becomes $|q\rangle = |-0-1+1+110\rangle$. Sender will send this information to receiver over quantum channel.

2. **Situation at Receiver Side:**

Receiver will receive a quantum state $|q\rangle = |-0-1+1+110\rangle$ and will randomly apply Hadamard and identity gates e.g.: HHIIHHIIHI. Quantum state will become $|q\rangle = |1+-10-+1-0\rangle$

Finally, sender will measure the state in {0,1} basis. Result of receiver's measurement will be same as that of sender bit string where they applied same encoding scheme, otherwise result will be probabilistic (50-50).

3. **Key Announcement:**

Sender and Receiver will publicly announce the encoding and decoding scheme used. They will retain only those qubits for which they chose same scheme. For example:

S=H I H I H I H I I I

R=H H I I H H I I H I

The same encoding and decoding is used in first, fourth, fifth, eighth and tenth place. Sender will then publicly announce the values of a subset of the retained bits. Receiver will check to see whether his measurements are the same.

If so, they will use the undisclosed bits as a private key for future secure communication.

Chapter 4

Quantum Secret Sharing – Literature Review

Quantum cryptography utilizes quantum physics to achieve cryptographic tasks and to break classical cryptographic systems. In order to break cryptographic systems, higher computational power proposed by quantum systems is estimated to break any complex cryptographic algorithm. Another significant feature of quantum systems is quantum no-cloning theorem that mitigates both active and passive eavesdropping.
The inspiration behind choosing quantum cryptography over classical cryptography is due to the inherent features proposed by quantum mechanics such as Quantum No-Cloning theorem, quantum measurement rule, quantum entanglement, quantum teleportation and others.
Another reason for preferring quantum cryptography over classical cryptography is, the enhanced computational power associated with quantum computers as compared to classical computers.

4.1 Secret Sharing

Concept of secret sharing evolved in 1979 by Adi Shamir [7]. In classical cryptography, if a person wants to share a secret between multiple parties such that if all of them come together and combine the message sent to them, they will be able to extract the message, not otherwise. This concept ensured honesty among secret keeping parties. The protocol proposed by Adi Shamir for secret sharing is as follows:
Take the original message to be sent and encrypt it. Now divide the message into n parts, in such a way that any k parts together could be able to extract the original message. Similarly, any k-1 or less parts of message should be of no use. Where n=2k-1. This scheme is termed as (k,n) threshold scheme.
This protocol has its limitations and it fails in classical cryptography because of the possibility of passive attacks in classical cryptography. Moreover, computational power can easily overrule this protocol. So one needs a secure algorithm independent of computational complexity. For this reason, we are moving towards quantum systems to ensure the secrecy of protocols independent of computational complexity.

4.2 Quantum Secret Sharing

Quantum Secret Sharing was initially proposed by Hillary[18]. QSS is the same as classical secret sharing with a difference that now instead of classical bits, qubits are used to share secret. This protocol starts with original message at sender side where the sender first encrypts the message and after encryption, divides the message into parts. These parts are then sent to the parties

involved in secret sharing. At the end to extract the secret all the parties need to collaborate together to decrypt the secret message. A generic architecture of secret sharing can be described by Fig.4.1

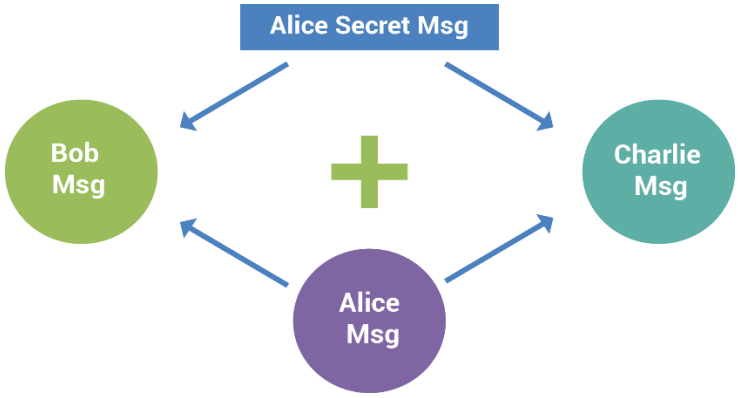

Fig. 4.1 Generic Secret Sharing Protocol

4.3 Quantum Secret Sharing Protocols

Hillary introduced the idea of doing secret sharing in terms of qubits and introduced the concept of Quantum Secret Sharing (QSS). He proposed that in quantum cryptography secure secret sharing could be possible among 3 parties via entangled GHZ states and entanglement swapping. This was done by applying operators on the entangled qubits and then sharing the measurement results among the parties to extract the secret. This idea was then generalized to N parties.

Later on [17], [19]–[23] proposed various protocols for quantum secret sharing on basis of entanglement, swapping, teleportation, bell states, GHZ states, super dense coding, local unitary operations, single photons and others.

Moreover, some researches utilized entanglement along with GHZ/ W/ Bell states [24]–[29]. In most of these cases the sender measured the entangled qubits in their possession without actually sending them over a channel to share the secret.

Some researchers proposed ways to apply local unitary operators on the qubits in possession of each party and then the parties shared their measurement results to extract the secret. This research was done in two ways [12]–[25]:

[a] the sender used the local unitary operator and by the measurements and collaboration among the parties; they can extract the results.

[b] the sender tells the measurement results and on basis of those results, parties determine the operator applied on qubits by the sender. This operator is matched with a pre-decided encoding on specific classical bits which was referred to be the secret in that case.

Some researchers proposed to perform secret sharing without performing entanglement [19], [23]. In contrast some researchers proposed ways to achieve secret sharing by using entanglement but without applying local unitary operators to exchange secret messages [24], [29], [30].

Here we will discuss quantum secret sharing with single particle, two particle and three particle states, along with relevant issues in them to generate our problem statement.

4.3.1 Quantum Secret Sharing Protocols with One Particle

Initially researchers started to propose quantum secret sharing with the help of single photons either by sending them back or fourth or via generating them through faint laser pulses. Some also utilized single photons but rather then transmitting them in pure form, they preferred mixed state. Single photons were preferred over initially used GHZ states as per proposed by Hillary in 1999 due to excess of qubits used along with the associated complexity. Some researchers also combined QKD with QSS as well. In case of using a photon in mixed state, non-orthogonal quantum states were used. Here in [2] the initial states to be used were either $\left(|0\rangle,|1\rangle\right)$ or (ψ_0,ψ_1), where

$$\psi_0 = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{4.1}$$

$$\psi_1 = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{4.2}$$

2 modes were proposed, message mode and control mode. In message mode, Alice and Bob communicated the secret to be shared where as in control mode they performed eavesdrop check to detect Eve.

Two operators were used in this mode I and $i\sigma_y$, where $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ such that

$$I|0\rangle = |0\rangle \tag{4.3}$$

$$I|1\rangle = |1\rangle \tag{4.4}$$

$$I|\psi_0\rangle = |\psi_0\rangle \tag{4.5}$$

$$I|\psi_1\rangle = |\psi_1\rangle \tag{4.6}$$

Where as $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$

$$i\sigma_y|0\rangle = -|1\rangle \tag{4.7}$$

$$i\sigma_y|1\rangle = |0\rangle \tag{4.8}$$

$$i\sigma_y|\psi_0\rangle = |\psi_1\rangle \tag{4.9}$$

$$i\sigma_y|\psi_1\rangle = -|\psi_0\rangle \tag{4.10}$$

Moreover, to a random person who does not know the initial state of qubit used by Alice, the qubit will be in a mixed state, i.e.:

$$\rho_0 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|\psi_0\rangle\langle\psi_0| \tag{4.11}$$

Protocol Steps:

Alice prepares a qubit in $|0\rangle$ or $|\psi_0\rangle$ randomly and sends that qubit to Bob. Bob after receiving that qubit decides to choose either message mode or control mode randomly. If control mode is used, Bob replaces the qubit received from Alice with a qubit randomly prepared by him in one of a predefined basis $(|0\rangle,|1\rangle,|\psi_0\rangle,|\psi_1\rangle)$ and sends it to Alice.

Alice then measures this qubit and announces that she received the qubit sent from Bob. Only then Bob announces that he was using control mode to detect eavesdropper., so he tells Alice the initial state of the qubit that he sent to Alice. Now if Alice had used same basis and the results differ, this means that there is an eavesdropper and Eve gets detected and they stop communication, otherwise they start secret sharing.

In case of message mode, if Bob wants to transmit 0, he will perform I operator on the qubit sent by Alice, and if he wants to send 1, he performs $i\sigma_y$ operator on the qubit sent by Alice and sends it back to Alice. After receiving the qubit, Alice performs measurement and announces that she received the qubit sent by Bob. When all of the information has been transmitted by Bob and received by Alice, communicated is successfully terminated.

4.3.1.1 Bidirectional Quantum Secret Sharing and Secret Splitting with Polarized Single Photons

This protocol made use of photons travelling back and forth between the participating parties, and made use of 2 modes, message mode and eavesdropping check mode. Moreover, the protocol used very low amount of classical information over the public channel and that information was used to do eavesdropping check. This paper was an extension to [31], the photons to be used were generated via faint laser pulses. Another importation feature of this protocol is that, they combined quantum key distribution with secret splitting. According to BID-QKD protocol [26], Bob prepares photons in one of the following basis: $(|\pm z\rangle,|\pm x\rangle)$ and sends that single photon to Alice. Alice then performs some unitary operator on the qubit sent by Bob to encode the information to be transmitted and sends it back to Bob. After receiving it, Bob measures it and gets the result. This protocol worked with good efficiency up to 100% only if the number of photons to be used were 2. So if the photons exceed, the protocol efficiency reduces. Hence this paper provided some modifications in this protocol.

Protocol Steps:

Alice creates a key K_B with Bob and K_C with Charlie in a way that $K_A = K_B \oplus K_C$. Moreover, one of them (bob or Charlie) may be dishonest. Now, keys to encrypt secret by Bob and Charlie are denoted by K_B' and K_C'. Alice will determine that whether $K_A' = K_B' \oplus K_C'$ obtained by combining the keys used by Bob and Charlie is same as $K_A = K_B \oplus K_C$ or not. If the error rate

between K_A and K_A' is 0, it means that there is no dishonest party and she will then send her secret message after encrypting it with K_A.

Now in order to create K_A, Alice will prepare a 2 photon product state:

$$|\psi_A\rangle = |\psi_B\rangle \otimes |\psi_C\rangle \tag{4.12}$$

Where $|\psi_B\rangle$ and $|\psi_C\rangle$ will be prepared in either rectilinear or diagonal basis. i.e.:

$$|+z\rangle = |0\rangle \tag{4.13}$$

$$|-z\rangle = |1\rangle \tag{4.14}$$

$$|+x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{4.15}$$

$$|-x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \tag{4.16}$$

Alice then sends $|\psi_B\rangle$ to Bob and $|\psi_C\rangle$ to Charlie. Now if they select message mode, they will apply unitary operator $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $U = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ and send the photons back to Alice where she will measure them to get the results.

In this protocol, there are 2 eavesdropping checks. One check is performed before sending message in a way that Alice sends a large number of photons to Bob and Charlie, where they measure those photons randomly in σ_z and σ_x basis and then announce the measuring basis for Alice. Alice then analyzes the error rate to determine the eavesdropper before communicating. Second eavesdropping check is performed while creating private keys, where Alice checks the difference between the state sent by her and the one received from Bob and Charlie. as they used same measuring basis so no information regarding measuring basis will be announced, if after applying the unitary operator, Alice gets the same qubit sent by her, there is no eavesdropper and communication is secure.

The information sent by Alice to Bob and Charlie is in such a way that she sends a random bit string **G** (private key to be used for decryption) to one of them while the cipher text **L** is sent to the other party. When both of them perform $G \oplus L$, they will get the secret message. So now, both of them have to collaborate together in order to extract the secret message.

Issues:

Security of message is depended on the randomness of the private key, so Alice and Bob had to perform a lot of secure private key distribution before transmitting the secret to be shared and they

had to make sure to use a different key each time. This possess a lot of computational work here along with lots of communication prior to secret sharing. Moreover, there are no means to check that whether Bob and Charlie are 2 different entities or a single user is pretending to be both Bob and Charlie in order to extract the secret on his own. So the protocol is not secure as there is no proper authentication mechanism for Bob and Charlie.

4.3.1.2 Experimental Single Qubit Quantum Secret Sharing

This protocol was proposed for N parties in such a way that a single qubit will travel sequentially among all the parties for secret splitting.[27] The qubit is initially prepared in state:

$$|+x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \tag{4.17}$$

This qubit will be sent sequentially to all the parties and each party will apply a certain phase operator with a randomly chosen phase value where,

$$U_j(\varphi_j) = \begin{cases} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow e^{i\varphi_j}|1\rangle \end{cases}$$

Where $\varphi_j \in \left\{0, \pi, \frac{\pi}{2}, \frac{3\pi}{2}\right\}$

Now, each party will perform some unitary operator and finally the qubit (4.17) will be converted into:

$$|x_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\left(\sum_j^N \varphi_j\right)}|1\rangle\right) \tag{4.18}$$

The Nth party will perform measurement on the qubit received in $|\pm x\rangle$ basis whereas:

$$|\pm x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right) \tag{4.19}$$

The resulting result will be ± 1. The restriction imposed upon the Nth party is that he can only use $\varphi_N = 0$ or $\varphi_N = \frac{\pi}{2}$.

The probability of detecting $|\pm x\rangle$ is:

$$p_{\pm}(\varphi_1, ..., \varphi_N) = \frac{1}{2}\left[1 \pm \cos\left(\sum_j^N \varphi_j\right)\right] \tag{4.20}$$

Whereas the expected value of measurement is:

$$E' = (\varphi_1, ..., \varphi_N) = p_+(\varphi_1, ..., \varphi_N) - p_-(\varphi_1, ..., \varphi_N) = \cos\left(\sum_j^N \varphi_j\right) \tag{4.21}$$

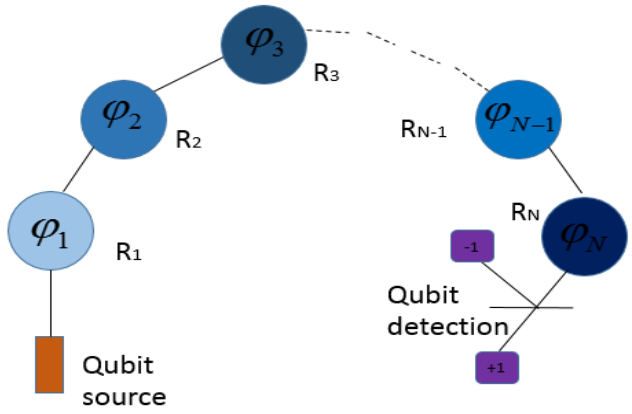

Fig 4.2 Demonstration of Experimental Single Qubit Secret Sharing Scheme[27]

Note that after distribution, prior to measurement all parties will announce some indirect information about the phase used. For this purpose, they have divided the phase information into two classes. Class X and class Y. class X means $\varphi_j \in \{0, \pi\}$, whereas class Y corresponds to $\varphi_j \in \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$.

So now all the parties randomly announce the class used by them and Nth party performs measurement that leads to a deterministic result i.e. ± 1. So now all parties have to collaborate together and provide the values of φ_j in order to extract the secret.

Issues:

The security of this protocol was justified through BB84 protocol regarding dishonest individuals and it does not tackle the latest emerging attacks. Moreover, what if the party immediately after the sender is dishonest one and it keeps intercepting all the qubits sent by the sender or acts as a middle man. Moreover, there is no way to ensure that whether the participating individuals are authentic or not.

4.3.2 Quantum Secret Sharing Protocols with Two Particles

There are two main schemes to do Quantum Secret Sharing:

- (n,n) threshold scheme
- (k,n) threshold scheme

In (n,n) scheme, it is necessary that all the parties that are involved in QSS must come together and share their part to generate the actual message. Whereas, in (k,n) at least k or more than k

individuals should come together so that they can extract the actual message. Whereas the bound on n is (n=2k-1)

Another important prospect of the protocols proposed initially was that all the parties involved in secret sharing must do their measurements together otherwise the entanglement will be destroyed and no one will be able to extract the secret.

Some protocols made use of entanglement swapping along with local unitary operators [10]-[12], [20]-[24],[32] while some proposed quantum secret sharing protocols without local unitary operators[29].

A 3-party QSS without local unitary operators involved 3 parties where Alice generates a string of EPR pairs and sends randomly some of the photons to Bob and leftover EPR photons are sent to Charlie.[29] The photons are sent in a random sequence, so Bob or Charlie don't know the order of entangled pairs. Also some of the photons sent to Bob and Charlie are not entangled with each other, instead they are entangled with the photons in direct possession of Alice.

Alice then asks Bob or Charlie to perform measurements on selective position photons along with the direction specified by Alice and send her the results. After that Alice performs same procedure for the other party and verifies their results, if the results are same it means that channel is safe. Then secret communication will be started.

Now if Alice wants to send 0, she will ask both of them to use the same direction for a pair that is entangled. Similarly, if Alice wants to send 1, she will ask them both to use different directions for measurements. So when Bob and Charlie collaborate, they will be able to know the secret by sharing their measurement results.

Moreover, it also utilized super dense coding to increase the efficiency by reducing the number of qubits involved in the procedure.

Some papers also claimed to be secure against eavesdropping by introducing two modes of the protocol:

- **Detecting mode:** the channel is first verified between sender and the parties involved to detect the eavesdropper
- **Message mode:** message is encoded on the qubits and distributed among the parties via bell states and entanglement

4.3.2.1 Quantum State Sharing Of An Arbitrary Two-Qubit State With Two-Photon Entanglements And Bell-State Measurements

In the proposed protocol, Alice will generate EPR {(1,2)}, Bob will generate {(3,4)} Charlie and Bob will share {(5,6)} together. Now for communication Bob will entangle itself by sending qubit 3 to Alice. Alice will send qubit 2 along with qubit to be sent to Charlie[33].

After that Alice will perform measurement on the qubits in her possession and announce the BSM. Bob and Charlie will interact to gain the secret via entanglement.

General Scenario:

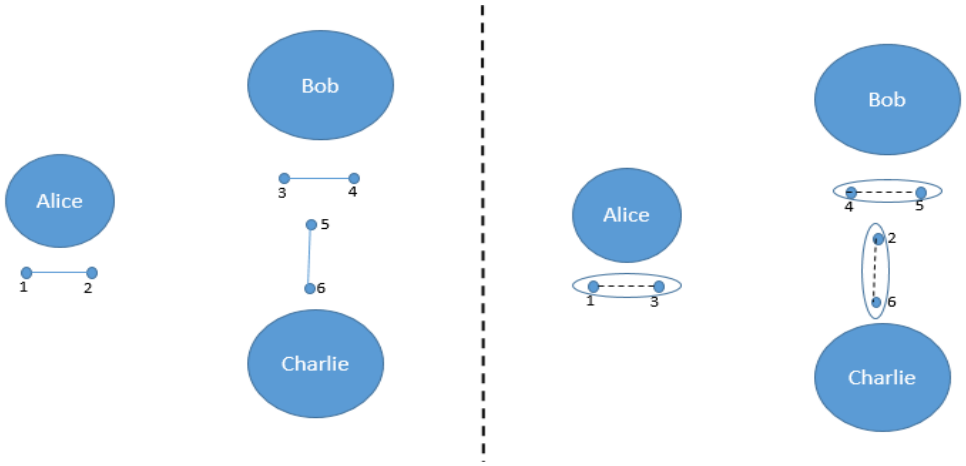

Fig 4.3 General Scenario for Quantum Secret Sharing in Proposed Protocol 4.3.2.1

Possible Attack Scenario:

In this case an attacker Eve can do eavesdropping by intercepting qubit 3 sent from Bob to Alice and will send her own qubit. Similarly, she will capture qubit 2 and will send her qubit 8 to Charlie to get entangled with Alice.

Now she is entangled with Alice and is receiving all the information. Thus attacker can access the information now and thus the protocol is no more secure.

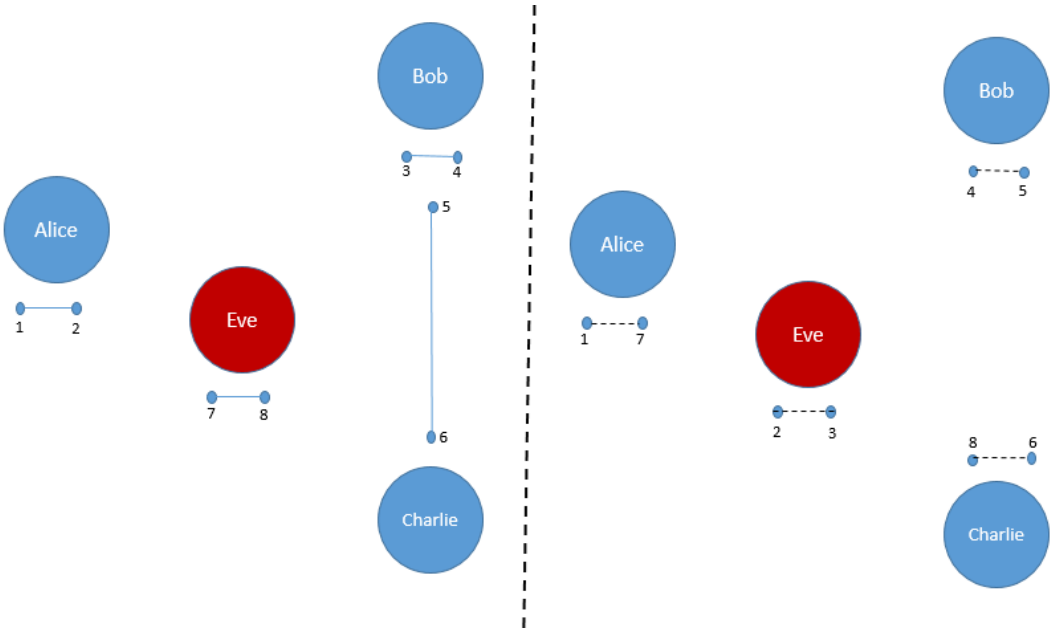

Fig 4.4 Attack Scenario on Proposed Protocol 4.3.2.1

4.3.2.2 A Quantum Secret Sharing Scheme With High Efficiency Based On Bell States

Let's suppose A desires to send a secret message (M bits) to 2 parties. She will generate N EPR pairs sufficient to transfer the message: $\{(b_1,c_1)(b_2,c_2)(b_3,c_3)\ldots(b_n,c_n)\}$[30]

She will then separate them in a way that she will create 2 qubit strings:

$$B=\{b_1,b_2,\ldots b_n\} \quad (4.22)$$

$$C=\{c_1,c_2,\ldots c_n\} \quad (4.23)$$

If N is multiple of 3, A will make 3 equal parts of these strings i.e: $B=B_1+B_2+B_3$ and same for $C=C_1+C_2+C_3$.

Now A will perform unitary operators on B dependent upon the message she desires to send. Table is shown below to choose the operators.

State / M'	$\lvert\Psi^+\rangle$	$\lvert\Psi^-\rangle$	$\lvert\Phi^+\rangle$	$\lvert\Phi^=\rangle$
00	U_0	U_1	U_2	U_3
01	U_1	U_0	U_3	U_2
10	U_2	U_3	U_0	U_1
11	U_3	U_2	U_1	U_0

Tab 4.1 Unitary Operators to be Applied Corresponding to the Measurement Results and Shared State[30]

Where $U_0=I$, $U_1=\sigma_x$, $U_2=\sigma_z$ and $U_3=i\sigma_y$

After that she will divide M (message) into 3 parts in a way that:

$$M_3'=M_2 \oplus M_3 \quad (4.24)$$

$$M_2'=M_1 \oplus M_2 \quad (4.25)$$

$$M_1'=M_3' \oplus M_1 \quad (4.26)$$

Where

$$M'=M_1'+M_2'+M_3' \quad (4.27)$$

Now after performing operation on B, A will send the qubits in a random sequence to B and C. i.e.:

$$B'=\alpha_4\alpha_5\alpha_6\alpha_1\alpha_2\alpha_3\alpha_9\alpha_8\alpha_7 \quad (4.28)$$

$$C'=\beta_3\beta_4\beta_1\beta_2\beta_7\beta_8\beta_5\beta_6\beta_9 \quad (4.29)$$

After that A will announce the respective positions of EPR pairs to B and C along with her M_1', M_2' and M_3' results.

Now by using following equations B and C will collaborate together to get the original message:

$$M_1=M_1' \oplus M_3' \quad (4.30)$$

$$M_2=M_1 \oplus M_2' \quad (4.31)$$

$$M_3=M_2 \oplus M_3' \quad (4.32)$$

Where $$M=M_1+M_2+M_3 \quad (4.33)$$

Issues:

It has been observed that there is no proper authentication mechanism to authenticate that whether the parties involved in secret sharing phase are legitimate or not? Similarly, we have seen that MiTM attacks can be initiated on discussed protocols.

4.3.3 Quantum Secret Sharing Protocols with Three Particles

Researchers provided many ways to perform quantum secret sharing with 3 particle GHZ states. Some researchers introduced protocols where GHZ states were shared among parties and entanglement had been performed among N parties.

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|00...0\rangle + |11...1\rangle\right)$$

This state had been shared among N parties where each party gets a single qubit share from this state. Later on all parties apply unitary phase operator and perform measurements on the local particle in their possession. Finally, all the parties announce the operator applied but do not announce the exact order. So all the parties perform a collaborative measurement to extract the secret. Similarly, some researchers [34] used both bell states and GHZ states in collaboration to perform secret sharing where initially GHZ states are securely distributed among Alice, Bob and Charlie. After that encoding of information from Alice and Bob is done where they encode their information on the bell states. Charlie then performs measurement on the qubit in his possession. At the end Alice and Bob announce their measurement results so that Charlie can extract the secret information.

Another way to perform QSS via GHZ state involved procedure where Alice creates GHZ states and divides them into 3 subsets S_1, S_2 and S_3. Alice then sends S_1 to Bob and keeps other by herself. Bob the performs unitary operators $\{I, \sigma_z, \sigma_x, i\sigma_y\}$ on those qubits and then inserts some random photons in that stream before sending it to Charlie.

After that Charlie along with Bob performs eavesdropping check on the random photons inserted by Bob. Meanwhile Alice encodes her secret information on S_2 by applying unitary operators $\{I, \sigma_z, \sigma_x, i\sigma_y\}$, and adds random photons to S_2 and S_3 and sends it to Charlie.

Alice then announces the position of random photons inserted to perform eavesdropping check with Charlie. After this check, Charlie performs measurements and collaborates with Bob to extract the secret encoded by Alice.

4.3.3.1 Quantum Secret Sharing Protocol via GHZ States

In 1999 Hillary et. Al came up with the idea of secret sharing in quantum cryptography to overcome the problem of passive attacks faced in classical cryptography[18]. As in case of quantum mechanics, quantum no-cloning theorem and quantum measurement rule can easily detect the eavesdropper so this issue can be resolved in quantum cryptography.

A 3 party Quantum Secret Sharing protocol proposed by Hillary was as follows:

GHZ entangled states will be used among three parties and all of them will be entangled together. Later on these entangled GHZ states will be divided into 2 equal parts in a way that by splitting them quantum information will split and later on by combining them quantum information will be extracted to get the secret.[18]

Initial GHZ state to be used will be:

$$\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{4.34}$$

Alice, Bob and Charlie will share each qubit and then they will publicly announce the basis they will use for measurements of their qubits. (Remember that measurement results will not be announced publicly.)

Now if Alice and Bob will interact together by combining their results they will be able to extract the information Charlie wanted to send to them. Table for measurements is shown below, here x axis shows Alice's and y axis shows Bob's measurements and by combining them the corresponding results are the measurements Charlie intended to send to them.

Alice					
Bob		**+x**	**-x**	**+y**	**-y**
	+x	$\|0\rangle+\|1\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle-i\|1\rangle$	$\|0\rangle+i\|1\rangle$
	-x	$\|0\rangle-\|1\rangle$	$\|0\rangle+\|1\rangle$	$\|0\rangle+i\|1\rangle$	$\|0\rangle-i\|1\rangle$
	+y	$\|0\rangle-i\|1\rangle$	$\|0\rangle+i\|1\rangle$	$\|0\rangle-\|1\rangle$	$\|0\rangle+\|1\rangle$
	-y	$\|0\rangle+i\|1\rangle$	$\|0\rangle-i\|1\rangle$	$\|0\rangle+\|1\rangle$	$\|0\rangle-\|1\rangle$

Tab 4.2 Measurement Results According to Alice and Bob to Determine Result at Charlie's Side

Information Splitting Procedure:

According to this protocol, Alice, Bob and Charlie will share an entangled GHZ state in following form as illustrated in eq. (4.34):

$$\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)$$

Now Alice will select a qubit he wants to send to Bob and Charlie. The qubit can be

$$\left(\alpha|0\rangle+\beta|1\rangle\right).$$

After that Alice will take tensor product of this state with her entangled GHZ qubit and will measure it. The results will be as follows[18]:

$$\frac{1}{2}\left(\begin{array}{l}\left|\Phi^{+}\right\rangle_{aa}\left(\alpha|00\rangle_{bc}+\beta|11\rangle_{bc}\right)+\left|\Psi^{+}\right\rangle_{aa}\left(\alpha|11\rangle_{bc}+\beta|00\rangle_{bc}\right)+\\ \left|\Psi^{-}\right\rangle_{aa}\left(\alpha|00\rangle_{bc}-\beta|11\rangle_{bc}\right)+\left|\Phi^{-}\right\rangle_{aa}\left(\alpha|11\rangle_{bc}-\beta|00\rangle_{bc}\right)\end{array}\right) \tag{4.35}$$

Where

$$\left|\Phi^{\pm}\right\rangle_{aa}=\frac{1}{\sqrt{2}}\left(|00\rangle_{aa}\pm|11\rangle_{aa}\right) \tag{4.36}$$

$$\left|\Psi^{\pm}\right\rangle_{aa}=\frac{1}{\sqrt{2}}\left(|01\rangle_{aa}\pm|10\rangle_{aa}\right) \tag{4.37}$$

Now Alice will not send her results to any one instead she will choose either Bob or Charlie to measure his qubit. Now to extract the information, Charlie will need 2 classical bits from Alice to know the magnitude of the qubit (α and β). In order to extract the information, Alice will need 1 bit from Bob.

The advantage of this protocol is that it can now protect from a passive eavesdropper because if he will try to capture a qubit or measures it, hewill be detected because state of qubit will be changed and errors will be introduced.

Issues:

The disadvantage associated with this protocol is that if a party having quantum computer and quantum processing power some-how succeeds in sharing the initial GHZ state, then Alice will be sharing her results and GHZ state with same attacker without knowing. Thus attacker can extract the information this way.

4.3.3.2 The GHZ State In Secret Sharing And Entanglement Simulation

This protocol makes use of entanglement and GHZ states to propose QSS-CR protocol.

Steps:

Suppose A wants to send a state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{4.38}$$

First A will generate a random string x where $x_i \in \{0,1\}$. Then A will choose a random bit from x, if x=0, she does nothing and if x=1, she performs operator N or her qubit[34]:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and gets

$$|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle \tag{4.39}$$

After that A creates (n-1) copies of the qubit obtained. Now A distributes x_i along with $|\psi'\rangle$ to the parties involved in QSS. Now because of quantum no cloning theorem, all the parties cannot have the result. So they will select one person on random to get the final qubit. For this purpose, suppose they choose P_1 to have the final qubit.

Now P_i applies H gate on his qubit and generates y_i where $y \in \{0,1\}$.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

After that P_i measures y_i and sends x_i and y_i to P_1. P_1 computes y, where $y= \oplus_{i-2}^{n} y_i$. if y=0, it does nothing and if y=1, P_1 applies Z gate:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Similarly it then computes x, where $x = \oplus_{i-2}^{n} x_i$. if x=0, it does nothing and if x=1, it applies N to reconstruct original qubit.

Issues:

It has been observed that using GHZ states, can increase the number of bits in a way that to share N bits, we have to use 7N bits. As GHZ states are combination of 2 bell states and it requires a noise free channel which is not possible ideally.

Moreover, it has been proved that to solve this issue one can use bell states as it reduces the overhead of qubits from 7N to N/(1-c) where c is the probability of choosing detection mode.

4.4 Extraction of Problem Statement

From the literature review, we have seen that in case of 1 photon particle user masquerading is possible and protocols need a lot of classical information sharing over the channel which can help eavesdroppers. Whereas in case of 2 photon state there is no proper authentication mechanism and MiTM attacks are possible. Similarly, in case of 3 particle state more number of bits and qubits are used and some attacks can also be initiated. So we need a system that must use lesser number of qubits that can be generated easily and has proper authentication mechanism as well. Moreover, lesser number of classical information must be sent over public channel and whatever is being sent over that channel should be of no use to attacker. Thus we will use 2 particle bell states to propose a secure and authenticated quantum secret sharing protocol with minimum classical information being sent over public channel.

Chapter 5

Proposed Model

5.1 Introduction

In this chapter non local correlations have been used to design a secure and authenticated quantum secret sharing protocol where classical secret has been sent in encrypted form along with the relevant decryption information with the help of quantum teleportation and entanglement swapping[35]. The scheme proposed in this thesis is a (n, n) threshold scheme which ensures that all the parties must collaborate for both encryption and decryption.
Some of the applications that make use of secret sharing are PGP recovery, visual cryptography, multiparty key agreement, hardware security modules and many others.
As per discussion in previous chapter, we have seen the importance and need for a secure and authenticated quantum secret sharing scheme, in this chapter, we will propose a secure and authenticated QSS scheme secure against internal and external eavesdropping to cater the issues described in chapter 4. Moreover, in our protocol there are some considerations including the fact that there is no pre-shared information between sender and receivers at any level in order to avoid both active and passive eavesdropping.

5.2 Problem Statement

In this particular case, the problem statement is to design a protocol to *"assure authentication and secrecy of secret from internal as well as external eavesdropping simultaneously for classical information.* $(|0\rangle,|1\rangle)$*"*

5.3 Desired Requirements

In this protocol the only requirement for security of secret information against eavesdropping is unsuppressed classical communication over public channels between distant users. The proposed procedure then remains secure against passive monitoring of classical information as well as active quantum attacks.
The proposed quantum secret sharing scheme is based on two-fold quantum non-local correlations that assure authentication and confidentiality of secret from internal and external eavesdropping simultaneously. The proposed quantum secret sharing scheme can be used as (2,2) threshold scheme for classical secret where both authenticity and secrecy is guaranteed [32]without relying on advanced quantum technology, pre-shared secret keys or private quantum/classical channels between distant users. Repetitive measurements and classical communication over public channels

assures availability of secret information and result in secure and authenticated quantum secret sharing scheme.

5.4 Proposed Methodology

The Quantum secret sharing proposed in this chapter is an extensive application of general setup of non-relativistic or relativistic quantum cryptography as per discussed in [32], [36], [37],[38]and their variants[39]–[44].

5.4.1 Generic Description

First of all, a generic description of proposed protocol is presented in figure 5.1. The fundamentals of quantum mechanics used in this protocol are entanglement swapping, bell state measurements, Pauli operators and quantum teleportation. Initially sender will perform authentication by generating authentication tokens and later on the results from authentication tokens will be used to split information between the receivers. Finally, sender will verify the authenticity of the receivers involved in quantum secret sharing, sender will give the final piece of information once receivers get validated.

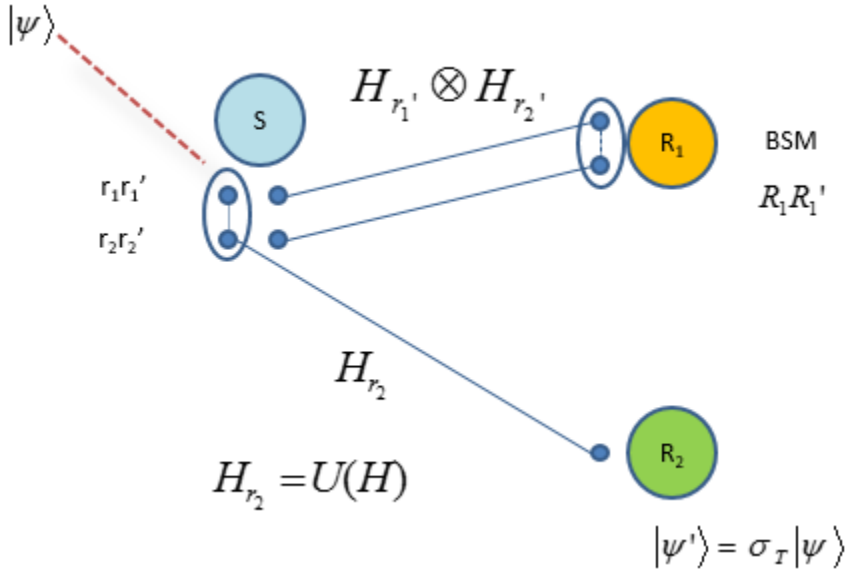

Fig 5.1 Generic Description of Proposed Protocol

5.4.2 Step Wise Protocol Description

Considerations:

- Quantum channel can be actively intercepted.
- Classical channels can be monitored passively.

Authentication Tokens

Initially sender will create four EPR pairs in bell states as shown in figure 5.2(a) to generate authentication tokens which will be used to split information and validate the receivers involved in quantum secret sharing.

Where:

$$\left|\Phi^{+}\right\rangle \rightarrow \frac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}} \tag{5.1}$$

$$\left|\Phi^{-}\right\rangle \rightarrow \frac{\left|00\right\rangle - \left|11\right\rangle}{\sqrt{2}} \tag{5.2}$$

$$\left|\Psi^{+}\right\rangle \rightarrow \frac{\left|10\right\rangle + \left|01\right\rangle}{\sqrt{2}} \tag{5.3}$$

$$\left|\Psi^{-}\right\rangle \rightarrow \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} \tag{5.4}$$

After that the sender will share 2nd half of his first 2 EPR pairs with R_1 and 2nd half of next 2 EPR pairs with R_2 to perform authentication as shown in figure 5.2(b)

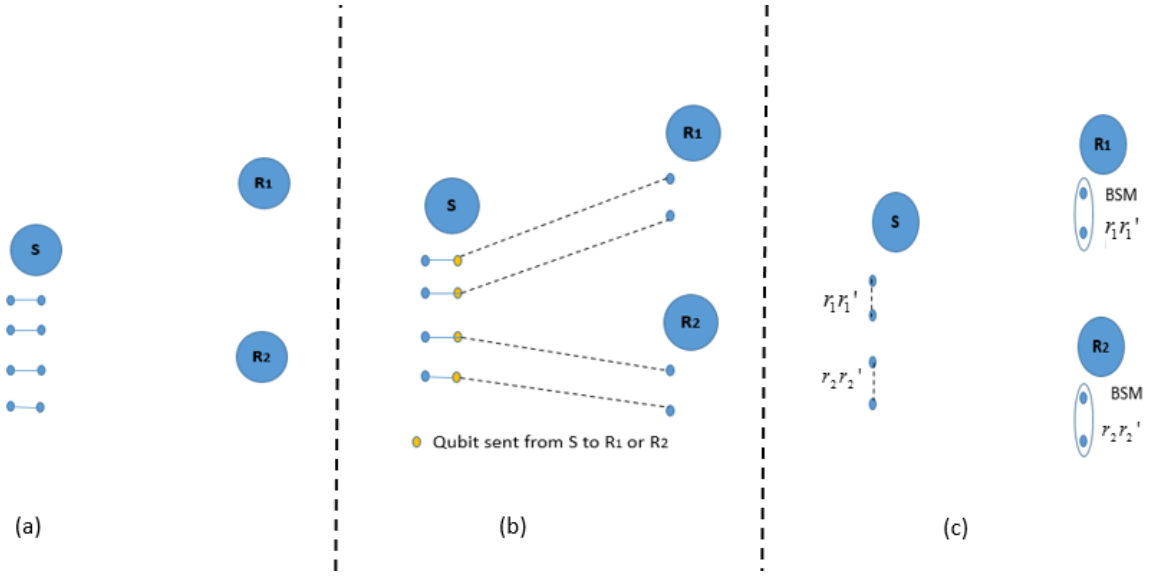

Fig 5.2: Generation of Authentication token between sender and receivers

After receiving the qubits, R_1 and R_2 will perform Bell State Measurements on qubits in their possession. This will result in a 2-bit classical information for both R_1 and R_2, i.e: r_1r_1' and r_2r_2' respectively. Now as sender has originally sent those qubits, he knows the initial state of the EPR pairs as well, he will automatically get the values of r_1r_1' and r_2r_2' as shown in figure 5.2 (c)

Information Splitting between R_1 and R_2

Now sender will create 2 EPR pairs on the basis of the classical results obtained while generating the authentication token, that is r_1r_1' and r_2r_2' as shown below in figure 5.3(a). Sender will then

send 2nd half of each pair, that is H_{r_1}' and H_{r_2}' to R_1 and will send 1st half of 2nd EPR pair H_{r_2} to R_2. The only qubit left at sender side will be H_{r_1} as shown in figure 5.3(b) below. After that R_1 will perform bell state measurements on qubits in his possession and will get a 2-bit classical result R_1R_1'. As a result of this BSM by R_1, sender and R_2 will get entangled because of the entanglement swapping performed by R_1. This scenario is shown in figure 5.3(c).

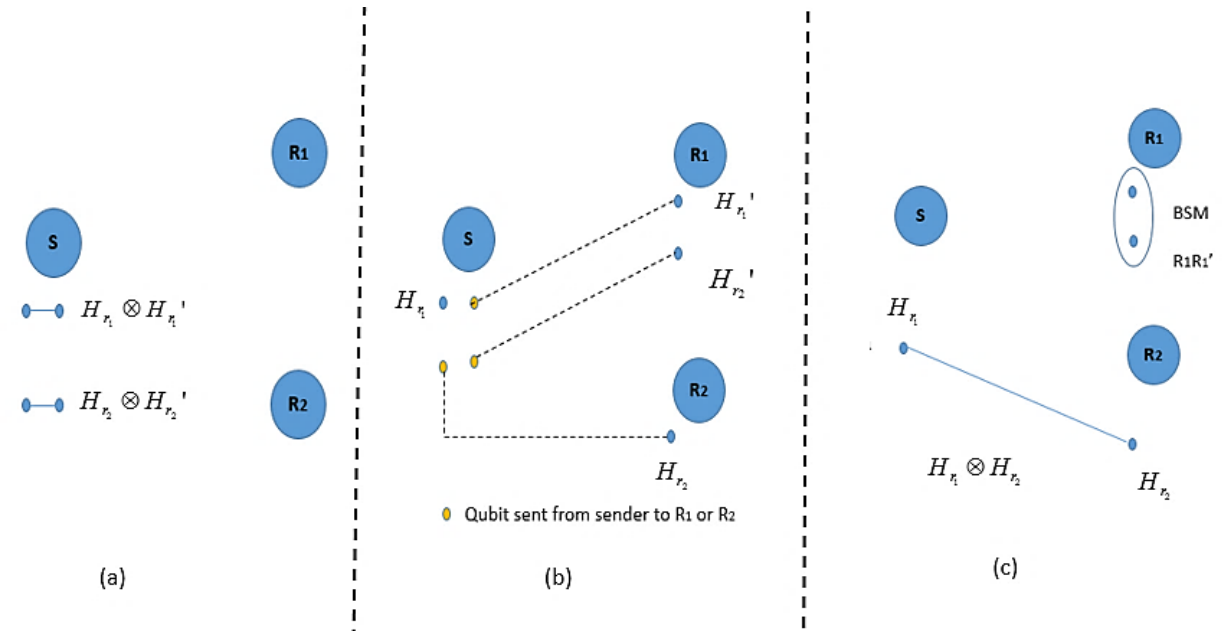

Fig.5.3 Qubit Sharing for Secret Information Splitting Between Sender, R_1 and R_2

After entanglement swapping, sender will send the secret message $|\psi\rangle$ to R_2 by performing teleportation. Here sender will generate the secret qubit $|\psi\rangle$ and will perform quantum teleportation on the qubit as shown in figure 5.4(a). In order to perform quantum teleportation successfully, sender will perform BSM on the secret to be shared along with the qubit shared between sender and R_2. As a result of this R_2 will get his qubit transformed into the desired secret. Sender will get ss' (2-bit classical result needed to decode the secret), R_2 will get his qubit transformed into $|\psi'\rangle = \sigma_T |\psi\rangle$ as shown in figure 5.4(b).Finally, all the information has been shared between sender, R_1 and R_2 in such a way that sender has ss', R_1 has R_1R_1' and R_2 has the secret qubit $|\psi'\rangle = \sigma_T |\psi\rangle$ as shown in figure 5.4(c)

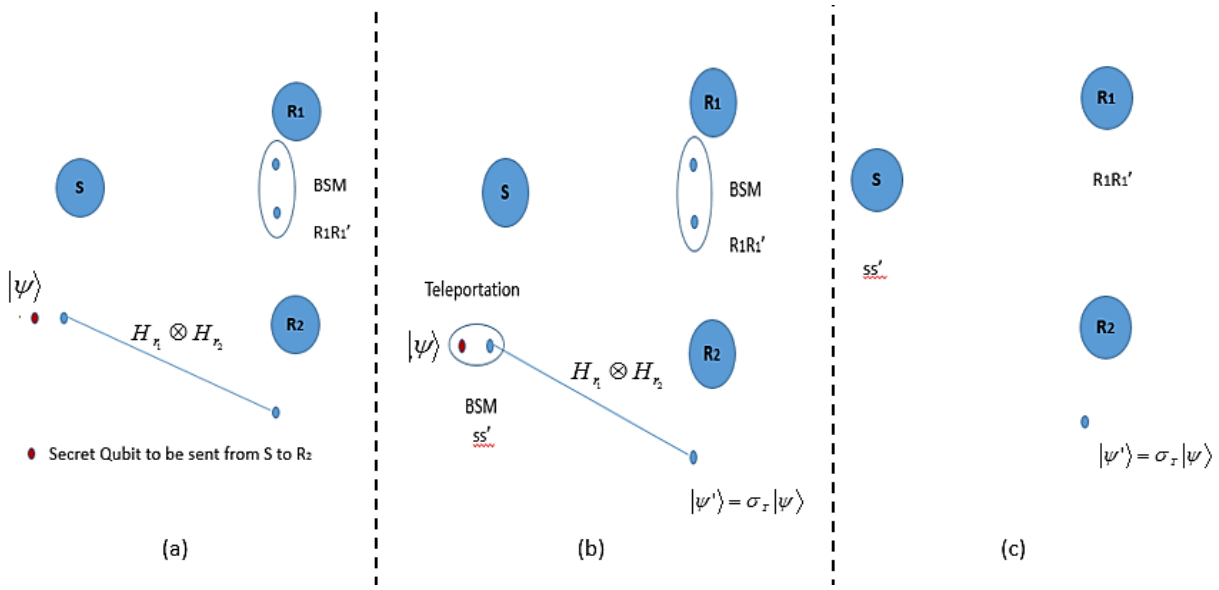

Fig 5.4 Shared Information between Sender, R_1 and R_2

Authentication

Before giving away the final piece of information (ss') to decode the secret, sender will first authenticate R_1 and R_2. To do this R_1 will send $(r_1 \oplus R_1)(r_{1'} \oplus R_{1'})$ to sender and R_2 will send $(\psi' \oplus r_2 \oplus r_{2'})$ to sender. As $R_1R_{1'}$ and r_1r_1' are known by the sender and they were the results of BSM performed by R_1 and were never shared on the channel. Sender will extract the results from the information sent by $R_1$by performing X-OR of received values with the values of R_1R_1' and r_1r_1' in his possession. If R_1 is a valid user, the information sent by R_1 will be the same as calculated by sender. Similarly, r_2r_2' are known only to sender and R_2, thus sender will verify the values of $r_2r_2'$and ψ ' sent by $R_2$by performing X-OR of received values with the values of r_2r_2' in his possession. If both results from R_1 and R_2 match with the results of sender, sender will share ss' with R_1 and R_2not otherwise.

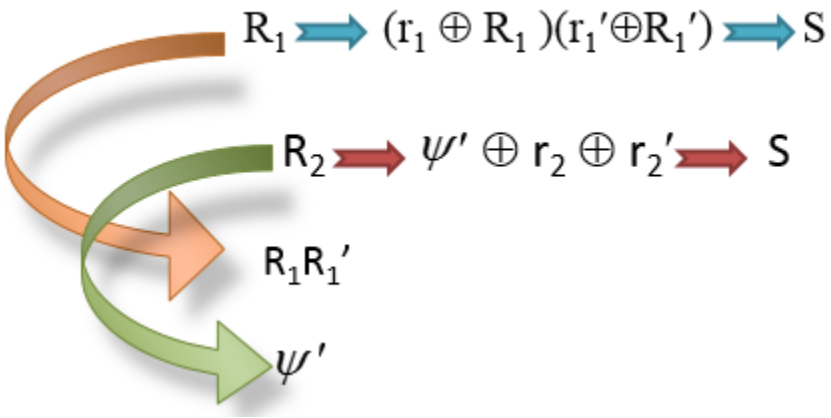

Fig 5.5 Authentication Information between R_1 and R_2

Combining Secret Shares

Receivers R_1 and R_2 can extract encoded message ψ from $\psi' = \sigma_T \left|\psi\right\rangle$ only if they meet and share their secrets: $r_1 r_1'$ and $R_1 R_1'$ kept by R_1 while ψ' and $r_2 r_2'$ kept by R_2.

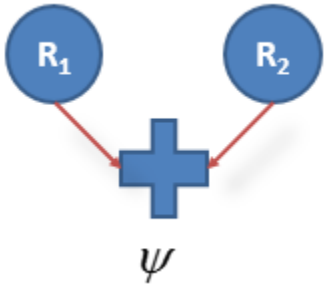

Fig 5.6 Combining Secret Shares Provided Sender Announces ss'

Chapter 6

Result and Discussion

In this chapter security analysis along with security requirements for quantum secret sharing protocol will be discussed. After that results will be discussed along with the final conclusions.

6.1 Security Analysis for Secure Quantum Secret Sharing

6.1.1 Threshold Scheme

"A threshold scheme must be designed and should satisfy in a way that (k,n) k or more than k parties together should be able to obtain the secret."

The secret sharing scheme used in our case is (n,n) threshold scheme where each communicating party possesses a certain valuable part of the secret and hence collaboration of all parties is necessary to extract the secret message [45].Hence this property has been fulfilled in our protocol.

6.1.2 Secrecy

"No party should be able to able to obtain the secret individually or with others against the protocol requirements."

This security requirement has been accomplished in our protocol as we have seen that each party has a share that is necessarily required in order to obtain the secret message in a way that even if any single party does not give its secret, [46]all other parties cannot get access to the secret message even if, they collaborate together.

6.1.3 Eavesdropping

"Though eavesdropper possesses infinite quantum processing power, he must not be able to eaves drop any information."

As we have described earlier in our protocol that if eavesdropper gets access to the classical information being sent over the public channel, [47] it is of no use to the eavesdropper as, if the eavesdropper wants to extract the secret message he needs the qubits/ EPR pair share which is not possible to be accessed because of the inherent nature of physics as per proved by the laws of physics including quantum no-cloning theorem and quantum measurement rule.

6.1.4 Computations

"Statistical analysis methods should not be able to override the defined protocol."

There are no known statistical attacks to extract the entangled EPR pair without getting detected. So there is no way to extract the secret information from proposed protocol even via infinite computational power.

6.1.5 Public Information

"Any information that is announced publically for the protocol should be of no use for the attacker and involved parties if they (involved parties) don't follow quantum secret sharing steps to gather secret information."

This property has been full filled in our security protocol as no classical information has been sent directly and whatever has been sent over the channel is of no use to the attacker.[48]

6.1.6 Entanglement Characteristics

"The party involved in generating entangled states to be used in protocol should either be the sender of message or if some other party is involved there must be proper mechanism so that it cannot be used for cheating."

Quantum Secret Sharing protocol proposed here makes use of the entangled EPR pairs purely generated by the sender himself. Hence this property for QSS has been fulfilled on all levels whenever required.

6.2 Protocol Specific Step by Step Security Analysis

6.2.1 Authentication Tokens

This step is secure as r_1r_1' and r_2r_2' (that are being used for secure communication) are kept secret by R_1, R_2 and sender, and have not been sent on the public channel so there is no chance that any attacker will get access to this secret authentication token.

Another important aspect is that the EPR pairs to be used are generated and shared by the legitimate sender and thus the eavesdropper cannot get access to them because if he tries to do so, he will be detected. Even if he somehow manages to get access to the pair, he has to measure it in order to know the information which will change the qubit to classical bit and thus according to no cloning theorem eavesdropper will not be able to regenerate the exact clone of EPR pair and thus it's not possible to render the communication by masquerading to be a legitimate sender or receiver.

6.2.2 Information Splitting between Receivers

This step proves to be inherently secure because r_1r_1' and r_2r_2' are used here to generate next set of EPR pairs over which the secret will be sent. As r_1r_1' and r_2r_2' were never sent over a public channel

so only legitimate sender and receivers know this information and without this information it is impossible to extract the original form of EPR pairs to be used.

Moreover, quantum teleportation has been performed where the sender is working in his own lab and encodes the secret information over the entangled EPR pair with R_2. So the secret will be encoded on the qubit in possession of sender and will be translated on the entangled EPR pair part of R_2, thus there is no way for an eavesdropper to extract the secret. If the eavesdropper needs to decode the secret, he will need the qubit in possession of R_2 along with the classical information ss' and R_1R_1'.

6.2.3 Authentication

Now as the information sent to S via R_1 is $(r_1 \oplus R_1)(r_1' \oplus R_1')$

Similarly, the information sent to S via R_2 will be $\psi' \oplus r_2 \oplus r_2'$

Sender will now perform additional authentication in order to ensure that whether the receivers are legitimate or not? This will be performed via extracting R_1R_1' and $|\psi'\rangle$ by performing X-OR operation on the classical information sent via R_1 and R_2. Now if the obtained values of R_1R_1' and $|\psi'\rangle$ match with the values in possession of sender, he will be sure about the legacy of the receivers participating in secret sharing. Finally, sender will announce ss' to both R_1 and R_2 so they will use this information along with R_1R_1' in possession of R_1 and $|\psi'\rangle$ in the possession of $R_2$to generate the original message $|\psi\rangle$ sent by the sender.

6.2.4 Combining Secret Shares

Finally, as discussed above, it is necessary to have r_1r_1', r_2r_2', R_1R_1' and $|\psi'\rangle$ to get access to the secret message. We know that r_1r_1' and R_1R_1' are in possession of R_1 whereas r_2r_2' and $|\psi'\rangle$ are in possession of R_2, and all these are the necessary elements to decode the secret, so as along as both R_1 and R_2 don't come together and provide their share from the secret, no party on its own will be able to extract the secret message and as per the assumptions in quantum secret sharing protocol at least one of the party is considered to be honest. So it is not possible to cheat the sender in order to obtain the secret message via cheating both the receivers.

6.3 Conclusion

In this thesis named as "***Non-Local Correlations and Quantum Cryptography*",** a secure and authenticated quantum secret sharing protocol has been proposed along with the relevant security analysis to show that the proposed protocol is secure against active and passive eavesdropping. Moreover, it has been checked that the proposed quantum secret sharing scheme protocol meets the following predefined required security conditions:

- A (n,n) or (k,n) Threshold scheme that could be verified
- Secrecy of the information to be communicated among the relevant parties
- Eavesdropping should not be possible even if someone eavesdrops, it should be of no use to him (eavesdropper or attacker)
- Attacker with infinite computational power must not be able to break the security of the proposed protocol
- Public information if available should not give any sort of secret related information to the attacker
- Entanglement characteristics must be obeyed

Here we have proposed a (n,n) quantum secret sharing protocol that desires the presence of all the n parties for both secret sharing during encryption and decryption. This security requirement has been fulfilled in our protocol. Secondly the information to be communicated among n parties is secure as the sender is generating the EPR pairs and sharing it with the parties that are part of the secret communication. An eavesdropper cannot know the initial states of EPR pairs used between sender and the receivers. Moreover, the classical information was never sent over the public channel during the generation of authentication token which was used later on for authentication verification. Again eavesdropper can have no information at all and thus secrecy of the information used during the secret sharing and secret reconstruction is secure. Thirdly if the eavesdropper gets access to the classical information sent over the channel, it is of no use to the eavesdropper unless he knows the initial states of the EPR pairs that were used during the secret sharing phase and hence whatever information gets eavesdropped by the eavesdropper is simply useless to him. Fourthly as shown in our protocol the secrecy of the quantum secret sharing protocol is not dependent on the complexity of the quantum computations instead it depends on the inherent laws of physics that are experimentally proved to be unconditionally secure, [49] hence the attacker even with infinite computational power cannot overrule our protocol, proving it to be unconditionally secure and authenticated. Fifthly as explained earlier that whatever public information has been sent over the channel (i.e. classical information) is of no use to the eavesdropper as this public information cannot give any information about the secret message, and the EPR pairs in their initial states are required along with this publicly sent information over the channel, so the user can extract the secret message in its original form. Hence our proposed method meets this particular security requirement. Finally, entanglement swapping and non-local correlations have been used and it has been ensured that the party involved in generating entangled states to be used in protocol should either be the sender of message or if some other party is involved there must be proper mechanism to avoid cheating. In our case the generator of the EPR pair is the sender himself and is not using any other third party to generate and communicate EPR pairs hence this security requirement has been fulfilled. So we can see that our protocol for quantum secret sharing among two parties is secure and authenticated to share classical secret and it fulfills all the predefined security requirements as well.

6.4 Future Work

Quantum cryptography is a relatively new field and there is a lot of room for improvements. A lot of work is still needed to be done and there are many questions that are still unanswered. The protocol defined here is complete in itself. However, there are some other ways that can be utilized to achieve quantum secret sharing provided the predefined security requirements met. One can make use of super dense coding where the classical information to be sent will also be encoded over the qubits formed in a shared EPR pair. Second important thing that is needed to be explored in field of quantum cryptography is "*Quantum Digital Signature*". Another important issue is user masquerading, i.e. if a user with infinite quantum computations power succeeds to capture a qubit before the legitimate party and starts participating in the authentication, the user will never be able to capture them. Hence these issues are needed to be addressed and can be treated as future work in field of quantum cryptography.

References

[1] C. J. W. Black, Paul E., D. Richard Kuhn, "Quantum computing and communication.," *Adv. Comput.*, vol. 56: 189-24, 2002.

[2] F. Hikmat and C. Khalil, "Combining Steganography And Cryptography: New Directions," *Int. J. New Comput. Archit. Their Appl.*, vol. Vol. 1, no. Issue No. 1, pp. 199–208, 2011.

[3] Boneh and Dan, "Twenty years of attacks on the RSA cryptosystem," *Not. AMS*, vol. 46.2, pp. 203–213, 1999.

[4] X. Tan, "Introduction to Quantum Cryptography," in *Theory and Practice of Cryptography and Network Security Protocols and Technologies*, 2013.

[5] Weigert and Stefan, "No-Cloning Theorem, Compendium of Quantum Physics.," *Springer Berlin Heidelb.*, pp. 404–405, 2009.

[6] Horodecki, Ryszard, and E. Al., "Quantum Entanglement," *Rev. Mod. Phys.*, vol. 81.2:865, 2009.

[7] A. Shamir and A. Shamir, "How To Share a Secret," *Commun. ACM*, vol. 22, no. 1, pp. 612–613, 1979.

[8] R. Cleve, D. Gottesman, and H.-K. Lo, "How to Share a Quantum Secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, 1999.

[9] Gisin, Nicolas, and E. Al., "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74.1:145, 2002.

[10] Noor Ul Ain, "A Novel Approach For Secure Multiparty Secret Sharing Scheme Via Quantum Cryptography," in *CCODE-17*, IEEE. 2017.

[11] Braginsky, V. B., V. B. Braginskiĭ, F. Y. Khalili, and K. S. Thorne, *Quantum measurement.* Cambridge University Press, 1995.

[12] Kreyszig and Erwin., *Introductory functional analysis with applications*. New York: wiley, 1989.

[13] Bennett, C. H., Brassard., and Gilles, "Quantum Cryptography: Public Key Distribution And Coin Tossing.," 1984.

[14] D. McMahon, *Quantum Computing Explained*. John Wiley & Sons, 2007.

[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information 10th Anniversary Edition*. .

[16] Busch, Paul, T. Heinonen, and P. Lahti, "Heisenberg's uncertainty principle," *Phys. Rep.*, pp. 155–176, 2007.

[17] Z. J. Zhang, Y. Li, and Z. X. Man, "Multiparty quantum secret sharing," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 71, no. 4, pp. 1–4, 2005.

[18] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 59, no. 3, pp. 1829–1834, 1999.

[19] G. P. Guo and G. C. Guo, "Quantum secret sharing without entanglement," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 310, no. 4, pp. 247–251, 2003.

[20] S. Lin and G. Guo, "Cryptanalysis the Security of Enhanced Multiparty Quantum Secret Sharing of Classical Messages by Using Entanglement Swapping," *Int. J. Theor. Phys.*, vol. 52, no. 9, pp. 3238–3243, 2013.

[21] X. Zhang, X. Tan, and C. Liang, "High Efficient Multi-party Quantum Secret Sharing Scheme," *2014 Ninth Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, pp. 245–250, 2014.

[22] X. B. Chen, X. X. Niu, X. J. Zhou, and Y. X. Yang, "Multi-party quantum secret sharing with the single-particle quantum state to encode the information," *Quantum Inf. Process.*, vol. 12, no. 1, pp. 365–380, 2013.

[23] J. Xu, H. Chen, W. Liu, and Z. Liu, "Selection of unitary operations in quantum secret sharing without entanglement," *Sci. China Inf. Sci.*, vol. 54, no. 9, pp. 1837–1842, 2011.

[24] L. Y. L. Yanyan and X. C. X. Chengqian, "Three-Party Quantum Secret Sharing Based on Secure Direct Communication," *2009 Int. Forum Inf. Technol. Appl.*, vol. 1, no. 1, pp. 0–4, 2009.

[25] Y.-H. Chou, C.-Y. Chen, R.-K. Fan, H.-C. Chao, and F.-J. Lin, "Enhanced multiparty quantum secret sharing of classical messages by using entanglement swapping," *IET Inf. Secur.*, vol. 6, no. 2, p. 84, 2012.

[26] F. G. Deng, H. Y. Zhou, and G. L. Long, "Bidirectional quantum secret sharing and secret splitting with polarized single photons," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 337, no. 4–6, pp. 329–334, 2005.

[27] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Phys. Rev. Lett.*, vol. 95, no. 23, pp. 1–4, 2005.

[28] J. Joo, J. Lee, J. Jang, and Y. Park, “Quantum Secure Communication via W States,” pp. 1–6, 2008.

[29] Y. Yang, G. Yin, and T. Deng, “Quantum secret sharing based on entanglement without local unitary Operations,” *Proc. - 2009 2nd Int. Work. Knowl. Discov. Data Mining, WKKD 2009*, pp. 619–621, 2009.

[30] L. Kai, L. Yuanyuan, H. Kehai, and H. Xiao-ying, “A Quantum Secret Sharing Scheme with High Efficiency Based on Bell States,” *2012 Fourth Int. Symp. Inf. Sci. Eng.*, no. 60803154, pp. 418–421, 2012.

[31] G. L. L. Fu-Guo Deng, Hong-Yu Zhou, “Bidirectional quantum secret sharing and secret splitting with polarized single photons,” 2005.

[32] M. Nadeem, C. Science, N. U. Ain, and C. Science, “Secure and authenticated quantum secret sharing,” pp. 1–7, 2016.

[33] Deng, F-G, and E. Al., “Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements,” *Eur. Phys. J. D-Atomic, Mol. Opt. Plasma Phys.*, vol. 39.3, pp. 459–464, 2006.

[34] A. Broadbent, P. R. Chouha, and A. Tapp, “The GHZ state in secret sharing and entanglement simulation,” *Proc. 3rd Int. Conf. Quantum, Nano Micro Technol. ICQNM 2009*, pp. 59–62, 2009.

[35] XingLan Zhang, “One-way quantum identity authentication based on public key,” *Chinese Sci. Bull.*, vol. 54, no. 12, 2009.

[36] X. Nadeem, Muhammad, Wang, “Quantum digital signature scheme with non-locally correlated signatures.,” 2015.

[37] M. Nadeem, “Secure positioning and non-local correlations,” *arXiv Prepr. arXiv1406.3013*, p. 6, 2014.

[38] M. Nadeem, “Position-based quantum cryptography over untrusted networks,” 2014.

[39] M. Nadeem, “Quantum non-locality, causality and mistrustful cryptography,” pp. 1–13.

[40] M. Nadeem, “Unconditionally secure commitment in position-based quantum cryptography.,” *Sci. Rep.*, vol. 4, p. 7, 2014.

[41] M. Nadeem, “Delayed choice relativistic quantum bit commitment with arbitrarily long commitment time,” pp. 1–11.

[42] M. Nadeem, “Standard quantum bit commitment – an indefinite commitment time,” pp. 1–8, 2016.

[43] M. Nadeem, “The causal structure of Minkowski space time - possibilities and impossibilities of secure positioning.,” 2015.

[44] M. Nadeem, “Quantum cryptography – an information theoretic security,” 2015.

[45] A. Mahmoud and Qassim., "Verifiable Secret Sharing Scheme Based On Integer Representation.," *J. Inf. Syst. Oper. Manag.*, vol. 1, 2013.

[46] Luu, N. T. V., and S. Shimamoto, "Advanced multiparty quantum secret sharing using entanglement swapping," *Inf. Commun. Technol.*, vol. 2, 2006.

[47] Beaudry and N. J., "Assumptions in quantum cryptography," *arXiv Prepr.*, vol. 1505.02792, 2015.

[48] Feng-Li, Yan, G. Ting, and L. You-Cheng, "Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations," *Chinese Phys. Lett.*, vol. 25.4, no. 1187, 2008.

[49] Y. Sun, F. G. Wen, YuanYan-Bing, and Z. Yuan, "Splitting a quantum secret without the assistance of entanglements," *Quantum Inf. Process.*, vol. 11, no. 6, pp. 1741–1750, 2012.