

Secret Sharing Schemes



Zahid Iqbal

Regn. No. NUST201463645MSNS78114F

A thesis submitted in partial fulfillment of the requirements for the
degree of **Master of Science**

in

Physics

Supervised by: Dr. Aeysha Khalique

Department of Physics

School of Natural Sciences
National University of Sciences and Technology
H-12, Islamabad, Pakistan
2018

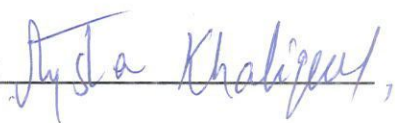
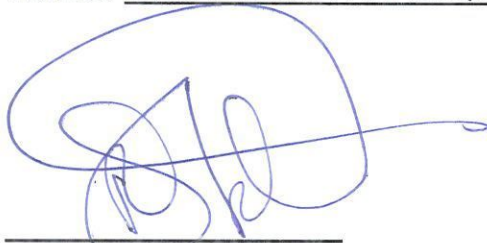
National University of Sciences & Technology**MASTER'S THESIS WORK**

We hereby recommend that the dissertation prepared under our supervision by: Zahid Iqbal, Regn No. NUST201463645MSNS78114F Titled: Secret Sharing Schemes be accepted in partial fulfillment of the requirements for the award of **MS** degree.

Examination Committee Members1. Name: DR. RIZWAN KHALIDSignature:  _____2. Name: DR. SHAHID IQBALSignature:  _____

3. Name: _____


Signature: _____


External Examiner: DR. TASAWAR ABBASSignature:  _____Supervisor's Name: DR. AEYSHA KHALIQUESignature:  __________
Head of Department15/08/18_____
Date**COUNTERSIGNED**Date: 15/08/18


Dean/Principal

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS thesis written by **Mr. Zahid Iqbal**, (Registration No. **NUST201463645MSNS78114F**), of **School of Natural Sciences** has been vetted by undersigned, found complete in all respects as per NUST statutes/regulations, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS/M.Phil degree. It is further certified that necessary amendments as pointed out by GEC members and external examiner of the scholar have also been incorporated in the said thesis.

Signature: 
Name of Supervisor: Dr. Aeysha Khalique
Date: 15/08/18

Signature (HoD): 
Date: 15/08/18

Signature (Dean/Principal): 
Date: 15/08/18

*Dedicated to my parents and brothers who
valued my education above all else*

Acknowledgements

In the name of Allah (S.W.T), the Most Merciful and the Most Gracious, I am thankful for His mercy upon me and for the knowledge He gave me to complete this dissertation. I am thankful to the most respectable personality and for whom the Creator has created this Universe, our Holy Prophet Muhammad (S.A.W).

I am grateful to Dr. Aeysha Khaliq for being my supervisor. She has always been so kind and helpful throughout my research. Without her guidance this research would not have been completed. I would like to thank my GEC members - Dr. Rizwan Khalid and Dr. Shahid Iqbal, who were always available in any need. I am really thankful for their help in my research.

I am indebted to my parents for their constant support and love. I also thank my siblings especially my brother, Dr. Shahid Iqbal and Razaqat Ali who had always been there for me as an inspiration. There are some other people I want to pay regards too, they are not related to blood but they share a special bond of brotherhood now. I want to mention the names of some of them - Aman Ullah, Muhammad Usman, Mureed Hussain, Mudassar Sabir and Saqib Hussain. Their guidance was very beneficial throughout my write-up. The office staff of NUST School of Natural Sciences was very kind and has provided whatever I have asked for, and not just the administration of our School but also our librarian Tahir Zareef Kiyani - one of the finest personalities I met at NUST.

I want to thank each and everyone I met at NUST and the people who made my stay memorable. I would like to pray for myself to be a proper guider and educationist in upcoming years. I wish to utilize this knowledge for the betterment of mankind and myself as well.

Zahid Iqbal

Abstract

Secret sharing is a method to split a message into several parts in such a way that no subset of parts is able to read the message, but the entire set is. In this thesis we explore the secret sharing schemes by the entanglement as well as without the entanglement with the discrete and continuous variables. Secret sharing has the vast importance in different areas of the recent technology due to its large security. In the first scheme, we review the secret sharing by the entanglement of discrete variable and use the Greenberger-Horne-Zeilinger (GHZ) states as a discrete variables. In this method we see that how this secret sharing is implemented and how the presence of the eavesdropper will introduce errors.

In the second , we review a particular symmetric variety of secret sharing, known as (k, n) threshold scheme. It involves a dealer who wants to distribute a secret among a group of n parties and any k number of players from n parties are sufficient to reconstruct the secret and any set of $k - 1$ or fewer parties has nothing about the secret and also it is noticed that threshold scheme exists for all value of k and n with $n \geq k$.

It is difficult to deal with multi-party entanglement, because the entangled states are difficult to prepare and maintained among growing the number of participants. So we explore sequential scheme for secret sharing, in which qubits are controlled by the parties without using any shared entanglement and it involves random hopping of the states by using the qdits (d -level states). This sequential method is required for any value of d . We also extend this idea into continuous basis by means of $d \rightarrow \infty$ and explore some tools needed for continuous variable secret scheme.

List of abbreviations

QI	Quantum Information
EPR	Einstein-Podolsky-Rosen
GHZ	Greenberger-Horne-Zeilinger
CV	Continuous Variables
MUBS	Mutually Unbiased Basis
BCH	Baker-Campbell-Hausdorff

List of Figures

4.1	The application of operators \hat{U} and \hat{V} by the players generating the random hopping of states in lattice.	40
4.2	The operator X and Z act as shift operators on $ \phi\rangle$ and $ \psi\rangle$ basis respectively. Operator F transform $ \phi\rangle$ into $ \psi\rangle$ and vice versa.	45
4.3	Random hopping in the lattice of state and the lattice points are unit distance from each other.	46
4.4	A random hopping by the four times application of Fourier operator.	48
4.5	Two different paths corresponding to two different random hopping of 6 players (R_0 to R_5) . In (a) only players R_3 and R_5 apply operator F while in (b)only R_1 and R_4	49
5.1	Schematic diagram of beam splitter.	58

Contents

List of Abbreviations	vi
List of Figures	vii
Contents	1
1 Introduction	4
1.1 Quantum bit	4
1.2 Entanglement	5
1.3 Bell states	6
1.3.1 Is the quantum state entangled?	6
1.4 Greenberger-Horne-Zeilinger (GHZ) state	8
1.5 Secret sharing	9
1.5.1 Secret sharing using quantum mechanics	9
1.6 Outline of Thesis	10
2 Continuous Variable	12

2.1	Continuous variables	12
2.1.1	The quadratures of electromagnetic (em) field	13
2.1.2	Squeezing of the field quadratures	16
2.2	Transformation of variables in linear optics	21
2.3	Transformation of variables in non-linear optics	22
3	Secret Sharing by using Entanglement	28
3.1	Secret sharing by discrete variables	28
3.1.1	Introduction	28
3.1.2	Working of scheme	29
3.1.3	Security against eavesdropper	32
3.2	Secret sharing by the entanglement of continuous variables	34
3.2.1	Introduction	34
3.2.2	Running the scheme	34
4	Secret Sharing without Entanglement	39
4.1	Secret sharing by a single qudit state for a prime d	39
4.1.1	Introduction	40
4.1.2	Running the scheme	41
4.2	Secret sharing by using a d -level state for any dimensions	43
4.2.1	Working of the scheme	46
4.2.2	Keys formation of the protocol	48
5	Tools for Random Hopping of Continuous Variables	51

5.1	Random hopping in continuous basis	51
5.2	Displacing the squeezed state	54
5.3	How a quantum state is displaced	58
6	Summary and Conclusion	65
	Bibliography	67
A	Wigner Function for Single Particle	69
	Appendix B–Properties of Fourier operator	70
B	Square of Fourier Operator	71

Introduction

1.1 Quantum bit

The quantum bit or qubit is a basic unit of quantum information science. It is representation of a two state quantum mechanical system such as a polarization of a single photon, or spin of a single electron in a hydrogen atom, and can take one of the two possible values 0 or 1. Any quantum system in quantum information theory, having two states $|0\rangle$ and $|1\rangle$ (in Dirac notation) can serve as a qubit.

Let us suppose we have a quantum system with two states $|0\rangle$ and $|1\rangle$, then any of the qubit state $|\psi\rangle$ of this system can be written as the linear superposition of $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

where α and β are complex numbers and known as probability amplitudes. Whenever we measure the qubit state $|\psi\rangle$ in the standard basis, then α comes as the probability amplitude of the output $|0\rangle$ and β for $|1\rangle$. Since the absolute square of probability amplitude is probability so the α and β must fulfil the requirement

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.2}$$

It should be noted that in Eq. (1.1) the qubit state $|\psi\rangle$ is not somewhere between the $|0\rangle$ and $|1\rangle$, it is in the linear superposition of both states $|0\rangle$ and $|1\rangle$. When someone wants to measure $|\psi\rangle$, he will find that it is in state $|0\rangle$ with the probability of $|\alpha|^2$ and in $|1\rangle$ with $|\beta|^2$. In the coordinate representation, these states $|0\rangle$ and $|1\rangle$ are represented as

$$|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \quad (1.3)$$

By using Eq. (1.3), the qubit state $|\psi\rangle$ can be written as

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \quad (1.4)$$

Thus we can say that unlike the classical bit which can only be set equal to 1 or 0, the quantum bit in a vector space can be parameterized by α and β . In the next section, we are going for a brief review on the theory of entanglement.

1.2 Entanglement

Quantum entanglement is one of the mysterious central principles of quantum physics. Entanglement depends upon two quantum properties known as "non-locality" and "non-separability", which are impossible in "classical" physics. Information physics (and the information interpretation of quantum mechanics) can explain them both with no equations, in a way that should be understandable to the lay person [1].

The roots of entanglement go back to the year 1935 when Einstein and two colleagues, Podolsky and Rosen (generally known as EPR) published a paper to show that quantum theory is incomplete. "The properties of physical systems have definite values whether system is being observed or not" this was the core by EPR and other "realists". When a system is entangled, individual component systems or particles are considered as single entity. Measurement of any component of system is a measurement on the entire system. The wave function for the system then collapses and component systems or particles assume definite states. In short, quantum entanglement correlates the

multiple particles or systems in such a way that measurement of one particle's quantum state gives the information about the other particle's quantum state irrespective of the location of the particles in space. Even if entangled particles are separated by billions of miles, changing the state of one particle will induce a change in that of the other. Now we are going to describe Bell states.

1.3 Bell states

In quantum information science, the Bell states are represent the simplest example of entanglement. In two particle system we have four maximally entangled states known as Bell states. We can write them compactly as [2]

$$|\beta_{ab}\rangle = \frac{1}{\sqrt{2}} \left(|0b\rangle + (-1)^a |1\bar{b}\rangle \right), \quad (1.5)$$

where \bar{b} denotes "not" b , (if b is 1 \bar{b} is 0 and vice versa) and a and b (having values 0 or 1) known as phase bit and parity bit respectively. It means that we can represent any two particles quantum state in terms of basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Now we are going to see how an entangled state can be identified.

1.3.1 Is the quantum state entangled?

The quantum states other than the entangled ones are known as product or separable states. We can differentiate between them in such a way that, the quantum states which can be written as a product of individual systems is separable and the state which cannot be written in product form is referred as entangled one. If we write two states by using the tensor product, the resulting state is composite state. The state of a composite system defined in Hilbert spaces as $|\psi\rangle \in H_A \otimes H_B$ are not surely entangled, where H_A and H_B are two dimensional Hilbert spaces. Let we have two states $|\phi_1\rangle \in H_A$ and $|\phi_2\rangle \in H_B$ and their composite state is defined $|\chi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$. Let the

composite state χ has the form

$$|\chi\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}, \quad (1.6)$$

then, state $|\chi\rangle$ is said to be entangled if and only if $ad \neq bc$, otherwise, it is separable state. Let us consider the Bell state $|\beta_{01}\rangle$ and check the above condition to show that Bell state is an entangled state.

$$\begin{aligned} |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle], \\ |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}[|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle], \end{aligned} \quad (1.7)$$

using the coordinate representation of $|0\rangle$ and $|1\rangle$, we have

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right],$$

after performing the tensor product, we have

$$\begin{aligned}
 |\beta_{01}\rangle &= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right], \\
 |\beta_{01}\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \tag{1.8}
 \end{aligned}$$

clearly $0 \neq 1$, this is what we have to prove. By using this procedure, we can check out whether the given state in 2×2 Hilbert space is entangled or not. Now we are going to describe our desired quantum states by using the quantum bit idea and then use them for further purposes.

1.4 Greenberger-Horne-Zeilinger (GHZ) state

In quantum information theory, a GHZ state is an entangled quantum state which involves at least three particles (subsystems). When each of the subsystems being two-dimensional (that is for qubits), it can be expressed as

$$|\text{GHZ}\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}},$$

with $N > 2$. The GHZ state can also be defined as the state representing the quantum superposition of all subsystems being in state $|0\rangle$ with all of them being in state $|1\rangle$. The most simplest form of GHZ state (for $N = 3$) is written as

$$|\text{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$

GHZ states have very interesting use in the field of secret sharing. We will use these states as a basic tool of a secret sharing scheme in Chapter 3. Now in the rest of this Chapter, we will discuss about secret sharing.

1.5 Secret sharing

The process in which a plaintext (secret) is converted into ciphertext by encoding and decoding it and then back into plaintext is known as cryptography. Traditionally cryptography involves only two people or parties: the sender and the receiver usually known as Alice and Bob respectively. However there are some applications when a sender wants to send the secret to more than one receiver due to some security reason so that only when all receivers or any subset of its collaborators get together, the secret can be recovered. Protocol used for this type of cryptocommunication is known as secret sharing protocol. Secret sharing protocols are needed in the situations for example, when the sender can not trust the individual receiver but he/she has a belief in a number of receiving parties collectively.

There are many types of secret sharing schemes in which the dealer distributes a share of the secret to many players, after fulfilling the specific conditions, the players are able to reconstruct the secret from their shares. The dealer plays with each player by giving a share to each of them and he can choose by his own wish what number of players (threshold members required for decoding) are allowed to retrieve the secret. One of the most important schemes of secret sharing, which is referred to as (k, n) threshold protocol of secret sharing. This protocol has a dealer, who distributes the secret message into n parties by encoding it. This scrambled information is then retrieved by the collective collaboration of a set of k players, while the remaining members of recipients get no information about the secret.

1.5.1 Secret sharing using quantum mechanics

Secret sharing can be said as the multi-party generalization of the quantum cryptography in which a secret message is not only protected against the criminal parties (eavesdropper) but only retrieved by the collective collaborations of several people [3]. There are some examples of quantum

mechanics based secret sharing which we will be discussed in detail in the coming chapters:

- **Discrete variables secret sharing** The quantum bits are used as discrete variables in order to implement the secret sharing of discrete variables. The first quantum mechanics based secret sharing scheme by discrete variables is proposed by using the GHZ state [4] and this state being the resource of entanglement, splits the secret information among all the participants. In this protocol, first a key is established between all the parties in such a way that when all the participants work together they retrieve the secret, while any single member is unable to do so. This work is discussed in chapter 3.
- **Continuous variables secret sharing** In continuous variables secret sharing, the GHZ state is replaced by the N-mode maximally entangled state $\int dx|x_1, x_2, \dots, x_N\rangle$. Continuous variable secret sharing is suggested by Tyc and Sanders [5] in 2002. In this protocol, secret is shared locally and only a sufficiently large subgroups of arbitrary participants can have access to the secret information. They used the multimode entangled states and produced the secret with the beam splitter and the squeezed light. The details of this scheme is in chapter 3.
- **Secret sharing without entanglement:** In chapter 4, we review the schemes of secret sharing which alleviates the need of entanglement by considering a sequential method for secret sharing. The random hopping of the states by using the qdits (d-level states) with the application of local operators will be performed there.

1.6 Outline of Thesis

The thesis is organized as follows: In second chapter, we will learn the basic information about the continuous variables, like the quadrature of the field and why they are called as continuous variables. Section 2.1 includes the definition of continuous variables, the quadrature of the field operator and how they can be squeezed. In section 2.2, we will see how continuous variables are transformed linearly via linear optics. In section 2.3, Non-linear optics of continuous variables are discussed in detail and it compromises of how the operator evolves in non-linear fashion. In section 2.4, the entanglement of continuous variables are briefly explained.

In chapter 3, we discuss the secret sharing by using the entanglement. In section 3.1, the discrete (GHZ state as discrete variable) variable secret sharing are briefly discussed. Section 3.2 includes the (k, n) threshold secret sharing scheme in which secret is share by using the entanglement of

continuous variables. In chapter 4, we present the entanglement free secret sharing without using entanglement. Section 4.1 includes the secret sharing by means of the random hopping of states of odd d (dimensions) whereas section 4.2 consists of random hopping scheme also but in that case it is for general dimension d .

Chapter 5 includes the three sections: in section 5.1, random hopping of states in continuous basis by using the Fourier and translation operators are explained and in section 5.2, we discuss the random hopping of continuous basis by using the squeezing and displacement operators. In the last section, we present a general scheme that how any arbitrary quantum state can be displaced and how it can be implemented physically. We conclude in sixth chapter.

Continuous Variable

In this Chapter, we are going to review the literature of continuous variables in quantum optics environment. We will discuss about the quantized electromagnetic field quadratures and then squeezing of these quadratures. In the last, we will study linear and nonlinear optics of continuous variables and conclude with some important remarks.

2.1 Continuous variables

Those variables that can take infinite numbers of possible values are known as continuous variables. Alternatively, it can be defined as if a variable can take any value between its minimum value and its maximum value known as continuous. Variables other than continuous are discrete. When a transition is made from classical mechanics to quantum mechanics of a system, then the observable in the Hamiltonian of that system changes into non-hermitian operators. Then the modes of the electromagnetic field of the system correspond to quantum harmonic oscillators and the quadratures of that mode play the role of position and momentum of the oscillators.

2.1.1 The quadratures of electromagnetic (em) field

In case of quantum harmonic oscillators, the Hamiltonian in terms of ladder operators having single mode k can be written as

$$\hat{H}_k = \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right), \quad (2.1)$$

where

$$\hat{a}_k = \frac{1}{\sqrt{2\hbar\omega_k}} (\omega_k \hat{x}_k + i\hat{p}_k), \quad (2.2)$$

$$\hat{a}_k^\dagger = \frac{1}{\sqrt{2\hbar\omega_k}} (\omega_k \hat{x}_k - i\hat{p}_k). \quad (2.3)$$

Now the Hamiltonian in terms of position and momentum have the form

$$\hat{H}_k = \frac{1}{2} (\omega_k^2 \hat{x}_k^2 + \hat{p}_k^2). \quad (2.4)$$

From Eqs. (2.2) and (2.3) the position and momentum operator can be written as

$$\hat{x}_k = \sqrt{\frac{\hbar}{2\omega_k}} (\hat{a}_k + \hat{a}_k^\dagger), \quad (2.5)$$

$$\hat{p}_k = -i\sqrt{\frac{\hbar\omega_k}{2}} (\hat{a}_k - \hat{a}_k^\dagger), \quad (2.6)$$

and the commutation relation of these operators are

$$[\hat{x}_k, \hat{p}_k] = \frac{i}{2} \delta_{kk'}. \quad (2.7)$$

This is the expected result, because of the bosonic commutation relation of creation and annihilation operator such as: $[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}$ and $[\hat{a}_k, \hat{a}_{k'}] = 0 = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger]$. From Eq. (2.2), it can be seen that operators \hat{p}_k and \hat{x}_k up to normalization factors are the imaginary and real parts of creation operators respectively. So we can define the dimensionless pairs of non-commuting variables such

as

$$\hat{X}_k \equiv \sqrt{\frac{\omega_k}{2\hbar}} \hat{x}_k = \text{Re} \hat{a}_k, \quad (2.8)$$

$$\hat{P}_k \equiv \sqrt{\frac{1}{2\hbar\omega_k}} \hat{p}_k = \text{Im} \hat{a}_k, \quad (2.9)$$

and their commutation relation will be

$$[\hat{X}_{k'}, \hat{P}_k] = \frac{i}{2} \delta_{kk'}. \quad (2.10)$$

In other words, we can say that the dimensionless pair of conjugate operators \hat{X}_k and \hat{P}_k are defined if we take $\hbar = \frac{1}{2}$ and they represent the quadratures of the single mode k of the field. Classically these operators correspond to the real and imaginary parts of complex amplitude of the oscillators. So now onwards by using (\hat{X}_k, \hat{P}_k) or (\hat{x}_k, \hat{p}_k) , we will call these quadratures representing the position and momentum variables. Now the variance of any two non-commuting observable \hat{A} and \hat{B} , for any arbitrary state can be written as

$$\langle (\Delta \hat{A})^2 \rangle \equiv \langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2, \quad (2.11)$$

$$\langle (\Delta \hat{B})^2 \rangle \equiv \langle \hat{B}^2 \rangle - \langle \hat{B} \rangle^2, \quad (2.12)$$

and their Heisenberg uncertainty relation

$$\langle (\Delta \hat{A})^2 \rangle \langle (\Delta \hat{B})^2 \rangle \geq \frac{1}{4} |\langle [\hat{A}, \hat{B}] \rangle|^2. \quad (2.13)$$

When we set $\hbar = \frac{1}{2}$ and $\omega_k = 1$, Eqs. (2.5) and (2.6) may reduce to

$$\hat{x}_k = \frac{1}{2} (\hat{a}_k + \hat{a}_k^\dagger), \quad (2.14)$$

$$\hat{p}_k = \frac{1}{2i} (\hat{a}_k - \hat{a}_k^\dagger). \quad (2.15)$$

Now the Heisenberg uncertainty relation of these observable will be

$$\langle (\Delta \hat{x})^2 \rangle \langle (\Delta \hat{p})^2 \rangle \geq \frac{1}{4} |\langle [\hat{x}, \hat{p}] \rangle|^2 = \frac{1}{16}, \quad (2.16)$$

with $[\hat{x}_k, \hat{p}_k] = \frac{i}{2}$. So the variance of these quadratures is similar to coherent or vacuum state. Now further we want to see what is the sense of quadratures in the electric field for a single mode [6],

$$\hat{E}_{k'}(\mathbf{r}, t) = u_0[\hat{a}_{k'}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)} + \hat{a}_{k'}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)}]. \quad (2.17)$$

From Eqs. (2.14) and (2.15), we can write \hat{a}_k and \hat{a}_k^\dagger as

$$\hat{a}_{k'} = \hat{x}_{k'} + i\hat{p}_{k'}, \quad (2.18)$$

$$\hat{a}_{k'}^\dagger = \hat{x}_{k'} - i\hat{p}_{k'}. \quad (2.19)$$

Now insert Eqs. (2.18) and (2.19) in Eq. (2.17), we have

$$\begin{aligned} \hat{E}_{k'}(\mathbf{r}, t) &= u_0[(\hat{x}_{k'} + i\hat{p}_{k'})e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)} + (\hat{x}_{k'} - i\hat{p}_{k'})e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)}], \\ \hat{E}_{k'}(\mathbf{r}, t) &= u_0[\hat{x}_{k'}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)} + i\hat{p}_{k'}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)} + \hat{x}_{k'}e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)} - i\hat{p}_{k'}e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_{k'}t)}], \end{aligned}$$

with the value $e^{i\theta} = \cos\theta + i\sin\theta$, above equation reduces to

$$\begin{aligned} \hat{E}_{k'}(\mathbf{r}, t) &= u_0[\hat{x}_{k'}(\cos(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t) + i\sin(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t)) + i\hat{p}_{k'}(\cos(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t) + i\sin(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t)) \\ &\quad + \hat{x}_{k'}(\cos(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t) - i\sin(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t)) - i\hat{p}_{k'}(\cos(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t) - i\sin(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t))], \end{aligned}$$

after doing some mathematics, we have

$$\begin{aligned} \hat{E}_{k'}(\mathbf{r}, t) &= u_0[2\hat{x}_{k'}(\cos(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t) - 2\hat{p}_{k'}(\sin(\mathbf{k}\cdot\mathbf{r} - \omega_{k'}t))], \\ \hat{E}_{k'}(\mathbf{r}, t) &= 2u_0[\hat{x}_{k'}(\cos(\omega_{k'}t - \mathbf{k}\cdot\mathbf{r}) + \hat{p}_{k'}(\sin(\omega_{k'}t - \mathbf{k}\cdot\mathbf{r}))]. \quad (2.20) \end{aligned}$$

From Eq. (2.20), it is obvious that the position and momentum operators \hat{x}_k and \hat{p}_k are the in-phase and out-of-phase components of the electric field amplitude of the single mode k with respect to a classical reference wave $\propto \cos(\omega_k t - k\cdot r)$. Now we dropped the mode index k and going to study few important relations such as

$$\hat{x}|x'\rangle = x'|x'\rangle, \quad \hat{p}|p'\rangle = p'|p'\rangle. \quad (2.21)$$

These quadratures form orthogonal and complete basis such as

$$\langle x'|x''\rangle = \delta(x' - x'') \quad \text{and} \quad \langle p'|p''\rangle = \delta(p' - p''), \quad (2.22)$$

$$\int_{-\infty}^{\infty} |x'\rangle\langle x'|dx' = 1 \quad \text{and} \quad \int_{-\infty}^{\infty} |p'\rangle\langle p'|dp' = 1. \quad (2.23)$$

Also the eigenstates of these quadratures are transform into one another by a Fourier transform

$$|x'\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-i2x'p'} |p'\rangle dp', \quad (2.24)$$

$$|p'\rangle = \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{i2x'p'} |x'\rangle dx'. \quad (2.25)$$

The quadratures eigenstates are very useful in order to calculate the wave function $\psi(x) = \langle x|\psi\rangle$ etc., and continuous variables based communication methods such as infinitely squeezed vacuum state in position basis can be represented by a zero position eigenstates $|x' = 0\rangle = \frac{1}{\sqrt{\pi}} \int |p'\rangle dp'$.

2.1.2 Squeezing of the field quadratures

When the uncertainty principle of any two observable in a quantum state is in saturation form, then this state is called as squeezed state. Noise of the electric field in squeezed states of light falls below a certain level than the vacuum state. This means that, when the squeezed light is turned on, we see less noise than no light at all [7].

When two operator \hat{A} and \hat{B} satisfy the commutation relation $[\hat{M}, \hat{N}] = i\hat{R}$, then the variance of these operators can be written as [8]

$$\langle(\Delta\hat{M})^2\rangle\langle(\Delta\hat{N})^2\rangle \geq \frac{1}{4}|\langle\hat{R}\rangle|^2. \quad (2.26)$$

The state of the system is said to be squeezed if either

$$\langle(\Delta\hat{M})^2\rangle < \frac{1}{2}|\langle\hat{R}\rangle|,$$

or

$$\langle(\Delta\hat{N})^2\rangle < \frac{1}{2}|\langle\hat{R}\rangle|.$$

But both variances are not less than $\frac{1}{2}|\langle\hat{R}\rangle|$ simultaneously. When we consider the squeezing of field quadratures, we take $\hat{M} = \hat{x}_k$ and $\hat{N} = \hat{p}_k$, being the quadratures operators of Eqs. (2.14) and (2.15) respectively and satisfying $[\hat{x}_k, \hat{p}_k] = \frac{i}{2}$. So Eq. (2.26) may be written as

$$\langle(\Delta\hat{x}_k)^2\rangle\langle(\Delta\hat{p}_k)^2\rangle \geq \frac{1}{16}, \quad (2.27)$$

and the quadratures squeezing exist whenever

$$\langle(\Delta\hat{p}_k)^2\rangle < \frac{1}{4} \quad \text{or} \quad \langle(\Delta\hat{x}_k)^2\rangle < \frac{1}{4}. \quad (2.28)$$

Now we are going to see, how the squeezing of quadratures can be done mathematically. Let us consider the operator which can generate the squeezed state, when it acts on any state and this operator is known as squeezing operator defined as [7]

$$\hat{S}(\xi) = \exp\left[\frac{1}{2}(\xi^*a^2 - \xi a^{\dagger 2})\right], \quad (2.29)$$

or

$$\hat{S}^\dagger(\xi) = \exp\left[\frac{-1}{2}(\xi^*a^2 - \xi a^{\dagger 2})\right], \quad (2.30)$$

with $\xi = re^{i\theta}$ and where r is known as squeezing parameter having values $0 \leq r \leq \infty$ and θ is the phase angle having values $0 \leq \theta \leq 2\pi$. Also note that the squeezing operator is unitary that is $\hat{S}^\dagger(\xi) = \hat{S}(-\xi)$ and the formation of this operator reveals that it is a kind of two photon generalization of the displacement operator, which is used to define the usual coherent states of a single mode field. The operators a^2 and $a^{\dagger 2}$ tell that when operator $\hat{S}(\xi)$ is acting on the vacuum state, it would create or destroy two-photon state. Let us denote the squeezed state $|\psi_s\rangle$ which is generated by the action of squeezing operator $\hat{S}(\xi)$ on any arbitrary state $|\psi\rangle$ as

$$|\psi_s\rangle = \hat{S}(\xi)|\psi\rangle. \quad (2.31)$$

In order to find the squeezing of quadratures (X_1, X_2) , we have to find the variance of these oper-

ators in $|\psi_s\rangle$ basis. First consider the operator $\hat{X}_1 = \frac{1}{2}(a + a^\dagger)$

$$\begin{aligned}\langle\psi_s|\hat{X}_1|\psi_s\rangle &= \langle\psi|S^\dagger\left(\frac{1}{2}(a + a^\dagger)\right)\hat{S}|\psi\rangle, \\ \langle\psi_s|\hat{X}_1|\psi_s\rangle &= \langle\psi|S^\dagger a \hat{S}|\psi\rangle + \frac{1}{2}\langle\psi|\hat{S}^\dagger a^\dagger \hat{S}|\psi\rangle.\end{aligned}\quad (2.32)$$

If we take $\hat{A} = -\frac{1}{2}(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2})$ then Eqs. (2.29) and (2.30) can be written as

$$\hat{S}(\xi) = e^{-\hat{A}} \quad \text{and} \quad \hat{S}^\dagger(\xi) = e^{\hat{A}}. \quad (2.33)$$

So Eq. (2.32) reduces to

$$\langle\psi_s|\hat{X}_1|\psi_s\rangle = \frac{1}{2}\langle\psi|e^{+\hat{A}}\hat{a}e^{-\hat{A}}|\psi\rangle + \frac{1}{2}\langle\psi|e^{+\hat{A}}\hat{a}^\dagger e^{-\hat{A}}|\psi\rangle. \quad (2.34)$$

Now consider the term $e^{+\hat{A}}\hat{a}e^{-\hat{A}}$ from Eq. (2.34) and apply the Baker-Campbell-Hausdorff lemma [9], which is define as, $e^{\hat{Y}}\hat{B}e^{-\hat{Y}} = \hat{B} + [\hat{Y}, \hat{B}] + \frac{1}{2}[\hat{Y}, [\hat{Y}, \hat{B}]] + \dots$

$$e^{\hat{A}}\hat{a}e^{-\hat{A}} = \hat{a} + [\hat{A}, \hat{a}] + \frac{1}{2}[\hat{A}, [\hat{A}, \hat{a}]] + \dots \quad (2.35)$$

Now we have to calculate the first few terms of the series and arrange our results, let us first consider $[\hat{A}, \hat{a}] = \hat{A}\hat{a} - \hat{a}\hat{A}$, using the value of \hat{A} we have

$$[\hat{A}, \hat{a}] = \frac{-1}{2}(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2})\hat{a} + \frac{1}{2}\hat{a}(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2}),$$

after doing some mathematics, we have

$$[\hat{A}, \hat{a}] = \frac{1}{2}\xi(\hat{a}^{\dagger 2}\hat{a} - \hat{a}\hat{a}^{\dagger 2}) = \frac{1}{2}\xi[(\hat{a}^{\dagger 2}, \hat{a})] = \frac{-1}{2}\xi[\hat{a}, \hat{a}^\dagger \hat{a}^\dagger],$$

now using the the property of commutator [10], $[\hat{A}, \hat{B}\hat{C}] = [\hat{A}, \hat{B}]\hat{C} + \hat{C}[\hat{A}, \hat{B}]$, above equation reduces to

$$[\hat{A}, \hat{a}] = -\xi \hat{a}^\dagger. \quad (2.36)$$

Now consider the term $[\hat{A}, [\hat{A}, \hat{a}]]$ and following the same procedure as we used earlier, we have

$$[\hat{A}, [\hat{A}, \hat{a}]] = \xi \xi^* a. \quad (2.37)$$

Inserting Eqs. (2.36) and (2.37) into Eq. (2.35), we have

$$e^{\hat{A}} \hat{a} e^{-\hat{A}} = \hat{a} - \xi \hat{a}^\dagger + \frac{1}{2} \xi \xi^* \hat{a} + \dots,$$

take $\xi = r e^{i\theta}$ and $\xi^* = r e^{-i\theta}$, above equation reduces to

$$e^{\hat{A}} \hat{a} e^{-\hat{A}} = \hat{a} - r e^{i\theta} \hat{a}^\dagger + \frac{1}{2} r^2 \hat{a} + \dots,$$

re-arrange above equation, we have

$$e^{\hat{A}} \hat{a} e^{-\hat{A}} = \hat{a} \left(1 + \frac{r^2}{2!} + \dots\right) - e^{i\theta} \hat{a}^\dagger \left(r + \frac{r^3}{3!}\right). \quad (2.38)$$

As we know that in general

$$\sinh r = r + \frac{r^3}{3!} + \dots, \quad \text{and} \quad \cosh r = 1 + \frac{r^2}{2!} + \dots, \quad (2.39)$$

using Eq. (2.39), Eq. (2.38) reduces to

$$e^{\hat{A}} \hat{a} e^{-\hat{A}} = \hat{S}^\dagger \hat{a} \hat{S} = a \cosh r - \sinh r e^{i\theta} \hat{a}^\dagger. \quad (2.40)$$

Similarly, by following the same procedure, we can find

$$e^{\hat{A}} \hat{a}^\dagger e^{-\hat{A}} = \hat{S}^\dagger \hat{a}^\dagger \hat{S} = \hat{a}^\dagger \cosh r - \hat{a} e^{-i\theta} \sinh r. \quad (2.41)$$

Now insert Eqs. (2.40) and (2.41) in Eq. (2.34) we have,

$$\langle \psi_s | \hat{X}_1 | \psi_s \rangle = \frac{1}{2} \langle \psi | a \cosh r - \sinh r e^{i\theta} \hat{a}^\dagger | \psi \rangle + \frac{1}{2} \langle \psi | \hat{a}^\dagger \cosh r - \hat{a} e^{-i\theta} \sinh r | \psi \rangle. \quad (2.42)$$

Let us consider the special case where $|\psi\rangle$ is the vacuum state $|0\rangle$ and $|\psi_s\rangle$ is the squeezed vacuum state and denoted by $|\psi_{sv}\rangle$;

$$|\psi_{sv}\rangle = \hat{S}(\xi)|0\rangle, \quad (2.43)$$

so that Eq. (2.42) reduces in terms of the squeezed vacuum state.

$$\langle\psi_{sv}|\hat{X}_1|\psi_{sv}\rangle = \frac{1}{2}\langle 0|\hat{a}\cosh r - \sinh r e^{i\theta}\hat{a}^\dagger|0\rangle + \frac{1}{2}\langle 0|\hat{a}^\dagger\cosh r - \hat{a}e^{-i\theta}\sinh r|0\rangle, \quad (2.44)$$

after doing some mathematics, we have

$$\langle\psi_{sv}|\hat{X}_1|\psi_{sv}\rangle = 0. \quad (2.45)$$

We now calculate the expectation of \hat{X}_1^2

$$\langle\psi_s|\hat{X}_1^2|\psi_s\rangle = \langle\psi_s|\frac{1}{4}(a + a^\dagger)^2|\psi_s\rangle,$$

when we consider the squeezed vacuum state, we have

$$\langle\psi_{sv}|\hat{X}_1^2|\psi_{sv}\rangle = \frac{1}{4}[\cosh^2 r + \sinh^2 r - 2\cosh r \sinh r \cos \theta]. \quad (2.46)$$

The variance for \hat{X}_1 in squeezed vacuum state is written as

$$\langle\psi_{sv}|(\Delta\hat{X}_1)^2|\psi_{sv}\rangle = \langle\psi_{sv}|\hat{X}_1^2|\psi_{sv}\rangle - \langle\psi_{sv}|\hat{X}_1|\psi_{sv}\rangle^2, \quad (2.47)$$

using Eqs. (2.45) and (2.46), we have

$$\langle\psi_{sv}|(\Delta\hat{X}_1)^2|\psi_{sv}\rangle = \frac{1}{4}[\cosh^2 r + \sinh^2 r - 2\cosh r \sinh r \cos \theta]. \quad (2.48)$$

Similarly for quadrature \hat{X}_2 , variance will be;

$$\langle\psi_{sv}|(\Delta\hat{X}_2)^2|\psi_{sv}\rangle = \frac{1}{4}[\cosh^2 r + \sinh^2 r + 2\cosh r \sinh r \cos \theta]. \quad (2.49)$$

Let us now consider the case when $\theta = 0$, which reduces

$$\langle(\Delta\hat{X}_1)^2\rangle = \frac{1}{4}[\cosh r - \sinh r]^2 = \frac{1}{4}e^{-2r}, \quad (2.50)$$

$$\langle(\Delta\hat{X}_2)^2\rangle = \frac{1}{4}[\cosh r + \sinh r]^2 = \frac{1}{4}e^{+2r}, \quad (2.51)$$

From above equations, it can be seen that the squeezing exists in \hat{X}_1 quadrature. Similarly if we consider the case when $\theta = \pi$ then by using Eqs. (2.48) and (2.49), we will have

$$\langle(\Delta\hat{X}_1)^2\rangle_{sv} = \frac{1}{4}e^{2r}, \quad (2.52)$$

$$\langle(\Delta\hat{X}_2)^2\rangle_{sv} = \frac{1}{4}e^{-2r}. \quad (2.53)$$

Thus we conclude this section by saying that uncertainty in one of the quadrature increases with the decrease in other quadrature because of unitary evolution and the over all state remain minimum uncertain.

2.2 Transformation of variables in linear optics

Linear optics is the branch of physics that deals with linear systems such that mirrors and lenses etc. The passive optical devices (beam splitters and phase shifters) preserve the number of photons and transform linearly the modes of annihilation operator. Any particular quantum state can be generated and manipulated by using the linear optics tool-box. Input and output relation for beam splitter is written as

$$\begin{pmatrix} \hat{a}'_1 \\ \hat{a}'_2 \end{pmatrix} = \hat{T}(2) \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \quad (2.54)$$

where $\hat{T}(2)$ is the transformation operator and it must be unitary, $\hat{T}^{-1}(2) = \hat{T}^\dagger(2)$ in order to ensure that the commutation relations such as; $[\hat{a}'_i, \hat{a}'_j] = [(\hat{a}'_i)^\dagger, (\hat{a}'_j)^\dagger] = 0$ and $[\hat{a}'_i, (\hat{a}'_j)^\dagger] = \delta_{ij}$ are preserved. The unitary of \hat{T} shows that the total number of photons during the transformation remains constant for a (lossless) beam splitter. The same transformation for two modes can be

written as [11]

$$\hat{T}(2) = \begin{pmatrix} e^{(\phi+\delta)} \sin \theta & e^{i\delta} \cos \theta \\ e^{(\phi+\delta')} \cos \theta & e^{-i\delta'} \sin \theta \end{pmatrix}, \quad (2.55)$$

with the phase factors ϕ and δ . Thus any ideal phase-free beam splitter can be expressed by the following relations

$$\begin{pmatrix} \hat{a}'_1 \\ \hat{a}'_2 \end{pmatrix} = \begin{pmatrix} \sin \theta & \cos \theta \\ \cos \theta & -\sin \theta \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}, \quad (2.56)$$

where $\sin \theta$ represents the reflectivity and $\cos \theta$ shows the transmittance of beam splitter. In general, transformation relation for a phase free and phase shift beam splitter can be expressed as

$$\hat{T}(2) = \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{-i\delta'} \end{pmatrix} \begin{pmatrix} \sin \theta & \cos \theta \\ \cos \theta & -\sin \theta \end{pmatrix} \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix}, \quad (2.57)$$

that is we can decompose any $N \times N$ matrix into such beam splitter operations.

2.3 Transformation of variables in non-linear optics

In quantum communication protocol the important tool is entanglement and squeezed light is necessary ingredient for the generation of continues variable entanglement. The quantum fluctuations of em field are squeezed by using the transfer matrices of non-linear optics.

So far, we have discussed a process that is initiated from linear optics in last section, which is based on passive optical devices as expressed in Eq. (??). Now we are going to discuss such a process that deals linearly with the input and output expressions but it eliminates the needs of ladder operators. It is the most general linear transformation and combines the elements from linear and non-linear optics and it is known as linear unitary Bogoliubov transformation [12] and

mathematically written as

$$\hat{a}'_i = \sum_j D_{ij} \hat{a}_j + E_{ji} \hat{a}_j^\dagger + \gamma_j, \quad (2.58)$$

where D and E are the matrices satisfying $DE^T = (DE^T)^T$ and $DD^\dagger = EE^\dagger + 1$, because of the bosonic commutation relation for \hat{a}'_i . Eq. (2.58) describes the relation of input and output for multi-port interferometers, the multi-mode squeezers and any quadratic Hamiltonian in \hat{a}^\dagger and \hat{a} . In the rest of this section, we are going to develop a squeezing method involving a non-linear optical χ^2 interaction, which is described by a quadratic interaction Hamiltonian. As increase of quantum fluctuation in one observable with the decrease of fluctuation in the conjugate observable below some level is referred as squeezing and practically implementation of squeezing can be done by a method know as the degenerate parametric amplification. The output state of this method involves the signal and idler frequencies and they are both equal to half of the pump frequency, corresponding to a single mode squeezed state. The single mode squeezing effect can be calculated by an interaction Hamiltonian, which is quadratic in creation and annihilation operators

$$\hat{H}_{\text{int}} = i\hbar \frac{\kappa}{2} \left(\hat{a}^{\dagger 2} e^{i\theta} - \hat{a}^2 e^{-i\theta} \right). \quad (2.59)$$

This equation describes the amplification of signal mode \hat{a} is at half of the pump frequency in the interaction picture. Here we suppose the coherent pump mode to be classical and the real amplitude of coherent states ($|\alpha\rangle$) is resolved in κ and θ is considered as pump phase. The number κ as well contains the material's susceptibility such that $\kappa \propto |\alpha_{\text{pump}}|$. So the interaction Hamiltonian will be $H_{\text{int}} \propto \hat{a}^{\dagger 2} \hat{a}_{\text{pump}} - \hat{a}^2 \hat{a}_{\text{pump}}^\dagger$ and with the parametric approximation we suppose, $\hat{a}_{\text{pump}} \rightarrow \alpha_{\text{pump}} = |\alpha_{\text{pump}}| e^{i\theta}$.

Now we are going to calculate the Heisenberg equation of motion of creation and annihilation operator by assuming that the pump phase is zero that is $\theta = 0$. The equation of motion of \hat{a} is written as

$$\begin{aligned} \frac{d}{dt} \hat{a}(t) &= \frac{i}{\hbar} [\hat{a}(t), \hat{H}_{\text{int}}(t)], \\ &= \frac{\kappa}{2} [\hat{a}(t), (\hat{a}^{\dagger 2}(t) - \hat{a}^2(t))]. \end{aligned} \quad (2.60)$$

After doing some mathematics of commutator algebra, we have

$$\frac{d}{dt}\hat{a}(t) = \kappa\hat{a}^\dagger. \quad (2.61)$$

Now take the hermitian conjugate, we have

$$\frac{d}{dt}\hat{a}^\dagger(t) = \kappa^*\hat{a}. \quad (2.62)$$

Eqs. (2.61) and (2.62) represent the equations of motion of the creation and annihilation operators respectively. Now in order to find the solution of these equations, we first differentiate Eq. (2.61) with respect to "time" and then put Eq. (2.62) in it, with $\kappa\kappa^* = |\kappa|^2 = \kappa^2$ we have

$$\frac{d^2}{dt^2}\hat{a}(t) - \kappa^2\hat{a}(t) = 0.$$

The solution of this equation is written as

$$\begin{aligned} \hat{a}(t) &= c_1 \cos \kappa t + c_2 \sin \kappa t, \\ &= \hat{a}(0) \cos \kappa t + \hat{a}^\dagger(0) \sin \kappa t. \end{aligned} \quad (2.63)$$

This equation shows the evolution of annihilation operator at time $t = 0$ to t in the interaction picture. Now we are going to calculate the evolution of the field quadratures defined in Eqs. (2.14) and (2.15). We first re-write these equations in terms of time dependence such as

$$\hat{x}(t) = \frac{1}{2} \left(\hat{a}(t) + \hat{a}^\dagger(t) \right), \quad (2.64)$$

$$\hat{p}(t) = \frac{1}{2i} \left(\hat{a}(t) - \hat{a}^\dagger(t) \right). \quad (2.65)$$

The evolution equation of motion for $\hat{a}(t)$ in the interaction picture can be written as

$$\begin{aligned} \frac{d}{dt}\hat{x}(t) &= \frac{1}{i\hbar} [\hat{x}(t), \hat{H}_{int}(t)], \\ &= \frac{\kappa}{4} \left[\left(\hat{a}(t) + \hat{a}^\dagger(t) \right), \left(\hat{a}^{\dagger 2}(t) - \hat{a}^2(t) \right) \right], \\ &= \frac{\kappa}{2} \left(\hat{a}(t) + \hat{a}^\dagger(t) \right), \end{aligned}$$

using Eq. (2.64), above equation reduces to

$$\frac{d}{dt}\hat{x}(t) = \kappa\hat{x}(t). \quad (2.66)$$

This is the equation of motion of quadrature $\hat{x}(t)$ and its solution is

$$\hat{x}(t) = \hat{x}(0)e^{\kappa t}. \quad (2.67)$$

Similarly, for the quadrature \hat{p}

$$\hat{p}(t) = \hat{p}(0)e^{-\kappa t}. \quad (2.68)$$

Eqs. (2.67) and (2.68) are representing the evolutions of quadratures \hat{x} and \hat{p} respectively. Now we are going to calculate the variance of these operators. Consider the vacuum state $|0\rangle$ and first calculate the relations $\langle 0|\hat{x}^2(t)|0\rangle$ and $\langle 0|\hat{x}(t)|0\rangle$. We take $\hat{a}(0) \equiv \hat{a}$ and $\hat{a}^\dagger(0) \equiv \hat{a}^\dagger$ for our convenience, so that

$$\langle 0|\hat{x}^2(t)|0\rangle = e^{2\kappa t}\langle 0|\hat{x}^2(0)|0\rangle = \frac{e^{2\kappa t}}{4}\langle 0|(\hat{a} + \hat{a}^\dagger)^2|0\rangle,$$

using the relations $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$, $\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$ and the orthogonality of the fock bases, the above equation reduces to $\langle 0|\hat{x}^2(t)|0\rangle = \frac{e^{2\kappa t}}{4}$ and in the same way, we will have $\langle 0|\hat{x}(t)|0\rangle = e^\kappa\langle 0|\hat{x}(0)|0\rangle = 0$. Thus

$$\langle (\Delta\hat{x}(t))^2 \rangle_{\text{vac}} = \frac{e^{2\kappa t}}{4}. \quad (2.69)$$

Similar procedure can be used to calculate the variance of quadrature $\hat{p}(t)$ to get

$$\langle (\Delta\hat{p}(t))^2 \rangle_{\text{vac}} = \frac{e^{-2\kappa t}}{4}. \quad (2.70)$$

The uncertainty relation of these variances can be calculated as

$$\langle (\Delta\hat{x}(t))^2 \rangle_{\text{vac}} \langle (\Delta\hat{p}(t))^2 \rangle_{\text{vac}} \approx \frac{1}{16}. \quad (2.71)$$

Eqs. (2.69), (2.70) and (2.71) show that the total uncertainty of evolving states remain minimum. So we can write as

$$\hat{U}(t, t_0) = \exp\left[\frac{1}{i\hbar}\hat{H}(t - t_0)\right], \quad (2.72)$$

with the Hamiltonian from Eq. (2.59) and $t_0 = 0$. Now we are going to introduce the unitary squeezing operator $\hat{S}(\xi)$ by defining the $\xi = -re^{i\Theta}$ with a dimensionless effective interaction time $r = \kappa t$ (the squeezing parameter)

$$\hat{U}(t, 0) = \exp\left[\frac{\kappa t}{2}(\hat{a}^{\dagger 2}e^{i\Theta} - \hat{a}^2e^{-i\Theta})\right] \equiv \hat{S}(\xi) = \exp\left[\frac{\xi^*}{2}\hat{a}^2 - \frac{\xi}{2}\hat{a}^{\dagger 2}\right]. \quad (2.73)$$

Due to the unitary evolution, the squeezing operator satisfies $\hat{S}^\dagger(\xi) = \hat{S}^{-1}(\xi) = \hat{S}(-\xi)$ and result of application of this operator on any arbitrary initial modes $\hat{a}(0) \equiv \hat{a}$ and $\hat{a}^\dagger(0) \equiv \hat{a}^\dagger$ are described in Eqs. (2.40) and (2.41). The squeezing operator $\hat{S}(\xi)$ defines mathematically squeezing of the quadratures and physically their squeezing can be done by the optical parametric amplification. More general minimum uncertainty states are displaced squeezed vacuum states, denoted by $|\alpha, \xi\rangle$, which can be calculated by the combined application of squeezing operator $\hat{S}(\xi)$ and displacement operator $\hat{D}(\alpha)$ on the vacuum state such as

$$|\alpha, \xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)|0\rangle, \quad (2.74)$$

where the unitary displacement operator $\hat{D}(\alpha) = \exp(\alpha\hat{a} - \alpha^*\hat{a}^\dagger) = \exp(2ip_\alpha\hat{x} - 2ix_\alpha\hat{p})$ with $\alpha = x_\alpha + ip_\alpha$ and $\hat{a} = \hat{x} + i\hat{p}$. So displaced squeezed vacuum wave function in position basis is written as

$$\phi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}}e^{\frac{r}{2}} \exp[-e^{2r}(x - x_\alpha)^2 + 2ip_\alpha x - ix_\alpha p_\alpha], \quad (2.75)$$

and the corresponding Wigner function is

$$W'(x, p) = \frac{2}{\pi} \exp[-2e^{2r}(x - x_\alpha)^2 - 2e^{-2r}(p - p_\alpha)^2]. \quad (2.76)$$

When we apply the two-mode squeezing and displacement operators on a vacuum state, then we

can write the wave function in position basis

$$\phi(x_1, x_2) = \sqrt{\frac{2}{\pi}} \exp \left[-e^{-2r} \frac{(x_1 + x_2)^2}{2} - e^{2r} \frac{(x_1 - x_2)^2}{2} \right], \quad (2.77)$$

and the corresponding Wigner function is written as

$$W'(x_1, p_1, x_2, p_2) = \left(\frac{2}{\pi}\right)^2 \exp[-e^{-2r}((x_1 + x_2)^2 + (p_1 - p_2)^2) - e^{2r}[(x_1 - x_2)^2 + (p_1 + p_2)^2]] \quad (2.78)$$

where we set $\xi = (x_1, p_1, x_2, p_2)$. This Wigner function approaches $\delta(x_1 - x_2)\delta(p_1 + p_2)$ in the limit of infinite squeezing $r \rightarrow \infty$, corresponding to the original EPR state. The derivations of Eqs. (2.76) and (2.78) are in appendix-A . The Wigner function can be used to obtain the probability of momenta or position wave functions by taking the marginal distributions such as:

$$\int dp_1 dp_2 W(\xi) = |\psi(x_1, x_2)|^2, \quad (2.79)$$

$$\int dx_1 dx_2 W(\xi) = |\psi(p_1, p_2)|^2. \quad (2.80)$$

These equations show that once we calculate the Wigner representations of any given wave function, then we will be able to find its counter parts by taking the marginal of Wigner function. Now in the next Chapter, we are going to discuss the secret sharing schemes by using the entanglement, which involves both discrete variables and continuous variables.

Secret Sharing by using Entanglement

In chapter 1, we presented an introduction of quantum mechanic based secret sharing and here we discuss it in detail. This chapter includes two schemes of secret sharing. In first scheme, the secret sharing is done by using the entanglement of discrete variables and Greenberger-Horne-Zeilinger (GHZ) states is used as a discrete variables. Whereas in the second scheme, the secret sharing by the entanglement of continuous variables will be discussed.

3.1 Secret sharing by discrete variables

3.1.1 Introduction

In particular we are reviewing the scheme presented by M.Hillery et.al. [4] and consider the case in which Alice (who is the admin of this protocol) wants to send an information to her clients, Bob and Charlie. Alice knows that only one of her clients is not trustworthy but she does not know which one. She cannot simply send the message to both because, the dishonest one will try to misuse her information. So a problem arises here that what should she do to keep her message secret?

The answer to this problem lies in the following procedure. Firstly, she can split her message into two parts in such a way that each part does not contain a complete information about her

original message but by combining both parts, complete information can be obtained. Then she will send these parts to each client (Bob and Charlie) so that they can get Alice's message by working together. As Alice's original message is in the form of binary bit string, she takes a string of bits as key bits having the same length as of her message string and add this to encrypts her message. The addition is done bit-wise under modulo 2. Then she sends the encrypted message string to one party and her random chosen key bit string to the other party. The two parties only get Alice's message only when they add their strings bitwise and modulo 2.

3.1.2 Working of scheme

In this scheme, GHZ state is used as a discrete variables which is N-qubits entangled state with 50 : 50 superposition $|0\rangle$ and $|1\rangle$. We consider the case when it is tripartite entangled state and we suppose that all three parties (Alice, Bob and Charlie) has one particle from this triplet

$$\begin{aligned} |\psi\rangle_{abc} &= \frac{1}{\sqrt{2}} [|000\rangle + |111\rangle], \\ &= \frac{1}{\sqrt{2}} [|0\rangle_a |0\rangle_b |0\rangle_c + |1\rangle_a |1\rangle_b |1\rangle_c]. \end{aligned} \quad (3.1)$$

The above equation is written in the eigenstates of z-basis spin and we also define eigenstates of the other two x and y spins

$$|\pm x\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle) \quad \text{and} \quad |\pm y\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm i|1\rangle),$$

From the set of equations, it can be written as

$$|0\rangle = \frac{1}{\sqrt{2}} (|+x\rangle + |-x\rangle), \quad (3.2)$$

$$|1\rangle = \frac{1}{\sqrt{2}} (|+x\rangle - |-x\rangle). \quad (3.3)$$

Also

$$|0\rangle = \frac{1}{\sqrt{2}} (|+y\rangle + |-y\rangle), \quad (3.4)$$

$$|1\rangle = \frac{i}{\sqrt{2}} (|-y\rangle - |+y\rangle). \quad (3.5)$$

The procedure is as follows: Before Alice sends the message, each party chooses randomly the direction of its measurement, it could be x or y direction. After the measurement, they publicly declare the direction of measurement but not the result of their measurements. There is a 50% chance that both Bob and Charlie's measurements are in the same direction so that half the time, they can get the result of Alice's measurement. Similarly, Alice can generate a random key to contact with one of them.

In order to check how the Charlie's state linked with Alice and Bob states, we decompose the GHZ triplet in terms of x eigenstates,

$$|\psi\rangle_{abc} = \frac{1}{\sqrt{2}} [|0\rangle_a |0\rangle_b |0\rangle_c + |1\rangle_a |1\rangle_b |1\rangle_c], \quad (3.6)$$

using Eqs. (3.2) and (3.3), we have

$$\begin{aligned} |\psi\rangle_{abc} = & \frac{1}{\sqrt{2}} \left[\left[\frac{1}{\sqrt{2}} (|+x\rangle_a + |-x\rangle_a) \left(\frac{1}{\sqrt{2}} (|+x\rangle_b + |-x\rangle_b) \right) |0\rangle_c \right] \right] \\ & + \frac{1}{\sqrt{2}} \left[\left[\frac{1}{\sqrt{2}} (|+x\rangle_a - |-x\rangle_a) \left(\frac{1}{\sqrt{2}} (|+x\rangle_b - |-x\rangle_b) \right) |1\rangle_c \right] \right], \quad (3.7) \end{aligned}$$

re-arrangement gives

$$\begin{aligned} |\psi\rangle_{abc} = & \frac{1}{2\sqrt{2}} \left[(|+x\rangle_a + |x\rangle_b + |-x\rangle_a - |x\rangle_b) (|0\rangle_c + |1\rangle_c) \right] \\ & + \frac{1}{2\sqrt{2}} \left[(|+x\rangle_a - |x\rangle_b + |-x\rangle_a + |x\rangle_b) (|0\rangle_c - |1\rangle_c) \right]. \quad (3.8) \end{aligned}$$

Similarly,

$$\begin{aligned}
|\psi\rangle_{abc} = & \frac{1}{2\sqrt{2}} \left[(|+y\rangle_a | +y\rangle_b + | -y\rangle_a | -y\rangle_b) (|0\rangle_c - |1\rangle_c) \right] \\
& + \frac{1}{2\sqrt{2}} \left[(|+y\rangle_a | -y\rangle_b + | -y\rangle_a | +y\rangle_b) (|0\rangle_c + |1\rangle_c) \right]. \quad (3.9)
\end{aligned}$$

From the decomposition of $|\psi\rangle$, we can see that what happens to Charlie's state, when Alice and Bob measure their states. For example, if both Alice and Bob make measurements in the x-direction and get the same result then Charlie will be in the state $\frac{1}{\sqrt{2}} (|0\rangle_c + |1\rangle_c)$ which is $|+x\rangle$ and if they get different result, then he will have the state $\frac{1}{\sqrt{2}} (|0\rangle_c - |1\rangle_c)$ which is $|-x\rangle$. Similarly if they make measurement in y-direction and both get the same results then he will have the state $\frac{1}{\sqrt{2}} (|0\rangle_c - |1\rangle_c)$ which is $|-x\rangle$ and if get different result then this state will be $\frac{1}{\sqrt{2}} (|0\rangle_c + |1\rangle_c)$ which is $|+x\rangle$.

By performing a measurement along x or y direction, Charlie can determine which of these state he has. If Charlie knows in what direction (x or y) Alice and Bob made measurements, he can determine whether they both have same or opposite results but he will not know about their actual results. Similarly, Bob will not be able to know about Alice's result without contact to Charlie because he does not know whether his result is the same as the Alice or the opposite to her. As each person is choosing randomly the direction of measurement (x or y), so there is 50% chance that the GHZ triplet will show a useful correlation.

For instance, when both Bob and Alice measure in x-basis, then Charlie will be constrained to measure his particle in x-basis to get the useful correlation. He will get nothing if he measures his particles in y-basis. Because Charlie chooses randomly the measurement basis, so he will be successful only half time. So in order to enhance the probability of success, all three parties announce their measurement direction. First both Bob and Charlie send their measurement basis to Alice, who then decides the given round is valid or not. From this procedure, Alice makes a key of random bit strings and uses it to encrypt her message.

3.1.3 Security against eavesdropper

Now we are going to discuss the problems of eavesdropping which Alice should take into account. Here Eavesdropper is the fourth member or it is among Bob and Charlie pair that tries to gain access to Alice's results. Eavesdroppers can however be detected by using different protocols.

Now we are going to discuss how it can be detected, let us consider the case that when the eavesdropper is Bob and try to access the Charlie's information and also his own. As he gets two particles from Alice, first he measures them and then transmit any of them to Charlie. Here Bob wants to get what is the result of Alice without contact to Charlie. Now we consider the case when Alice measures in x-basis and the GHZ triplet is

$$\begin{aligned} |\psi\rangle_{abc} &= \frac{1}{\sqrt{2}} [|0\rangle_a |0\rangle_b |0\rangle_c + |1\rangle_a |1\rangle_b |1\rangle_c], \\ &= \frac{1}{2} [| + x\rangle_a (|00\rangle + |11\rangle)_{bc} + | - x\rangle_a (|00\rangle - |11\rangle)_{bc}]. \end{aligned} \quad (3.10)$$

Similarly, when she measures in y-direction

$$|\psi\rangle_{abc} = \frac{1}{2} [| + y\rangle_a (|00\rangle + i|11\rangle)_{bc} + | - y\rangle_a (|00\rangle - i|11\rangle)_{bc}]. \quad (3.11)$$

Bob does not know in which direction Alice made measurement, he has a problem here either he measures in this basis $\frac{1}{2} (|00\rangle \pm |11\rangle)$ or in $\frac{1}{2} (|00\rangle \pm i|11\rangle)$ basis. Since Bob chooses at random, he has a probability of $\frac{1}{2}$ of making a mistake. If he chooses correctly and takes a valid combination of measurement axis, then he will be able to know about the result of Charlie's particle from his measurement. Then he is able to know about Alice's bit. For instance, when Alice makes measurement in x-basis and has result $| + x\rangle$ then the state which Bob has $\frac{1}{2} (|00\rangle + |11\rangle)$. Now when Bob makes measurement in $\frac{1}{2} (|00\rangle \pm |11\rangle)$, he will come to know what is the state of two particle. Since

$$\frac{1}{2} (|00\rangle + |11\rangle) = \frac{1}{2} [| + x\rangle | + x\rangle + | - x\rangle | - x\rangle], \quad (3.12)$$

After measurement Bob came to know Charlie's result is similar to his result. So Bob will get access easily to Alice's bit.

Now we want to see that how Bob's cheating caught, when he choose the wrong basis of measurements. Let us consider when Alice measures in y -basis and Bob makes measurements in x -basis and gets $\frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle)$. He has a half probability to get either basis vector.

Now he sends one of his particles to Charlie and then both Bob and Charlie measure their particles. Since, Alice measures in y -direction, so in order to produce a valid key bit from the measurement results of all three parties, it is necessary for Bob and Charlie have different direction of measurements. We consider the case when Bob and Charlie measure their particles in x and y basis respectively. It is obvious from Bob measurement basis $\frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle)$ no connection in between x and y basis is found. Let us consider $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|0\rangle_b|0\rangle_c + |1\rangle_b|1\rangle_c), \quad (3.13)$$

using Eqs. (3.2), (3.3), (3.4) and (3.5) and after doing some algebra, we have

$$\begin{aligned} \frac{1}{\sqrt{2}} [|0\rangle_b|0\rangle_c + |1\rangle_b|1\rangle_c] &= \frac{1}{2} \left[\exp\left(-i\frac{\pi}{4}\right) (|+x\rangle_b|+y\rangle_c + |-x\rangle_b|-y\rangle_c) \right] \\ &+ \frac{1}{2} \left[\exp\left(+i\frac{\pi}{4}\right) (|+x\rangle_b|-y\rangle_c + |-x\rangle_b|+y\rangle_c) \right], \quad (3.14) \end{aligned}$$

where we have written $\frac{1}{\sqrt{2}} \pm \frac{i}{\sqrt{2}} = \exp(\pm i\frac{\pi}{4})$. From above equation it can be seen that in half the situation the results of the measurement will be wrong. For example, if Alice found $|+y\rangle$ and Bob found $|+x\rangle$ then Charlie should measure in $|-y\rangle$ if he measures his particle in y -direction. But because of Bob measurement (cheating) Charlie also has a probability of $\frac{1}{2}$ in $|+y\rangle$. So in this cheating scheme, the overall probability of an error is $\frac{1}{4}$, one half is for choosing a wrong basis and one half for wrong result. So this increment in error tells to Alice that something unusual is happening.

Now consider when Bob came to know about both Alice and Charlie basis before the announcement of his basis, but he made the wrong measurement basis. When he tells his basis to Alice, both Alice and Charlie notice a failure rate that is higher than usual (75% as against to 50%). To make this kind of cheating more difficult, Alice asks first both Bob and Charlie to send their measurement basis and then announce all three measurement basis. Now in the next section, we will discuss the protocol in which secret sharing is done by using the entanglement of continuous variables.

3.2 Secret sharing by the entanglement of continuous variables

In the previous section, we reviewed the secret sharing by the entanglement of discrete variables, now in this section we are going to review secret sharing scheme given by T. Tyc et.al. [5], which involves the continuous variables (CV) entanglement.

3.2.1 Introduction

A protocol of secret sharing, which is referred as (k, n) threshold secret sharing protocol. In this scheme we have a dealer and he wants to distribute secret message among the m number of players and any k number of players from m parties are enough to retrieve the message. Any arbitrary set of $k - 1$ parties get nothing about that secret message [13].

The secret message is considered as any arbitrary quantum state, and this message is encrypted by the "dealer" into an shared entangled state of m parties and then by the collaboration of authorized group of k players, this message is decrypted and the remaining $m - k$ players form an EPR pair without any information about secret message. [14].

3.2.2 Running the scheme

In this scheme we consider the quantum state $|\psi\rangle$ as secret and we encoded by some how this secret in terms of entangled state $|\Phi\rangle_1 \in H^{\otimes m}$ as m parts one for each party. This entanglement is generated in such a way that when swapping of entanglement is made by the authorized group of players, the secret state may be recovered but the adversary group recover nothing about that state. As the QSS is concerned with the access structure and a general group of adversary, so that in this scheme we consider a particular access structures.

Our present threshold scheme is $(k, 2k - 1)$ having a dealer, which distributes $|\psi\rangle$ (secret state) into the entangled state $|\Phi\rangle_1$ by operating on k collaborators. So the $|\Phi\rangle_1$ is the entangled state which is expressed by the product of $|\psi\rangle$ and $k - 1$ pair wise. Advantages of this entanglement among the collaborator and non-collaborator is that the non-collaborator got nothing about $|\psi\rangle$. Before following the procedure, let us introduce the continuous variable representation for secret

state $|\psi\rangle$. We can express the secrete state $|\psi\rangle$ as

$$\psi(x') = \langle x'|\psi\rangle, \quad (3.15)$$

the canonical position operator \hat{x} are not normalized and it satisfy the orthogonality condition

$$\langle x'|x''\rangle = \delta(x' - x''). \quad (3.16)$$

Since dealer wants to distribute the secret $|\psi\rangle$ among the $2k - 1$ players so that he uses a special kind of linear mapping L on $x \cong (x_1, x_2, \dots, x_k)^T$ in such a way that he defines a specific position for each player such that

$$L : R^k \rightarrow R^{2k} : x \rightarrow L(x) = [x_1, L_1(x), \dots, L_{2k-1}(x)]^T. \quad (3.17)$$

This linear mapping is done in such a way that any components of k -elements subset of $\{x_1, L_1, \dots, L_{2k-1}\}$ are linearly independent and the dealer is used this linear mapping to encode secret $|\psi\rangle$ into the entangled state $|\Phi\rangle$ such as

$$|\Phi\rangle_1 = \int_{R^k} \langle \psi|L(x)\rangle d^k x, \quad (3.18)$$

using Eq. (3.17), we have

$$\begin{aligned} |\Phi\rangle_1 &= \int_{R^k} \langle \psi|(x_1, L_1(x), \dots, L_{2k-1}(x))^T\rangle d^k x, \\ &= \int_{R^k} \psi(x_1, |L_1(x)\rangle, \dots, |L_{2k-1}(x)\rangle)^T d^k x. \end{aligned}$$

Here $|\Phi\rangle_1$ is not normalized because $|x\rangle$ is not. In this way the secrete is first decoded and then distributed among all the parties in the form of entangled state $|\phi\rangle$. Now we are going to see how it can be decoded by the authorized group of players. For this purpose, let us consider $\{r_1, r_2, \dots, r_{2k-1}\}$ as any random permutation of numbers $1, 2, \dots, 2k - 1$, that permutes the linear mapping L such that $\{L_{r_1}, L_{r_2}, \dots, L_{r_k}\}$. As both sets of linear mapping $\{L_{r_1}, L_{r_2}, \dots, L_{r_k}\}$ and $\{x, L_1, L_2, \dots, L_{2k-1}\}$ are not linearly dependent so that a non-singular matrix T' having $k \times k$

dimensions exists, such as

$$T' \begin{bmatrix} L_{r_1} \\ L_{r_2} \\ \vdots \\ L_{r_k} \end{bmatrix} = \begin{bmatrix} x_1 \\ L_{r_{k+1}} \\ \vdots \\ L_{r_{2k-1}} \end{bmatrix}, \quad (3.19)$$

so that for any T' matrix, we have a transformation operator $\hat{U}(T')$ such as

$$U(T') \begin{bmatrix} L_{r_1} \\ L_{r_2} \\ \vdots \\ L_{r_k} \end{bmatrix} = \|T'\|^{\frac{1}{2}} \begin{bmatrix} x_1 \\ L_{r_{k+1}} \\ \vdots \\ L_{r_{2k-1}} \end{bmatrix}, \quad (3.20)$$

or

$$U(T')|L_{r_1}\rangle_{r_1}|L_{r_2}\rangle_{r_2}, \dots, |L_{r_k}\rangle_{r_k} = \|T'\|^{\frac{1}{2}}|x_1\rangle_{r_1}|L_{r_{k+1}}\rangle_{r_2}, \dots, |L_{r_{2k-1}}\rangle_{r_k}, \quad (3.21)$$

where $\hat{U}(T')$ is unitary operator and $\|T'\| = |\det T'|$. Now we have to find the matrix element of unitary operator \hat{U} in the continuous basis $|x''\rangle \equiv |x''_1\rangle_{r_1}, \dots, |x''_k\rangle_{r_k}$, that is we have to calculate $\langle x'|U(T')|x''\rangle$.

First consider

$$\begin{aligned} U(T')|x''\rangle &= \|T'\|^{\frac{1}{2}} \begin{bmatrix} T_{11} & T_{12} & \dots & T_{1k} \\ T_{21} & T_{22} & \dots & T_{2k} \\ \vdots & \vdots & & \vdots \\ T_{k1} & T_{k2} & \dots & T_{kk} \end{bmatrix} \begin{bmatrix} x''_1 \\ x''_2 \\ \vdots \\ x''_k \end{bmatrix}, \\ &= \|T'\|^{\frac{1}{2}} \sum_{j=1}^k T_{ij} x''_j. \end{aligned} \quad (3.22)$$

Now we consider the inner product of two continuous variables such that

$$\begin{aligned}\langle x''|x'\rangle &= (\langle x''_1|\langle x''_2|, \dots, \langle x''_k|) (|x'_1\rangle|x'_2\rangle, \dots, |x'_k\rangle), \\ &= \prod_{i=1}^k \delta(x''_i - x'_i).\end{aligned}\quad (3.23)$$

From Eq. (3.2.2) and Eq. (3.23), the matrix elements can have the values

$$\langle x'|U(T')|x''\rangle = \|T'\|^{\frac{1}{2}} \prod_{i=1}^k \delta\left(\sum_{j=1}^k T_{ij}x''_j - x'_i\right), \quad (3.24)$$

where T_{ij} is the matrix element of T' matrix. Now the collaborators with the shared index by r_1, r_2, \dots, r_k reconstruct the secret state by transforming their shares by the application of $\hat{U}(T)$ as

$$\begin{aligned}\hat{U}(T')|\phi\rangle_1 &= \hat{U}(T') \int_{R^k} \psi(x_1)|L_1(x_1)_{r_1} \dots |L_{2k-1}(x_1)_{r_{2k-1}} d^k x, \\ &= \|T'\|^{\frac{1}{2}} J \int_{R^k} \psi(x_1)|x_1\rangle_{r_1} |\Theta\rangle_{r_2, r_{k+1}} |\Theta\rangle_{r_3, r_{k+2}} \dots |\Theta\rangle_{r_k, r_{2k-1}},\end{aligned}\quad (3.25)$$

where $|\Theta\rangle_{ij} = \int_{R^k} |x\rangle_i |x\rangle_j dx$ and a quantity J called Jacobian comes here due to the change of basis and it has value

$$J = \begin{bmatrix} \frac{\partial L_{r_{k+1}}}{\partial x_1} & \frac{\partial L_{r_{k+1}}}{\partial x_2} & \dots & \frac{\partial L_{r_{k+1}}}{\partial x_k} \\ \frac{\partial L_{r_{k+2}}}{\partial x_1} & \frac{\partial L_{r_{k+2}}}{\partial x_2} & \dots & \frac{\partial L_{r_{k+2}}}{\partial x_k} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{\partial L_{r_{2k-1}}}{\partial x_1} & \frac{\partial L_{r_{2k-1}}}{\partial x_2} & \dots & \frac{\partial L_{r_{2k-1}}}{\partial x_k} \end{bmatrix}. \quad (3.26)$$

Now consider the term $\int \psi(x_1)|x_1\rangle_{r_1} dx_1$ from Eq. (3.25)

$$\begin{aligned}\int \psi(x_1)|x_1\rangle_{r_1} dx_1 &= \int \langle x_1|\psi\rangle |x_1\rangle_{r_1} dx_1, \\ &= |\psi\rangle_{r_1} \hat{I},\end{aligned}\quad (3.27)$$

by using this value, Eq. (3.25) becomes

$$\hat{U}(T')|\phi\rangle_1 = ||T'\|^{\frac{1}{2}}J|\psi\rangle_{r_1}|\Theta\rangle_{r_2,r_{k+1}}|\Theta\rangle_{r_3,r_{k+2}}\cdots|\Theta\rangle_{r_k,r_{2k-1}}. \quad (3.28)$$

From the above equation, it can be seen that the r_1 -th part is the state $|\psi\rangle$ which is our secret and the remaining parts r_2, \dots, r_k are entangled maximally with the parts of unauthorized group of players (adversaries). Thus the secret is decoded in this way from any k parts by the application of unitary operator $\hat{U}(T')$. Any remaining $k - 1$ parts get nothing about the secret $|\psi\rangle$ and they just result in Einstein-Podolski-Rosen (EPR) states.

In next Chapter, we are going to review secret sharing without using entanglement.

Secret Sharing without Entanglement

In the previous chapter, we reviewed two secret sharing schemes, the first one involves the idea of secret sharing among three people by using the entanglement of GHZ states and it was shown that local measurements of GHZ state enables three parties, to generate and share the key for secret sharing. In second scheme, we reviewed a sequential method that involved the multi-party entanglement of continuous variable and established a secret sharing theme. The problem which arises with all the entangled-based methods is that they are not scalable, because the entangled states are difficult to prepare and maintain among growing number of the participants. In this Chapter, to avoid the above mentioned problem, a sequential scheme is reviewed, which is proposed by V. Karimipour et.al [15], for secret sharing in which qubits are controlled by the parties without using any shared entanglement.

4.1 Secret sharing by a single qudit state for a prime d

In this section, we are going to discuss a secret sharing scheme which is free of entanglement and it involves the random hopping of the states by using the qdits (d -level states). In this protocol, we performed the action of some operators on the basis vectors and results into the random hopping.

4.1.1 Introduction

Let us consider the set of MUBS [15]

$$|e_p^j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(p+jk)} |k\rangle, \quad (4.1)$$

where $j = 0, 1, \dots, d$ represents the basis and $p = 0, 1, \dots, d - 1$ labels the basis vector in each individual basis. These states satisfy the property of MUBS

$$|\langle e_p^j | e_{p'}^{j'} \rangle|^2 = \frac{1}{d} \text{ where } j \neq j'. \quad (4.2)$$

This is only true when d is an odd prime because complete set of MUBS exists only for odd d .

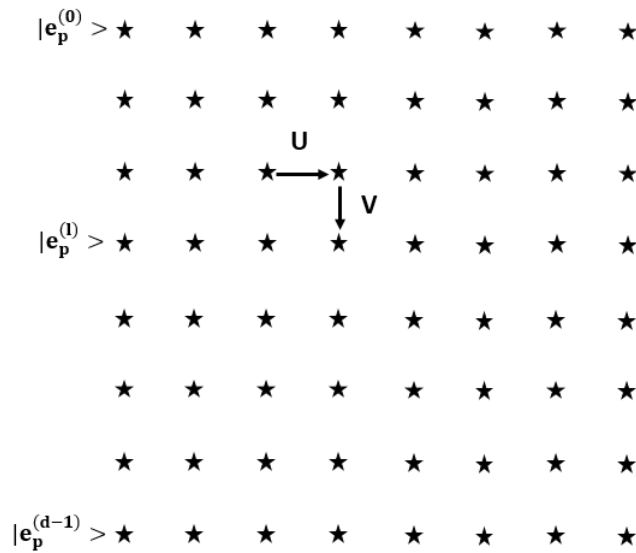


Figure 4.1: The application of operators \hat{U} and \hat{V} by the players generating the random hopping of states in lattice.

We consider these states in a square lattice as shown in Fig. 4.1 and the lattice points have unit distance from each other. The lattice is periodic in both directions so it has a topology of a torus.

4.1.2 Running the scheme

Let us now define the operators

$$\hat{U} \equiv \sum_{k=0}^{d-1} \omega^k |k\rangle \langle k| \quad \text{and} \quad \hat{V} \equiv \sum_{k=0}^{d-1} \omega^{k^2} |k\rangle \langle k|. \quad (4.3)$$

Application of operators \hat{U} and \hat{V} to the states of lattice results in a single-step hopping in the horizontal and vertical of lattice point as shown in Fig. 4.1. We consider $N + 1$ players P_o, P_1, \dots, P_N and the first player may be considered as Alice who will control the protocol and use the secret key for sending the message and Player P_N may be considered as Bob. All the other players considered collectively by Charlie and Bob retrieve Alice's message by contacting to Charlie. The working steps of this scheme are

- The first player P_o (Alice), prepares a state $|e_p^0\rangle$ (the top left corner of the lattice) and apply two operators $\hat{U}^{a_o} \hat{V}^{b_o}$ on it, where $0 \leq (a_o, b_o) \leq d - 1$ are random numbers which she can chose randomly (suppose she chose $a_o = 2$ that will means she apply \hat{U} operator two times on the state). Application of these operators results in hopping the state a_o units forward and b_o units downwards and state passes to the next player.
- The second player P_1 receive the state from P_o and apply its own operators $\hat{U}^{a_1} \hat{V}^{b_1}$ with $0 \leq a_1, b_1 \leq 1 - d$ and state moves a_1 units forward and b_1 units downwards as well as passes to the next player P_2 . This procedure continues until Bob will received the state.
- The last party P_N receives the state from P_{N-1} and performs the same action with its own operators $\hat{U}^{a_N} \hat{V}^{b_N}$ and passes the state to next and makes measurement in next basis which should be $|e_p^0\rangle$.

From Fig. 4.1, we can see that when all the parties apply their respective operators, the point will perform a random hopping and it will move a distance $R \equiv \sum_{i=0}^N a_i$ to the right and $D \equiv \sum_{i=0}^N b_i$ downwards. When the distance $D \equiv \sum_{i=0}^N b_i = 0 \pmod{d}$, this will represent that the point has moved a full round around the torus and landed in the first row. Thus the measurement, which is made by the last player P_N always be done in the first row and the round of random hopping is treated as valid when the result of his measurement m is perfectly correlated with the distance

traveled in the forward direction

$$\sum_{i=0}^N a_i = m, \quad \text{or} \quad -m + \sum_{i=0}^N a_i = 0. \quad (4.4)$$

If Eq. (4.4) is not satisfied, then the round is considered as invalid. For every valid round, a set of completely random dits $(0, 1, 2, \dots, d - 1)$ are shared among all the parties. If we consider p valid rounds and denote the results of Bob's measurement by $\kappa = (-m_1, -m_2, \dots, -m_p)$ and a long sequence of dits by $k_i = (a_{i1}, a_{i2}, \dots, a_{ip})$, then according to Eq. (4.4), we can write as

$$\kappa \oplus k_o \oplus k_1 \oplus k_2 \oplus \dots \oplus k_N = 0, \quad (4.5)$$

where \oplus represents the addition is done dit-wise and modulo 2 and k_o, k_1, \dots, k_N are random chosen keys for each player. Once these randomly shared keys are established among all the players then Alice send the message (M) to Bob in form of $M \oplus k_o$. Since Bob has access of his own key k_N as well as the measurement key κ , so that he can easily retrieve Alice's message by asking the keys to other members $(P_1, P_2, \dots, P_{N-1})$. That is he has to just perform the summation as

$$\begin{aligned} \text{Sum} &= (M \oplus k_o) \oplus k_1 \oplus \dots \oplus k_{N-1} \oplus (k_N \oplus \kappa), \\ &= M \oplus (k_o \oplus k_1 \oplus \dots \oplus k_{N-1} \oplus k_N \oplus \kappa) = M \oplus (0), \\ &= M. \end{aligned} \quad (4.6)$$

In this way Alice sends secret message to her colleague Bob, who retrieves her message by collaboration of all the other players and is unable to do that without them. So we have a successful secret sharing scheme by the random hopping of lattice points but we are restricted to only to prime dimensions d of the mutually unbiased basis. Now in the next topic, we are going to establish a secret sharing scheme which follows the same procedure but it will be for any general dimensional lattice.

4.2 Secret sharing by using a d -level state for any dimensions

In previous topic, the secret sharing in a lattice of states using random hopping motivates us to look for other lattices of other dimensions, shapes, geometries and perform the random hopping to model secret sharing schemes. In order to do that, we consider such a lattice which has again topology of torus but not a square $d \times d$, instead of square, it is torus of $4 \times d$ dimensions, where d is any positive integer [15]. This lattice is based on the property of Fourier transform operator. This operator has properties that when applied to the computational basis, turns it into another basis which is mutually unbiased with respect to it and four times application of this operator on the states does nothing.

We consider a orthonormal d dimensional basis, which is defied as

$$|\phi\rangle = \{|k\rangle, 0 \leq k \leq n - 1\}, \quad (4.7)$$

where n is any arbitrary positive integer and we called this basis as the computational basis because we always measure in this basis. The operator \hat{F} is to be defined as the Fourier transform operator with $u^{mj} = \exp\left[\frac{i2\pi mj}{n}\right]$ be the n -th roots of unity

$$\hat{F} = \frac{1}{\sqrt{n}} \sum_{m,j=0}^{n-1} u^{mj} |m\rangle \langle j|. \quad (4.8)$$

Application of \hat{F} operator on any state $|k\rangle$ results in another state $|a_k\rangle$ such that

$$\begin{aligned} |a_k\rangle &= \hat{F}|k\rangle, \\ &= \frac{1}{\sqrt{n}} \sum_{m=0}^{n-1} u^{mk} |m\rangle, \end{aligned} \quad (4.9)$$

and we call it as another basis $|\psi\rangle$ which is defined as $|\psi\rangle = \{|a_k\rangle, 0 \leq k \leq n - 1\}$ and it is mutually unbiased with respect to $|\phi\rangle$. The square of \hat{F} has the form

$$\hat{F}^2 = \sum_{k=0}^{n-1} |-k\rangle \langle k|. \quad (4.10)$$

This property of Fourier operator reveals that two times application of it on some basis state results in the negative of this basis state. For example

$$\begin{aligned}\hat{F}^2|c\rangle &= \sum_{k=0}^{n-1} |-k\rangle\langle k|c\rangle, \\ &= |-n\rangle,\end{aligned}\tag{4.11}$$

and four times application of Fourier operator is

$$\hat{F}^4 = \hat{I}.\tag{4.12}$$

Proofs of Eqs. (4.10) and (4.12) are in appendix-B. Now consider the generalized Pauli operators

$$\hat{X} \equiv \sum_{k=0}^{n-1} |k+1\rangle\langle k| \text{ and } \hat{Z} \equiv \sum_{k=0}^{n-1} u^k |k\rangle\langle k|,\tag{4.13}$$

operators \hat{X} and \hat{Z} act as shift operators on the basis $|\phi\rangle$ and $|\psi\rangle$ respectively. We first consider the operator \hat{X} as acting on state of basis $|\phi\rangle$ and shifts it into a step forward

$$\begin{aligned}\hat{X}|k'\rangle &= \sum_{k=0}^{n-1} |k+1\rangle\langle k|k'\rangle = \sum_{k=0}^{n-1} |k+1\rangle\delta_{kk'}, \\ &= |k'+1\rangle.\end{aligned}\tag{4.14}$$

Similarly, when the operator \hat{Z} acts on a state of basis $|\psi\rangle$, it shifts it a step forward

$$\begin{aligned}\hat{Z}|a'_k\rangle &= \left(\sum_{k=0}^{n-1} u^k |k\rangle\langle k| \right) \left(\frac{1}{\sqrt{n}} \sum_{m=0}^{n-1} u^{mk'} |m\rangle \right), \\ &= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \sum_{m=0}^{n-1} u^{k+mk'} |k\rangle\langle k|m\rangle,\end{aligned}$$

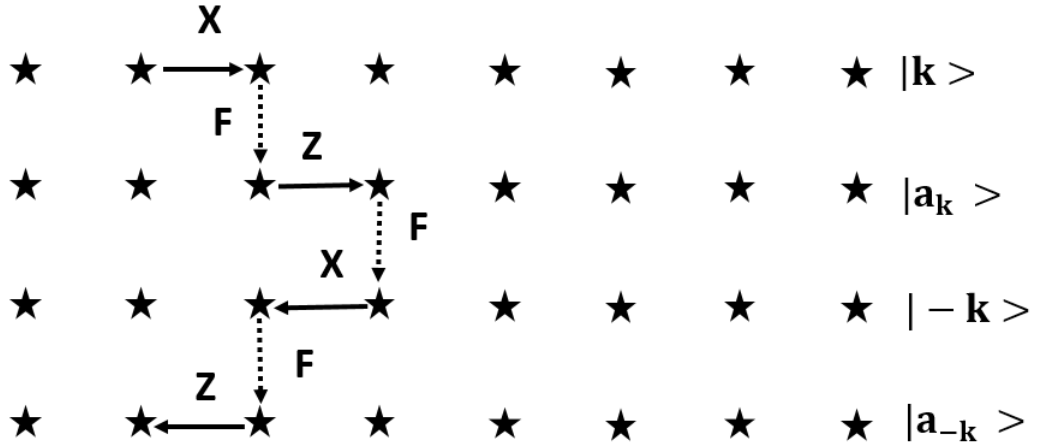


Figure 4.2: The operator X and Z act as shift operators on $|\phi\rangle$ and $|\psi\rangle$ basis respectively. Operator F transform $|\phi\rangle$ into $|\psi\rangle$ and vice versa.

with the property $\sum_{k=0}^{n-1} |k\rangle\langle k| = \hat{I}$, above equation reduces to

$$\begin{aligned}\hat{Z}|a'_k\rangle &= \frac{1}{\sqrt{n}} \sum_{m=0}^{n-1} u^{m+mk'} |m\rangle, \\ &= |a'_{k'+1}\rangle.\end{aligned}\quad (4.15)$$

On the other hand, when the operator \hat{X} acts on state of $|\psi\rangle$, it does nothing without the addition of phase factor. Let us consider the action of \hat{X} on a state $|a_k\rangle$

$$\begin{aligned}\hat{X}|a'_k\rangle &= \left(\sum_{k=0}^{n-1} |k+1\rangle\langle k| \right) \left(\frac{1}{\sqrt{n}} \sum_{m=0}^{n-1} u^{mk'} |m\rangle \right), \\ &= u^{-k'} |a'_k\rangle.\end{aligned}\quad (4.16)$$

Similarly, when the application of \hat{Z} on a state of $|\phi\rangle$ basis, it will act as phase operator

$$\begin{aligned}\hat{Z}|k'\rangle &= \sum_{k=0}^{n-1} u^k |k\rangle\langle k|k'\rangle, \\ &= u^{k'} |k'\rangle.\end{aligned}\quad (4.17)$$

All these properties of the operators are shown in Fig. 4.2. In this figure, the action of operator \hat{Z} on the first and third row and the operator \hat{X} on the second and fourth row is not shown, that means they just add a phase factor there.

4.2.1 Working of the scheme

Similar to the previous section protocol, there are $N + 1$ players and to be specific we name them as, the player R_o is Alice, R_N as Bob and all the other players R_1 to R_{N-1} collectively by Charlie. Alice controls the protocol and she is supposed to send her message (M) to Bob by using the shared secret key and Bob then retrieves the message with collaboration of Charlie. Running steps of this

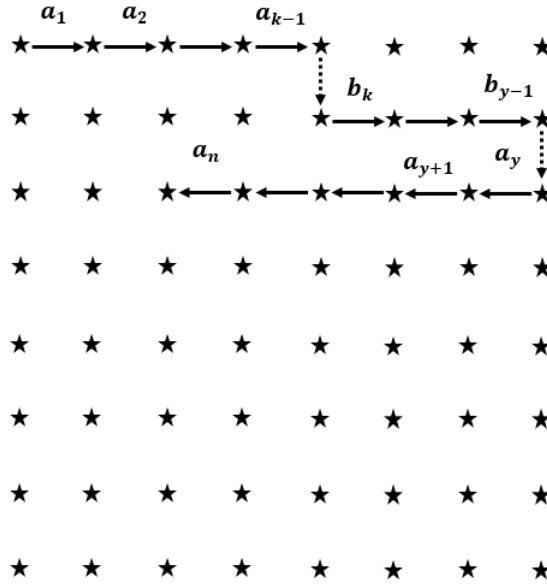


Figure 4.3: Random hopping in the lattice of state and the lattice points are unit distance from each other.

protocol are

- Player R_o starts from state $|0\rangle$ (which is a first basis vector of the computational basis ϕ) and a set of operators $\hat{X}^{a_0} \hat{Z}^{b_0} \hat{F}^{c_0}$ applies to it (where $0 \leq a_0, b_0 \leq n - 1$ are random chosen positive integers and $c_0 = 1, 0$). This application results into the shifting of state a_0 or b_0 times forward in the respective basis and state passes to the next player R_1 . Player R_1 does the same by the operators $\hat{X}^{a_1} \hat{Z}^{b_1} \hat{F}^{c_1}$. This process is repeated until the last player Bob

receives the state. Bob also applies his operators $\hat{X}^{a_N} \hat{Z}^{b_N} \hat{F}^{c_N}$ on the received state and then he measure it in the computational basis. Here c_i has only value 1 or 0, which means that operator \hat{F}^i is applied or not.

- After the measurement by Bob, Alice asks all players R_0, R_1, \dots, R_{N-1} to announce their integer c_i in random orders. There is no need for Bob to announce his c_i integer. It is crucial that the integer values of a_i and b_i chosen by individual player are kept secret and are not announced at any stage.
- After the announcement of c_i value from every player, Bob knowing his own value of c_N , checks the following condition

$$\sum_{i=0}^N c_i = 0 \quad (\text{under the mod } 2). \quad (4.18)$$

If this condition is satisfied then the round will be treated as a valid round and is kept for further analysis, otherwise it is discarded. The condition in Eq. (4.18) reveals that the final state before measurement is landed in $|\phi\rangle$ basis. The reason why Bob doesn't announce his c_N value is that he has the advantage of knowing which round is valid or not.

- In a valid round, Bob's measurement result has a perfect correlation with the random bits applied by all players, including Bob's.

Now we are going to perform a random hopping by following above discussed procedure, consider the Fig 4.3 and it can be seen that only players R_k and R_l apply operator \hat{F} and we have random hopping of states. Then final state will have the form

$$|\beta\rangle = \left| \sum_{i=0}^{k-1} a_i + \sum_{i=k}^{y-1} b_i - \sum_{i=k}^n a_i \right\rangle \doteq |W_{0,k-1} + G_{k,y-1} - W_{y,n}\rangle, \quad (4.19)$$

with $W_{r,s} \doteq \sum_{i=r}^{s-1} a_i$ and $G_{r,s} \doteq \sum_{i=r}^{s-1} b_i$. Similarly, the random hopping of Fig. 4.4 shows that \hat{F} is applied four times by R_m, R_n, R_p and R_l . The corresponding final state is written as

$$|\hat{\beta}\rangle = |A_{0,m-1} + B_{m,n-1} - A_{n,p-1} - B_{p,l-1} + A_{l,k}\rangle. \quad (4.20)$$

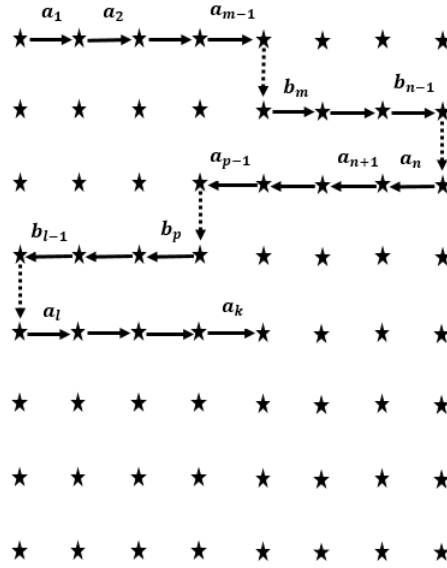


Figure 4.4: A random hopping by the four times application of Fourier operator.

Now we are in a position to understand all the patterns of random hopping. The important point here to emphasize is that after the publicly announcement of c_i numbers, all players, Alice, the middle ones and Bob know the positions of vertical step.

4.2.2 Keys formation of the protocol

Now we are going to explain how the secret keys of each individual player can be arranged and how these can be used to send the secret message. Let us consider we have total six players and two rounds 1 and 2 and the operator \hat{F} is applied two times in each round as shown in Fig. 4.5. The position of operator \hat{F} is at third and fifth players in round 1 and at first and fourth players in round 2. If we denote m and m'' as the measurements values of Bob in round 1 and 2 respectively, then according to Eq. (4.18) it can be written as

$$a_0 + a_1 + a_2 + b_3 + b_4 - a_5 = m, \quad (4.21)$$

$$a_0'' + b_1'' + b_2'' + b_3'' - a_4'' - a_5'' = m''. \quad (4.22)$$

As through the public announcement of c_i values, the positions of operator \hat{F} are known and they know how to arrange their keys K_0, K_1, \dots, K_5 from the d -level integers. For instance, the number

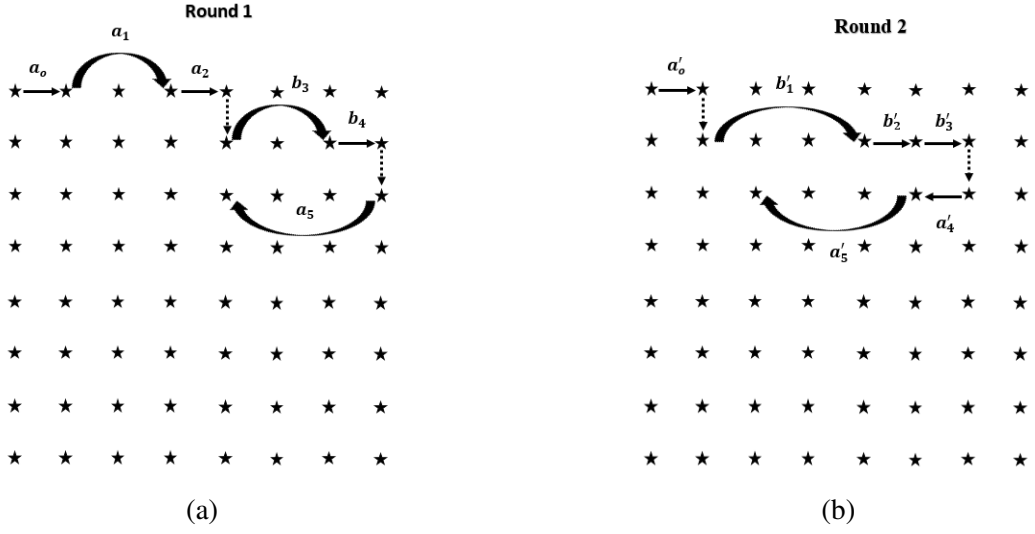


Figure 4.5: Two different paths corresponding to two different random hopping of 6 players (R_o to R_5). In (a) only players R_3 and R_5 apply operator F while in (b) only R_1 and R_4 .

of these keys are

$$\begin{aligned}
 k_o &= (a_o, a''_o, \dots), k_1 = (a_1, b''_1, \dots), k_2 = (a_2, b''_2, \dots), k_3 = (b_3, b''_3, \dots), k_4 = (b_4, -a''_4, \dots), \\
 k_5 &= (-a_5, -a''_5, \dots), \kappa = (-m, -m'', \dots).
 \end{aligned} \tag{4.23}$$

The important point is to be clear that the order of numbers inside the keys is completely random and the continuity of the numbers inside the keys represents that if you have more than two rounds then the respective number can be placed there. After the keys establishment they just have to perform the sum defined in Eq. (4.4) as

$$k_o \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \oplus \kappa = 0. \tag{4.24}$$

From Fig. 4.5, it can be seen that in round 1, the player R_o moves one step forward that means its number has value $a_o = 1$ and player R_1 moves two steps so it has $a_1 = 2$. For other players it can be written as, $a_2 = 1, b_3 = 2, b_4 = 1, a_5 = 3$ and measurement is done at $m = 4$ by the last player. Similarly for round 2, the values of numbers are $a'_o = 1, b'_1 = 3, b'_2 = 1, b'_3 = 1, a'_4 = 1, a'_5 = 3$ and $m' = 2$. Now we arrange the keys from two rounds and this arrangement is arbitrary, we can

choose any order. We consider the order as defined in Eq. (4.23)

$$k_o = (1, 1), k_1 = (2, 3), k_2 = (1, 1), k_3 = (2, 1), k_4 = (1, -1), k_5 = (-1, -3), \kappa = (-4, -2).$$

Now the sum of these keys under the modulus of 2 is calculated as

$$\begin{aligned} &= k_o \oplus k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5 \oplus \kappa, \\ &= (1, 1) \oplus (2, 3) \oplus (1, 1) \oplus (2, 1) \oplus (1, -1) \oplus (-1, -3) \oplus (-4, -2), \\ &= 0. \end{aligned} \tag{4.25}$$

In above equation, the sum of the first entries of all the keys is 2, which is zero under the modulo 2. Similarly the sum of all the second entries of all the keys is 0, and we lead to over all result to be zero. As Alice is sender of secret (M) in this scheme to Bob, and she wants to send secret in such a way that Bob is unable to attend her information without any third party. So that after the creation of randomly shared keys between all the players, Alice combines secret information (M) with her key in the form of $M \oplus k_o$ and then sends this combination to Bob. Since Bob has access of his own key k_N as well as the measurement key κ , so that he first asks the keys of other members (P_1, P_2, \dots, P_{N-1}) and then by using the Eq. (4.24), he can easily retrieve Alice's message.

Tools for Random Hopping of Continuous Variables

In this Chapter, we will discuss some possible tools to generate the random hopping of states. In the first section, random hopping of continuous variables is generated by the application of Fourier and translation operators. In the second section, the displacement operator and squeezing operator will be used for this purpose. The last section of this chapter, includes how any quantum mechanical state is physically displaced.

5.1 Random hopping in continuous basis

In the last chapter, we have described an interesting secret sharing protocol for multi-party, which is based on a single d -level states and free us for using entanglement. We inspired by a recent result of [16] and go for any d -level state. The basic theme of the protocol is that we generate the random hopping of state (state of lattice) by the operation of several operator by one after the other. After validation of certain types of conditions we are able to establish a shared key and then this key is used to sending the required information.

In this chapter, we are going to discuss the possible direction for continuation of this work. There are some possible directions to continue this task, that is we can consider secret sharing with more

general access structure having certain subset of players, which are authorized to retrieve the secret. We can also consider three dimensional lattice, with more number of operators in order to increase the security of the protocol. But here we extend this work to continuous variables that is by considering the continuous lattice size and the $\hat{X}\hat{Z}\hat{F}^c$ turns into $\hat{U}(x_o)\hat{U}(p_o)\hat{\mathcal{F}}^c$, where x_o and p_o are continuous parameters and $c \in \{0, 1\}$. Operators $\hat{U}(x_o) = e^{-ix_o\hat{p}}$ and $\hat{U}(p_o) = e^{ip_o\hat{x}}$ are referred as the translational operators of position and momentum bases respectively. The operator $\hat{\mathcal{F}}$ is Fourier operator that transforms position basis into momentum basis and vice versa.

In order to perform the random hopping in continuous bases, we have to follow a specific procedure. For this, we have a squeezed wave function in position basis and we want to translate it in the same basis

$$\Psi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp\left(\frac{r}{2}\right) \exp\left[-\exp(2r)(x - x_\alpha)^2 + 2ip_\alpha x - ix_\alpha p_\alpha\right]. \quad (5.1)$$

As defined earlier, position translation operator contains momentum operator so that we have to first take a Fourier transform of the given position wave function and convert it into the momentum basis. Take Fourier transform by considering $\hbar = 1$ and simplify the result

$$\begin{aligned} \mathcal{F}\Psi(x) &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}} \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp\left(\frac{r}{2}\right) \exp(ipx) \exp\left[-\exp(2r)(x - x_\alpha)^2 + 2ip_\alpha x - ix_\alpha p_\alpha\right] dx, \\ &= \frac{1}{\sqrt{2\pi}} \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp\left(\frac{r}{2}\right) \exp(-ip_\alpha x_\alpha) \int_{-\infty}^{\infty} \exp(ipx) \exp\left[-\exp(2r)(x - x_\alpha)^2 + 2ip_\alpha x\right] dx, \end{aligned} \quad (5.2)$$

here we suppose $A = \frac{1}{\sqrt{2\pi}} \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp\left(\frac{r}{2}\right) \exp(-ip_\alpha x_\alpha)$ and $\exp(2r) = a$ for our convenience, so after doing some mathematics and inserting $\mathcal{F}\Psi(x) = \psi(p)$ above equation reduces to

$$\psi(p) = A \sqrt{\frac{\pi}{a}} \exp\left[-\frac{(2p_\alpha + p)((2p_\alpha + p) - 4iax_\alpha)}{4a}\right].$$

Now apply position translation operator

$$\hat{U}(x_o)\psi(p) = A \sqrt{\frac{\pi}{a}} \exp(-ix_o\hat{p}) \exp\left[-\frac{(2p_\alpha + p)((2p_\alpha + p) - 4iax_\alpha)}{4a}\right],$$

as we want translation in position basis, so we must have take the inverse Fourier transform

$$\hat{U}(x_0)\mathcal{F}^{-1}\psi(p) = A\sqrt{\frac{\pi}{a}}\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}\exp(-ix_0p)\exp(-ixp)\exp\left[-\frac{(2p_\alpha+p)(2p_\alpha+p-4iax_\alpha)}{4a}\right]dp,$$

so after solving integral and simplification, we get

$$\hat{U}(x_0)\psi(x) = A\sqrt{\frac{1}{2a}}2\sqrt{a\pi}\exp\left[-\exp^{2r}(x+x_0-x_\alpha)^2+2ip_\alpha(x+x_0)\right],$$

Now put back the values of constants A and a , we have

$$\hat{U}(x_0)\psi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}}\exp\left(\frac{r}{2}\right)\exp\left[-\exp(2r)(x+x_0-x_\alpha)^2+2ip_\alpha(x+x_0)-ix_\alpha p_\alpha\right].$$

If we look at Eqs. (5.1) and (5.3), we can see that after the application of translation operator the parameter x is translated into $x+x_0$, thus overall we can write as

$$\hat{U}(x_0)\psi(x) = \psi(x+x_0). \quad (5.3)$$

Similarly, the translation can be generated in momentum bases by the application of $\hat{U}(p_0)$ operator and as a result we will be able to perform a random hopping. Since we have three operators $\mathcal{F}^c\hat{U}(p_0)\hat{U}(x_0)\psi(x)$ with $c = 0, 1$, which we apply on given state. As we have seen earlier $\hat{U}(x_0)\psi(x) = \psi(x+x_0)$ and after the application of first operator, second operator $\hat{U}(p_0)$ is to be applied on the translated state that is $\hat{U}(p_0)(\psi(x+x_0))$ and the result of this application is

$$\begin{aligned} \exp(ip_0\hat{x})\psi(x+x_0) &= \left(\frac{2}{\pi}\right)^{\frac{1}{4}}\exp\left(\frac{r}{2}\right)\exp(ip_0\hat{x}) \\ &\quad \exp\left[-\exp(2r)(x+x_0-x_\alpha)^2+2ip_\alpha(x+x_0)-ix_\alpha p_\alpha\right], \\ &= \exp(ip_0x)\psi(x+x_0). \end{aligned}$$

Above equation shows that the application of momentum translation operator on the position bases does nothing, it just adds a phase factor. Now the third operator which is to be applied is the Fourier transform operator and its application totally depends on the c number. If $c = 0$ then it means that we are not going to apply it, and if $c = 1$ then we must apply the Fourier operator and

its application will lead us into momentum bases

$$\begin{aligned}
\psi(p) &= \mathcal{F}^{c=1} \hat{U}(p_0) \hat{U}(x_0) \psi(x) = \sqrt{\frac{1}{2\pi}} \int_{-\infty}^{\infty} \exp(ipx) \exp(ip_0x) \psi(x + x_0) dx, \\
&= C \exp \left[\frac{1}{4a} [2a(x_o - x_\alpha) - i(p + p_o + 2p_\alpha)]^2 \right], \tag{5.4}
\end{aligned}$$

with $a = \exp(2r)$ and $C = \sqrt{\frac{1}{2a}} \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp \left[-a(x_o - x_\alpha)^2 + 2ip_\alpha x_\alpha \right] \exp \left[-a(x_o - x_\alpha)^2 + 2ip_\alpha x_\alpha \right]$.

We are now shifted into momentum basis. Now by following the same procedure, as used earlier for position basis, we will be resulting into the translation of momentum basis. As a result of the above discussed procedure, we have a random hopping of the basis states and it can be further used for secret sharing purpose.

5.2 Displacing the squeezed state

In this section, we are going to develop a scheme of random hopping in which a state is displaced by the action of displacement operator in a specific bases, then squeezing operator changes the bases into an other one and then again the application of displacement operator results into hopping in that bases. This random hopping in the two bases will then be used for secret sharing process. The scheme is that, suppose we have a state which may be squeezed in position bases or in momentum bases. If it is squeezed in position bases, then the application of displacement operator displaces this state by a specific number in the same bases and n times application of this operator results in n times displacement in the same bases. When the squeezing operator acts on this state, this changes into the momentum bases and now the application of displacement operator does the same as it did in the position bases. In this way we can generate hopping in the given state and it can be used for secret sharing purpose.

Since we want to deal with a state which is comprised of both position and momentum at the same time, so we have to deal with Wigner function of state. But it is not easy to deal with the application of any operator on the Wigner function, so we have to adopt a specific procedure. This procedure is as follows: first of all we find the wave function (in position or momentum bases) of the given state. Then, take the density matrix of that given state and displace it if it is required. Finally, find the Wigner function and the resulting Wigner function will clearly show the hopping of state is

done or not.

Now, let us start with the coherent state wave function in position bases. As the annihilation operator of \hat{x} and \hat{p} is defined as

$$\hat{a} = \frac{1}{\sqrt{2\hbar\omega}} (\omega\hat{x} + i\hat{p}),$$

to make it dimensionless we take $\omega = 1$ and $\hbar = \frac{1}{2}$, so that $\hat{a} = \hat{x} + i\hat{p}$. Since $\hat{p} = -i\hbar\frac{\partial}{\partial x} = \frac{-i}{2}\frac{\partial}{\partial x}$ then above equation reduces to

$$\hat{a} = x + \frac{1}{2}\frac{\partial}{\partial x}. \quad (5.5)$$

As the coherent state is an eigenstate of annihilation operator

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle,$$

take $\langle x|$

$$\hat{a}\langle x|\alpha\rangle = \alpha\langle x|\alpha\rangle, \quad \Psi^\alpha(x) = \langle x|\alpha\rangle,$$

using Eq. (5.5) we have

$$\left(x + \frac{1}{2}\frac{\partial}{\partial x}\right)\Psi^\alpha(x) = \alpha\Psi^\alpha(x),$$

the solution of above differential equation is

$$\psi^\alpha(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp[-(x - \text{Re}\alpha)^2 + 2i\text{Im}\alpha x]. \quad (5.6)$$

This is position wave function of coherent state. As density operator of coherent state is $\hat{\rho}_\alpha = |\alpha\rangle\langle\alpha|$, so Wigner function is written as

$$\begin{aligned} W'(x, p) &= \frac{2}{\pi} \int_{-\infty}^{\infty} \langle x-y|\hat{\rho}_\alpha|x+y\rangle \exp(4ipy) dy, \\ &= \frac{2}{\pi} \int_{-\infty}^{\infty} \psi^\alpha(x-y)\psi^{*\alpha}(x+y) \exp(4ipy) dy. \end{aligned} \quad (5.7)$$

Now using Eq. (5.6), we can calculate easily

$$\psi^\alpha(x-y) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp \left[-(x - \text{Re}\alpha - y)^2 + 2i\text{Im}\alpha(x-y) \right],$$

and

$$\psi^{*\alpha}(x+y) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} \exp \left[-(x - \text{Re}\alpha + y)^2 - 2i\text{Im}\alpha(x+y) \right].$$

After doing some algebra, we have

$$\Psi_\alpha(x-y)\Psi_\alpha(x+y) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \exp \left[-2(x - \text{Re}\alpha)^2 \right] \exp \left[-2y^2 - 4i\text{Im}\alpha y \right],$$

using above equation, Eq. (5.7) reduces to

$$\begin{aligned} W'(x,p) &= \frac{2}{\pi} \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_{-\infty}^{\infty} \exp \left[-2(x - \text{Re}\alpha)^2 \right] \exp \left[-2y^2 - 4i\text{Im}\alpha y \right] \exp \left[4ipy \right] dy, \\ &= \left(\frac{2}{\pi}\right)^{\frac{3}{2}} \exp \left[-2(x - \text{Re}\alpha)^2 \right] \int_{-\infty}^{\infty} \exp \left[-2y^2 + 4i(p - \text{Im}\alpha)y \right] dy, \end{aligned}$$

after solving the integral and simplification, we have

$$W'(x,p) = \frac{2}{\pi} \exp \left[-2(x - \text{Re}\alpha)^2 - 2(p - \text{Im}\alpha)^2 \right],$$

after using the scale transformation for squeezing, it may be written as

$$W'(x,p) = \frac{2}{\pi} \exp \left[-2\xi(x - \text{Re}\alpha)^2 - 2\frac{(p - \text{Im}\alpha)^2}{\xi} \right], \quad (5.8)$$

where ξ is the squeezing parameter. Above equation represents the Wigner function of state, which we want to take as an initial state. Now, we are going to calculate the Wigner function after the application of displacement operator on the initial state. The displacement operator in terms of \hat{x} and \hat{p} is written as $\hat{D}(\alpha) = \exp [2ip_0\hat{x} - 2ix_0\hat{p}]$. Since the operators \hat{x} and \hat{p} do not commute, so

that

$$\hat{D}(\alpha) = \exp[2ip_0\hat{x}] \exp[-2ix_0\hat{p}] \exp\frac{-1}{2}[2ip_0\hat{x}, -2ix_0\hat{p}].$$

Then, after doing some steps of commutator algebra, we have

$$\hat{D}(\alpha) = \exp[2ip_0\hat{x}] \exp[-2ix_0\hat{p}] \exp[-ip_0x_0],$$

and

$$\hat{D}^\dagger(\alpha) = \exp[-2ip_0\hat{x}] \exp[2ix_0\hat{p}] \exp[ip_0x_0].$$

The density operator for our initial state is $\hat{\rho} = |\alpha\rangle\langle\alpha|$, so the displaced density operator is written as

$$\begin{aligned} \hat{\rho}' &= \hat{D}^\dagger \hat{\rho} \hat{D}, \\ &= \exp[-2ip_0\hat{x}] \exp[2ix_0\hat{p}] \exp[ip_0x_0] \hat{\rho} \exp[2ip_0\hat{x}] \exp[-2ix_0\hat{p}] \exp[-ip_0x_0], \\ &= \exp[-2ip_0\hat{x}] \exp[2ix_0\hat{p}] |\alpha\rangle\langle\alpha| \exp[2ip_0\hat{x}] \exp[-2ix_0\hat{p}]. \end{aligned}$$

Now the Wigner function for displaced coherent state is written as

$$\begin{aligned} W''(x, p) &= \frac{2}{\pi} \int_{-\infty}^{\infty} \langle x-y | \hat{\rho}' | x+y \rangle \exp[4ipy] dy, \\ &= \frac{2}{\pi} \int_{-\infty}^{\infty} \exp[-2ip_0(x-y) + 2ip_0(x+y)] \Psi_\alpha(x-y) \Psi_\alpha^*(x+y) \exp[4ipy] dy, \end{aligned}$$

using Eq. (5.6) and after simplifying we get

$$W''(x, p) = \frac{2}{\pi} \exp \left[-2\xi(x - \text{Re}\alpha)^2 - 2\frac{((p - \text{Im}\alpha) + p_0)^2}{\xi} \right]. \quad (5.9)$$

This equation shows that the displacement is done by a factor p_o in the momentum basis by the displacement operator. Similarly, displacement by a factor of x_o will be done, when we will repeat the whole process by using the coherent state wave function in momentum bases. The n times

application of displacement operator will add displacement of nx_o and np_o in the respective bases.

5.3 How a quantum state is displaced

In Chapter 4, we have learnt how a discrete state can be translated or displaced, and this idea is used for implementation of a key to share a secret. In present Chapter, previous sections include how the continuous bases can be translated with the application of some operators which depend on continuous parameters. So far, we have not learnt any idea how any state, discrete or continuous, can be physically displaced. In the present section, we are going to review a method, which is proposed by M.G.Paris [17], how any quantum mechanical state can be displaced and how we can implement this idea.

As we know that the unitary operation of displacement operator $\hat{D}(\alpha)$ on \hat{X} results in the dis-

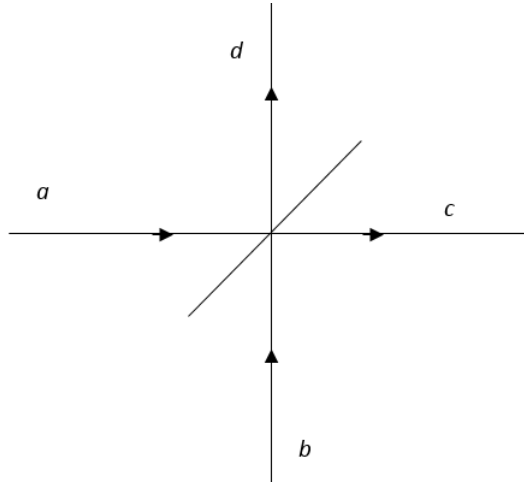


Figure 5.1: Schematic diagram of beam splitter.

placement by a complex number α . The physical implementation of this result can be done with the beam splitter [17]. We take input signal (which we want to displace) on one of the input ports and idler signal on the port of beam splitter which is a coherent state $|z\rangle$ with high intensity.

We can think of beam splitter as a linear medium where the polarization vector is simply proportional to the incoming field $\hat{P} = x\hat{E}$, where $x = x^1$ is the linear first order susceptibility. The relation for field of incoming beam of the device having a and b modes with frequency ω is

$$\hat{E}(r, t) = i\sqrt{\frac{\hbar\omega}{2\epsilon_0 v}} \left[(a + b) \exp i(\vec{k} \cdot \vec{r} - \omega t) + h.c. \right]. \quad (5.10)$$

The interaction Hamiltonian in terms of field and polarization vectors is

$$\hat{H}_I = -\hat{P} \cdot \hat{E} = -x\hat{E}\hat{E} = -x\hat{E}^2, \quad (5.11)$$

using value of \hat{E} from Eq. (5.10) and doing some mathematics

$$\begin{aligned} \hat{H}_I &= -xi\sqrt{\frac{\hbar\omega}{2v\epsilon_0}} i\sqrt{\frac{\hbar\omega}{2v\epsilon_0}} \left[(a + b)e^{i\phi} + (a^\dagger + b^\dagger)e^{-i\phi} \right] \left[(a + b)e^{i\phi} + (a^\dagger + b^\dagger)e^{-i\phi} \right], \\ &= \frac{x\hbar\omega}{2v\epsilon_0} \left[a^\dagger b + ab^\dagger \right]. \end{aligned} \quad (5.12)$$

In general the interaction Hamiltonian and evolution operator for beam splitter in interaction picture is defined as respectively [18]

$$\hat{H}_I = \kappa \left(a^\dagger b + ab^\dagger \right), \quad (5.13)$$

$$\hat{U} = \exp \left[i\kappa \left(a^\dagger b + ab^\dagger \right) \right], \quad (5.14)$$

where κ is coupling constant of the two modes and transmittivity of the device is

$$\tau = \cos^2 \kappa. \quad (5.15)$$

In order to see the value of coupling constant in our case, comparing Eqs. (5.12) and (5.13), we have

$$\kappa = \frac{\chi\hbar\omega}{2v\epsilon_0}, \quad (5.16)$$

so the unitary evolution operator will be

$$\hat{U} = \exp \left[i\frac{\chi\hbar\omega}{2v\epsilon_0} (a^\dagger b + ab^\dagger) \right]. \quad (5.17)$$

Now consider the Eq. (5.15) and insert value of κ from Eq. (5.16)

$$\tau = \cos^2 \kappa = \cos^2 \frac{\chi \hbar \omega}{2v\epsilon_0}, \quad (5.18)$$

and by using the formula $\sin^2 \kappa + \cos^2 \kappa = 1$, Eq. (5.18) can be written as

$$1 - \tau = \sin^2 \frac{\chi \hbar \omega}{2v\epsilon_0}. \quad (5.19)$$

From Eqs. (5.18) and (5.19) we can write

$$\begin{aligned} \tan \left(\frac{\chi \hbar \omega}{2v\epsilon_0} \right) &= \sqrt{\frac{1 - \tau}{\tau}}, \\ \frac{\chi \hbar \omega}{2v\epsilon_0} &= \tan^{-1} \sqrt{\frac{1 - \tau}{\tau}}. \end{aligned} \quad (5.20)$$

Using Eq. (5.20), the unitary evolution operator of Eq. (5.14) becomes

$$\hat{U} = \exp \left[i \tan^{-1} \sqrt{\frac{1 - \tau}{\tau}} (a^\dagger b + ab^\dagger) \right]. \quad (5.21)$$

So the evolution equations of the field modes can be written as

$$\begin{pmatrix} c \\ d \end{pmatrix} = U^\dagger \begin{pmatrix} a \\ b \end{pmatrix} U. \quad (5.22)$$

Now we consider a mode b is our signal and we want it to displace, the idler of the device is taken on mode a which can be supposed a highly intense coherent state $|z\rangle$. The output of the device is written as

$$\begin{aligned} \text{output} &= \text{Tr}_a \left(U^\dagger \hat{\rho}_a \otimes \hat{I}_b U \right) ; \quad a \rightarrow |z\rangle, \\ &= \langle z | U^\dagger | z \rangle \hat{I}_b \langle z | U | z \rangle. \end{aligned} \quad (5.23)$$

From Eq. (5.23), we can see that to find the evolution of input mode, we have to find $\langle z | U | z \rangle$ and $\langle z | U^\dagger | z \rangle$. In order to find similarity transformation of operator \hat{U} , we need first to disentangled

it. The evolution operator \hat{U} can be disentangle by using the Baker-Hausdorff relation for the Schwinger realization of the SU(2) algebra. In SU(2) algebra, we have the following relations: $J_+ = a^\dagger b$; $J_- = ab^\dagger$ and $J_3 = \frac{1}{2}[J_+, J_-]$, which leads to

$$\begin{aligned} J_3 &= \frac{1}{2} [a^\dagger b, ab^\dagger], \\ &= \frac{1}{2} (a^\dagger a - b^\dagger b). \end{aligned} \quad (5.24)$$

For any operator $\hat{A} = \exp [z(J_+, J_-)]$ with $z = \phi e^{i\theta}$, the Baker-Hausdorff relation is define as

$$\hat{A} = \exp \left[\frac{z}{|z|} \tan |z| J_+ \right] \exp [\log(1 + \tan |z|^2) J_3] \exp \left[\frac{-z^*}{|z|} \tan |z| \right]. \quad (5.25)$$

In addition

$$z = |z| = i \tan^{-1} \sqrt{\frac{1-\tau}{\tau}} \quad \text{and} \quad |z|^2 = \tan^{-1} \left(\frac{1-\tau}{\tau} \right), \quad (5.26)$$

so that the operator \hat{U} can be written as by using Eq. (5.25)

$$\hat{U} = \exp \left[i \sqrt{\frac{1-\tau}{\tau}} J_+ \right] \exp \left[\log \left(1 + \frac{1-\tau}{\tau} \right) J_3 \right] \exp \left[i \sqrt{\frac{1-\tau}{\tau}} J_- \right], \quad (5.27)$$

let us take $\xi = i \sqrt{\frac{1-\tau}{\tau}}$ and $\beta = -\log \tau$, above equation reduces to

$$\begin{aligned} \hat{U} &= \exp[\xi J_+] \exp[\log(\frac{\tau+1-\tau}{\tau}) J_3] \exp[\xi J_-] = \exp[\xi J_+] \exp[\log(\frac{1}{\tau}) J_3] \exp[\xi J_-], \\ &= \exp(\xi a^\dagger b) \exp \left[\frac{1}{2} \beta (a^\dagger a - b^\dagger b) \right] \exp(-\xi^* ab^\dagger). \end{aligned} \quad (5.28)$$

Now consider the BCH formula in Heisenberg algebra

$$\exp[t(\hat{X} + \hat{Y})] = \exp(t\hat{X}) \exp(t\hat{Y}) \exp\left(\frac{-t^2}{2} [\hat{X}, \hat{Y}]\right). \quad (5.29)$$

and apply it to the term $\exp[\frac{1}{2}\beta(a^\dagger a - b^\dagger b)]$, we have

$$\exp\left[\frac{1}{2}\beta(a^\dagger a - b^\dagger b)\right] = \exp\left(\frac{1}{2}\beta a^\dagger a\right) \exp\left(\frac{-1}{2}\beta b^\dagger b\right),$$

Eq. (5.28) becomes

$$\hat{U} = A \exp[\rho a^\dagger b] \exp\left[\frac{1}{2}\beta a^\dagger a\right] \exp\left[\frac{-1}{2}\beta b^\dagger b\right] \exp[-\rho^* a b^\dagger] = \exp[\rho a^\dagger b] \exp[-\rho^* a b^\dagger],$$

where $A = \exp[\frac{1}{2}\beta a^\dagger a] \exp[\frac{-1}{2}\beta b^\dagger b]$. Consider the identities

$$\exp(\gamma a^\dagger a) \exp(\delta a) \exp(-\gamma a^\dagger a) = \exp(\delta a \exp(-\gamma)), \quad (5.30)$$

and

$$\exp(\gamma a^\dagger a) \exp(\delta a^\dagger) \exp(-\gamma a^\dagger a) = \exp(\delta a^\dagger \exp(\gamma)), \quad (5.31)$$

and taking $\rho b a^\dagger \rightarrow \delta(a^\dagger)$ and $-\rho b^\dagger a \rightarrow \delta(a)$, operator \hat{U} can have the form

$$\hat{U} = A \exp(\delta a^\dagger) \exp(\delta a).$$

After re-arranging

$$\hat{U} = A \exp\frac{-1}{4}\beta a^\dagger a \exp(\delta a^\dagger) \exp\left(\frac{1}{4}\beta a^\dagger a\right) \exp\left(-\frac{1}{4}\beta a^\dagger a\right) \exp(\delta a) \exp\left(\frac{-1}{4}\beta a^\dagger a\right).$$

After simplification, we have

$$\begin{aligned} \hat{U} &= A \exp\left[-\rho^* a b^\dagger \tau^{\frac{1}{4}}\right] \exp\left[\rho \tau^{\frac{1}{4}} a^\dagger b\right], \\ &= \exp\left[-\rho^* a b^\dagger \tau^{\frac{1}{4}}\right] \exp\left[\rho \tau^{\frac{1}{4}} a^\dagger b\right] \exp\left[\frac{1}{2}\beta a^\dagger a\right] \exp\left[\frac{-1}{2}\beta b^\dagger b\right]. \end{aligned}$$

Now consider $\langle z|\hat{U}|z\rangle$ and putting value of \hat{U} from above equation, we have

$$\begin{aligned}\langle z|\hat{U}|z\rangle &= \left\langle z \left| \exp\left[-\rho^* ab^\dagger \tau^{\frac{1}{4}}\right] \exp\left[\rho \tau^{\frac{1}{4}} a^\dagger b\right] \exp\left[\frac{1}{2}\beta a^\dagger a\right] \exp\left[\frac{-1}{2}\beta b^\dagger b\right] \right| z \right\rangle, \\ &= \exp\left[\rho z b^\dagger \tau^{\frac{1}{4}}\right] \left[-\rho^* \tau^{\frac{1}{4}} z^* b\right] \exp\left[\frac{1}{2}\beta |z|^2\right] \exp\left[\frac{-1}{2}\beta b^\dagger b\right].\end{aligned}\quad (5.32)$$

with $\rho = -\rho^*$. As the displacement operator for the complex amplitude α is defined as

$$D(\alpha) = \exp[\alpha a^\dagger - \alpha^* a],$$

similarly for $\rho \tau^{\frac{1}{4}} z$, it can be written as

$$D(\rho \tau^{\frac{1}{4}} z) = \exp[\rho \tau^{\frac{1}{4}} z b^\dagger - \rho^* z^* \tau^{\frac{1}{4}} b],$$

using formula defined in Eq. (5.29)

$$D(\rho \tau^{\frac{1}{4}} z) = \exp[\rho \tau^{\frac{1}{4}} z b^\dagger] \exp[-\rho^* z^* \tau^{\frac{1}{4}} b] \exp\left(\frac{-1}{2} |\rho|^2 |z|^2 \tau^{\frac{1}{2}}\right).\quad (5.33)$$

So Eq. (5.32) can be written as

$$\langle z|\hat{U}|z\rangle = D(\rho \tau^{\frac{1}{4}} z) \exp\left(\frac{1}{2} |\rho|^2 |z|^2 \tau^{\frac{1}{2}}\right) \exp\left[\frac{1}{2}\beta |z|^2\right] \exp\left[\frac{-1}{2}\beta b^\dagger b\right].\quad (5.34)$$

As we supposed the idler is very intense coherent state so that transmittivity of the device approaches to unity and a slight mixing of input signal and idler are allowed so that we can take the following approximations: $\tau \approx 1$; $1 - \tau \approx 0$; $\beta |z| \rightarrow \infty$ and $|z| \sqrt{1 - \tau} \rightarrow \text{constant}$. By using these approximations, the terms from Eq. (5.34) are reduced as

$$\exp\left(\frac{1}{2}\beta |z|^2\right) = \exp\left(\frac{-1}{2} \log \tau |z|^2\right) \approx 1,$$

$$\exp\left(\frac{-1}{2}\beta b^\dagger b\right) \approx 1,$$

and

$$\exp\left[\frac{1}{2}|\rho|^2|z|^2\tau^{\frac{1}{2}}\right] \approx 1.$$

Eq. (5.34), thus reduces to

$$\langle z|\hat{U}|z\rangle = D(iz\sqrt{1-\tau}) = D(\alpha). \quad (5.35)$$

where $\alpha = iz\sqrt{1-\tau}$ is the complex displacement that the incoming signal displaces. Similarly, it can be proved that $\langle z|\hat{U}^\dagger|z\rangle = D^\dagger(\alpha)$. Now consider the input signal state $\hat{\rho}_{\text{in}}$, which has to be displaced at one of the ports b of beam splitter and other port a as the idler of the device is fed with a highly coherent state $|z\rangle$ then, the evolution of $\hat{\rho}_{\text{in}}$ is written as

$$\begin{aligned} \hat{\rho}_{\text{out}} &= \text{Tr}_a[U^\dagger \hat{\rho}_{\text{in}} \otimes |z\rangle\langle z|U] = \text{Tr}_z[U^\dagger|z\rangle\hat{\rho}_{\text{in}}\langle z|U], \\ &= \langle z|U^\dagger|z\rangle\hat{\rho}_{\text{in}}\langle z|U|z\rangle, \\ &= D^\dagger(\alpha)\hat{\rho}_{\text{in}}D(\alpha). \end{aligned} \quad (5.36)$$

Above equation shows that, input state is displaced. Thus by following the same procedure we can displace any quantum state by using beam splitter and we used a highly intense coherent state as an idler of the device.

Summary and Conclusion

In this thesis, we have studied the secret sharing schemes by using the discrete variables and continuous variables. We have started our discussion by reviewing the theory of discrete and continuous variables which includes quadratures of the electromagnetic field, the squeezing of these operators and conclude that due to unitary evolution, the uncertainty in one of quadratures decreases with the growth in the other one but revolving states remain minimum uncertain. We have also studied the transformations of these variables in linear and non linear optics.

First scheme of secret sharing, which is reviewed, is the secret sharing by using the discrete variable entanglement, where GHZ states are used as discrete states. In this scheme, there are three members Alice, Bob and Charlie and they take one particle from the given triplet of GHZ. Alice, who is the administrator of this protocol, splits the message among Bob, Charlie and herself in such a way that she is able to make a key and then she uses that key to send the secret. In this scheme whenever the eavesdropper, which may be the third party or the dishonest member of Bob-Charlie pair, is trying to cheat, she will be detected.

In second scheme, which is secret sharing by the entanglement of continuous variables, we have studied a particular symmetric variety of secret sharing known as threshold (k, n) secret sharing protocols, and in this protocol a secret is distributed among a group of n parties and k members from n parties are sufficient to retrieve the secret and players other than k get nothing about the secret. The protocol that we studied is $(k, 2k - 1)$ threshold, in which the dealer distributes the secret into entangled state of the protocol. The entangled state of decoded secret is prepared in

such a way that dealer performs a linear mapping and he defines a specific position for each player. In order to reconstruct the secret, we explore an unitary operator $U(\hat{T})$, which acts on the decoded state and retrieves the secret to the authorized k players and the remaining members of the protocol results into EPR states without any information about the secret.

Further we discussed the secret sharing schemes which are free of entanglement. In these schemes, we studied sequential methods of secret sharing that include random hopping of the states by using qdits and it is based on the mutually unbiased basis for the prime dimension as well as for any general dimension. In the first case, we considered the lattice in the form $d \times d$ torus and we have two operators and their application to the lattice (states) results in single step hopping in horizontal and vertical and the state traveled the round trip of the torus. Random hopping of the states results into a correlation in such a way that we end with a procedure for the formation of keys and then these keys are used to send the secret and we conclude this case by a protocol of sharing the secret without entanglement.

In the second case, we consider the torus of $4 \times d$ dimensions and d is any positive integer. In this scheme two computational basis are considered, which are mutually unbiased with respect to each other. A Fourier operator is applied on computation basis, which results into other and four times action of Fourier operator results into same basis with the identity operator. We also considered two generalized Pauli operators, which shift the state one step forward in the respective basis. Thus with the application of these three operators, a random hopping is performed and results into the formation of the key, which is used to share the secret. Further, we extend this idea in continuous basis and we take the momentum and position basis as continuous basis. The Fourier transform operator, position translation operator and the momentum translation operator do the same job as we discussed in discrete case.

In the last of this thesis, we studied the experimental setup for the translation of any quantum state. In this setup we have a beam splitter and its one port includes the state to be displaced and the other port is fed by a highly excited coherent state, which results into the displacement of the quantum state.

Bibliography

- [1] McMahon D. Quantum Computing Explained. John Wiley & Sons; 2007.
- [2] Kim YH, Kulik SP, Shih Y. Quantum Teleportation of a Polarization State with a Complete Bell State Measurement. *Physical Review Letters*. 2001;86(7):1370.
- [3] Braunstein SL, Pati AK. Quantum Information with Continuous Variables. Springer Science & Business Media; 2012.
- [4] Hillery M, Buzek V, Berthiaume A. Quantum Secret Sharing. *Physical Review A*. 1999;59(3):1829.
- [5] Tyc T, Sanders BC. How to Share a Continuous-variable Quantum Secret by Optical Interferometry. *Physical Review A*. 2002;65(4):042310.
- [6] Braunstein SL, Van Loock P. Quantum Information with Continuous Variables. *Reviews of Modern Physics*. 2005;77(2):513.
- [7] Loudon R, Knight PL. Squeezed Light. *Journal of Modern Optics*. 1987;34(6-7):709–759.
- [8] Gerry C, Knight P. *Introductory Quantum Optics*. Cambridge University Press; 2005.
- [9] Zachos C. Crib Notes on Campbell-Baker-Hausdorff Expansions. High Energy Physics Division, Argonne National Laboratory, Argonne. 1999;.
- [10] Sakurai JJ, Tuan SF, Commins ED. *Modern Quantum Mechanics, Revised Edition*. AAPT; 1995.

- [11] Reck M, Zeilinger A, Bernstein HJ, Bertani P. Experimental Realization of any Discrete Unitary Operator. *Physical Review Letters*. 1994;73(1):58.
- [12] Bogoliubov N. On the Theory of Superfluidity. *J Phys*. 1947;11(1):23.
- [13] Deng FG, Li XH, Li CY, Zhou P, Zhou HY. Multiparty Quantum-state Sharing of an Arbitrary Two-particle State with Einstein-Podolsky-Rosen Pairs. *Physical Review A*. 2005;72(4):044301.
- [14] Lance AM, Symul T, Bowen WP, Sanders BC, Tyc T, Ralph TC, et al. Continuous-variable Quantum-state Sharing via Quantum Disentanglement. *Physical Review A*. 2005;71(3):033814.
- [15] Karimipour V, Asoudeh M. Quantum Secret Sharing and Random Hopping: Using Single States Instead of Entanglement. *Physical Review A*. 2015;92(3):030301.
- [16] Tavakoli A, Hameedi A, Marques B, Bourennane M. Quantum Random Access Codes Using Single D-level Systems. *Physical Review Letters*. 2015;114(17):170502.
- [17] Paris MG. Displacement operator by Beam Splitter. *Physics Letters A*. 1996;217(2-3):78–80.
- [18] Prasad S, Scully MO, Martienssen W. A Quantum Description of the Beam Splitter. *Optics Communications*. 1987;62(3):139–145.

Wigner Function for Single Particle

Wigner function for single particle is defined as

$$W'(x, p) = \frac{1}{2\pi\hbar} \left\langle x - \frac{1}{2}y \left| \hat{\rho} \right| x + \frac{1}{2}y \right\rangle \exp\left(\frac{ipy}{\hbar}\right) dy,$$

her we take $\hbar = \frac{1}{2}$ to make dimension less quadrature operators and after replacing y to $2y$ and $dy = 2dy$, we have

$$W'(x, p) = \frac{2}{\pi} \langle x - y | \hat{\rho} | x + y \rangle \exp(4ipy) dy,$$

for pure state, $\hat{\rho} = |\psi\rangle\langle\psi|$, above equation reduces to

$$W'(x, p) = \frac{2}{\pi} \int_{-\infty}^{\infty} \psi(x - y) \psi^*(x + y) \exp(4ipy) dy. \quad (\text{A.1})$$

Now consider the wave function

$$\phi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{4}} e^{\frac{r}{2}} \exp\left[-e^{2r}(x - x_{\alpha})^2 + 2ip_{\alpha}x - ix_{\alpha}p_{\alpha}\right].$$

From Eq. (A.2), we can write easily

$$\begin{aligned}\phi(x-y) &= \left(\frac{2}{\pi}\right)^{\frac{1}{4}} e^{\frac{r}{2}} \exp \left[-e^{2r}(x-x_\alpha-y)^2 + 2ip_\alpha(x-y) - ix_\alpha p_\alpha \right], \\ \phi^*(x+y) &= \left(\frac{2}{\pi}\right)^{\frac{1}{4}} e^{\frac{r}{2}} \exp \left[-e^{2r}(x-x_\alpha+y)^2 - 2ip_\alpha(x+y) + ix_\alpha p_\alpha \right],\end{aligned}$$

also

$$\begin{aligned}\phi(x-y)\phi^*(x+y) &= \left(\frac{2}{\pi}\right)^{\frac{1}{2}} e^r \exp \left[-e^{2r}((x-x_\alpha-y)^2 + (x-x_\alpha+y)^2) + 2ip_\alpha(x-y-x-y) \right], \\ &= \left(\frac{2}{\pi}\right)^{\frac{1}{2}} e^r \exp \left[-2e^{2r}(x-x_\alpha)^2 \right] \exp \left[-2e^{2r}y^2 - 4ip_\alpha y \right].\end{aligned}\quad (\text{A.2})$$

Now insert Eq. (A.2) into Eq. (A.1) we have

$$W'(x,p) = \left(\frac{2}{\pi}\right)^{\frac{3}{2}} e^r \exp \left[-2e^{2r}(x-x_\alpha)^2 \right] \int_{-\infty}^{\infty} \exp \left[-2e^{2r}y^2 + 4i(p-p_\alpha)y \right] dy,$$

let us take $B = \left(\frac{2}{\pi}\right)^{\frac{3}{2}} e^r \exp[-2e^{2r}(x-x_\alpha)^2]$ and solving the above equation by compleat square, we have

$$\begin{aligned}W'(x,p) &= B \int_{-\infty}^{\infty} \exp[-2e^{2r}y^2 + 4i(p-p_\alpha)y] dy = B \int_{-\infty}^{\infty} \exp[-2e^{2r}(y^2 - 2e^{-2r}i(p-p_\alpha)y)] dy, \\ &= B \int_{-\infty}^{\infty} \exp[-2e^{2r}(y + ie^{-2r}(p-p_\alpha))^2 - 2e^{-2r}(p-p_\alpha)^2],\end{aligned}$$

using the Gaussian integral formula $\int_{-\infty}^{\infty} e^{-\alpha(x+b)^2} dx = \sqrt{\frac{\pi}{\alpha}}$, above equation reduces to

$$W'(x,p) = B \sqrt{\frac{\pi}{2e^{2r}}} \exp \left[-2e^{-2r}(p-p_\alpha)^2 \right],$$

after simplification

$$W'(x,p) = \frac{2}{\pi} \exp \left[-2e^{2r}(x-x_\alpha)^2 - 2e^{-2r}(p-p_\alpha)^2 \right]. \quad (\text{A.3})$$

Square of Fourier Operator

Fourier operator defined as

$$\hat{F} = \frac{1}{\sqrt{d}} \sum_{m,j=0}^{d-1} \omega^{mj} |m\rangle \langle j|. \quad (\text{B.1})$$

Take self multiplication of this operator

$$\begin{aligned} \hat{F}^2 &= \hat{F} \times \hat{F} = \left(\frac{1}{\sqrt{d}} \sum_{m,j=0}^{d-1} \omega^{mj} |m\rangle \langle j| \right) \times \left(\frac{1}{\sqrt{d}} \sum_{m',j'=0}^{d-1} \omega^{m'j'} |m'\rangle \langle j'| \right), \\ &= \frac{1}{d} \sum_{m,j=0}^{d-1} \sum_{m',j'=0}^{d-1} \omega^{mj} \omega^{m'j'} |m\rangle \langle j| m'\rangle \langle j'|, \\ &= \frac{1}{d} \sum_{m,j=0}^{d-1} \sum_{m',j'=0}^{d-1} \omega^{mj} \omega^{m'j'} |m\rangle \langle j'| \delta_{jm'}, \end{aligned}$$

as $\delta_{jm'}$ in above equation goes to 1 for $j = m'$, so that

$$\begin{aligned} \hat{F}^2 &= \frac{1}{d} \sum_{m,m'=0}^{d-1} \sum_{m',j'=0}^{d-1} \omega^{mm'} \omega^{m'j'} |m\rangle \langle j'|, \\ &= \frac{1}{d} \sum_{m'=0}^{d-1} \sum_{m,j'=0}^{d-1} \omega^{mm'} \omega^{m'j'} |m\rangle \langle j'|, \end{aligned}$$

using definition of roots of unity $\omega^{mm'} = \exp\left(\frac{i2\pi mm'}{d}\right)$ in above equation, we have

$$\begin{aligned} &= \frac{1}{d} \sum_{m'=0}^{d-1} \sum_{m,j'=0}^{d-1} \exp\left[\frac{i2\pi mm'}{d}\right] \omega^{m'j'} |m\rangle \langle j'|, \\ &= \frac{1}{d} \sum_{m'=0}^{d-1} \sum_{m,j'=0}^{d-1} \exp\left[\frac{-i2\pi(-mm')}{d}\right] \omega^{m'j'} |m\rangle \langle j'|, \end{aligned}$$

here we consider $\exp\left[\frac{-i2\pi(-mm')}{d}\right] = \overline{\omega^{-mm'}}$

$$\begin{aligned} &= \frac{1}{d} \sum_{m'=0}^{d-1} \sum_{m,j'=0}^{d-1} \overline{\omega^{-mm'}} \omega^{m'j'} |m\rangle \langle j'|, \\ &= \frac{1}{d} \left(\sum_{m'=0}^{d-1} \overline{\omega^{-mm'}} \omega^{m'j'} \right) \sum_{m,j'=0}^{d-1} |m\rangle \langle j'|, \end{aligned} \tag{B.2}$$

consider the identity of roots of unity

$$\sum_{k=0}^{n-1} \overline{\omega^{(jk)}} \omega^{j'k} = n\delta_{jj'},$$

using this identity, Eq. (B.2) becomes

$$\begin{aligned} &= \frac{1}{d} (d\delta_{-mj}) \sum_{m,j'=0}^{d-1} |m\rangle \langle j'|, \\ &= \sum_{m,j'=0}^{d-1} |m\rangle \langle j'| \delta_{-mj}, \\ &= \sum_{j'=0}^{d-1} | -j' \rangle \langle j'|, \end{aligned}$$

since m, j are dummy variables, so we can write as in general

$$\hat{F}^2 = \sum_{k=0}^{d-1} | -k \rangle \langle k|. \tag{B.3}$$

Fourth Power of Fourier Operator

Now taking the self multiplication of the operator \hat{F}^2

$$\hat{F}^4 = \hat{F}^2 \times \hat{F}^2, \quad (\text{B.4})$$

using Eq. (B.3), we have

$$\begin{aligned} \hat{F}^4 &= \left(\sum_{k=0}^{d-1} | -k \rangle \langle k | \right) \times \left(\sum_{k'=0}^{d-1} | -k' \rangle \langle k' | \right), \\ &= \sum_{k=0}^{d-1} \sum_{k'=0}^{d-1} | -k \rangle \langle k' | \langle k | -k' \rangle = \sum_{k=0}^{d-1} \sum_{k'=0}^{d-1} | -k \rangle \langle k' | \delta_{-kk'}, \\ &= \sum_{k=0}^{d-1} |k\rangle \langle k| = \hat{I}. \end{aligned} \quad (\text{B.5})$$