Quantum Secret Sharing in a Distributed Quantum Network

Dissertation submitted in partial fulfillment of the requirements for the degree of Master of Computer Science

by

Partha Mukhopadhyay
(Roll No. mtc0016)

under the supervision of

Dr. Guruprasad Kar
Physics and Applied Mathematics Unit
I.S.I.

Department of Computer Science
Indian Statistical Institute
Kolkata - 700 108

Physics And Applied Mathematics Unit

Indian Statistical Institute

This is to certify that the dissertation entitled "Quantum Secret Sharing in a Distributed Quantum Network" has been carried out by Partha Mukhopadhyay under my guidance and supervision and is accepted in partial fulfillment of the requirement for the degree of Master of Computer Science.

Guruprasad Kar. 25.7.2002

Guruprasad Kar
Physics and Applied
Mathematics Unit
I.S.I
Kolkata
India

Acknowledgements

I gratefully acknowledge the guidance and support rendered to me by Dr. Guruprasad Kar in preparing the report, developing the concepts of the subject and related topics which was absolutely new to me. My special thanks to Mr. Sibasish Ghosh , Mr. Anirban Roy and Mr. Debasis Sarkar for their all sorts of help to me in understanding the problem I have dealt and providing many useful suggestions.

Partha Mukhopadhyay 25.7.02

Partha Mukhopadhyay

Computer Sc. Division,
Indian Statistical Institute
Kolkata 108

Contents

Chapter 1

Overview

1.1 Introduction

Quantum computation and quantum information is the study of information processing task that can be accomplished using quantum mechanical system.Like many simple but profound ideas it was a long time before anybody thought of doing information processing using quantum mechanical system.

The story began at the turn of the twentieth century when a revolution was going in science. Several problem arisen in physics. To explain those problems the modern theory of Quantum mechanics was introduced . Since then quantum mechanics has been an indispensable part of Science , and has been applied with enormous success to everything under and inside Sun , including the structure of the atom , superconductors , the structure of DNA , and the elementary particles of Nature.

What is Quantum mechanics ? in a word quantum mechanics is a mathematical framework for the construction of physical theory.For example Quantum electrodynamics can describe the interaction of atoms and light with accuracy. Quantum electrodynamics is built under the framework of quantum mechanics. The relation of a particular physical theory like Quantum electrodynamics with quantum mechanics is just as computer operating system is related to a specific application software.

The rules of quantum mechanics are simple but even the experts find them counterintuitive. One of the major goals of quantum information and quantum computation is to develop tools which sharpen our intuition about quantum mechanics. In the early 1980 the interest arose whether it is possible to signal faster than light using quantum mechanics which is a big no-no according to Einstein's theory of relativity. This problem has a nice implication towards another famous problem of quantum mechanics - can we clone an unknown quantum state ? If the answer is 'yes' then it is possible to signal faster than light! fortunately it was proved that unknown quantum state can not be cloned in general - a landmark result of quantum mechanics which effectively supports Einstein's theory of relativity.Another related historical strand contributing to the development of quantum computation and quantum information is the interest dating to the 1970s , of obtaining complete control over single quantum system.Since the 1970s many technique for controlling single quantum state has been developed. Quantum computation and Quantum information naturally fits into this problem. Despite this intense interest , efforts to build quantum information processing systems have resulted in modest success to date. Small quantum computers , ca-

pable of doing dozen of operations on a few qubits(state of a two level quantum mechanical system) represent the current art of practical quantum computing. Experimental prototype of quantum cryptography has been demonstrated and has reached in the level of real world application.

So far we have been talking about rules and power of quantum mechanics. But what this has to do with computer science? Let us now turn our attention to computer science - another triumph of twentieth century. The modern incarnation of computer science was announced by Alan Turing in a remarkable paper in 1936. Turing developed a model of computation known as Turing machine , which now we know as programmable computer. Turing showed that there is a Universal Turing Machine(UTM) which can be used to simulate any other Turing machine. Furthermore he claimed that the Universal Turing machine completely captures what is means to perform a task by algorithmic means. That is , if an algorithmic can be performed on any piece of hardware , then there is an equivalent algorithm for a UTM which performs the same task as the algorithm running on the *personal* computer. This assertion is known as Church - Turing thesis.

On the other hand Computer hardware development really was of to a pace when Barden, Brattain, Shockley developed transistor(1947). The enormous growth of computer hardware was codified by Gordan Moore which is known as Moore's law. The laws states that computer power will double for constant cost roughly once every two years.

Amazingly Moore's law held true in the decades since 1960s. Nevertheless, most observers expect that the dream run will end some time during the first two decades of twenty-first century.The approach to fabrication technology will not help because the size of the chips are going small and small and quantum effect has stared to dominate the current IC fabrication technology. So it seems that if we want to overcome the problem we really need to go in different computing paradigm. Fortunately quantum computation and the possibility of building quantum computer has really shown a real challenge towards this above mentioned problems. But the earlier question arose if classical computer can simulate quantum computer? The answer was given by Richard Feynman. He showed that if quantum computer is simulated by classical one then the effectiveness of quantum computer will be reduced and it's computing power will not be exploited totally.

So Feynman's idea suggested that we need to built quantum computer if we want to use the power completely. So far lot of progress has made towards the building of quantum computer and the progress rate is not too bad. IBM has already made a small model of quantum computer. So the hope of making an useful quantum computer within next, may be 5yrs are very well alive.

Let us now look for what quantum computer can do in principle? and what is it's advantage over today's even best computer? It is really nice to say that quantum computer can be used to perform some tasks in real time (polynomial time) which have no known real time algorithm in classical computer at least up

to these days.

Let us now again turn our attention towards Church-Turing thesis(Strong!). Randomized algorithm pose a challenge to the strong Church-Turing thesis. There is some problem which have solution through randomized algorithm but are not yet possible to solve with deterministic Turing machine. This threat to C-T thesis was solved by adding a rather ad-hoc portion in the C-T thesis. The modified C-T thesis was:

Any algorithmic process can be simulated efficiently using a probabilistic Turing machine

This ad-hoc change motivated Deustch. He began to think that is there any paradigm of computing whose equivalence is absent in even the modified Church Turing thesis. Fortunately he got an example. Suppose we have a boolean function of single variable. Call the function f(x) where x ϵ{0,1}. Suppose it is required say 1hr to compute the function in today's computer (it must be complicated !). So if we are asked to check whether the function is constant or balanced in 1hr on a single processor system, simply we can not. Deustch was able to design a quantum algorithm to effectively conclude within the required time, whether the function is balanced or not. After this remarkable result by Deustch, he himself with Josza extended this procedure to a n variables boolean function. The problem was as follows: Given a n variable boolean function f where the promise is given that the function is either constant or balanced. The problem is to decide in polynomial time whether the function is balanced or constant. This problem has no solution by classical algorithm in polynomial time. But the Deustch-Josza algorithm showed that quantum circuit can be made which can decide the problem in polynomial time!

But the most striking result came in 1994 when Peter Shor developed a polynomial time algorithm for factorization. Factorization is a problem which has no polynomial time algorithm in classical computation so far. It is the shor's result which really motivated computer scientists to think seriously about quantum computation. Beside Deustch-Josza & Shor's algorithm another landmark algorithm came through Grover. Popularly known as Grover's search algorithm. Grover's algorithm is a search algorithm. If some one is given an unsorted file and asked to search for a particular one , the worst case classical time complexity is O(N) where N is the no of entity in the file. Surprisingly the worst case performance of Grover's algorithm is $O(\sqrt{N})$.

What are the sources of the enormous power of these quantum algorithm? The answer in a word is "Quantum parallelism". What is meant by quantum parallelism? Let's think about it in informal way. We will come to more formal definition later. We all know that the smallest unit of computation in classical computation is bit. It can be either zero or one. Can it be in the superposed state of zero and one? From classical computing view the answer is a big 'no-no'.

But let us think about qubit, the fundamental unit of quantum computation. Let us consider the state of a two level qubit $|\psi\rangle$. It can be in the state $|0\rangle$ or $|1\rangle$. Surprisingly enough it can be in the state of a superposition of $|0\rangle$ & $|1\rangle$, i.e it can be in the state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. This feature is really allowed by the superposition principle of quantum mechanics.

Now one can informally think as the quantum state can be in a superposition of $|0\rangle$ & $|1\rangle$ so the essence of zero and one come together and create parallelism. Informally speaking this intuition is quite correct. We will come to more formal prescription when we will be dealing with quantum algorithm.

One of the ever biggest question of computer science is "Whether P=NP or not". This question arose many many years back and remains unanswered ever since instead of some intense effort by some of the best brains. After the remarkable "Shor's magic" people started to think about whether quantum computer can resolve the big question. Here we note that factorization problem is NPI problem (not known to be NP complete). So solving factorization problem in polynomial time does not give any help towards solving "P=NP" issue.

Many effort have been made to attack this NP complete problem by quantum algorithm. But designing polynomial time quantum algorithm for this problems seems very difficult and looks as hard as designing classical algorithm for this problems. There is recently some weak indication by C.H.Bennett that even quantum computer will not be able to solve NP complete problems in polynomial time. Although still it is widely believed and proved to be fruitful in many cases that quantum algorithm can surely speed up some NP complete problems, which is also an almost impossible task by classical means.

Let's now move from computer science to information theory. One of the most fascinating aspects of recent work in fundamental quantum theory is the emergence of a new notion, the concept of quantum information, which is quite different from it's classical counterpart.

We may think of classical information as being embodied in a physical system which has been prepared in a state unknown to us. By performing a measurement to identify the state we acquire the information. We know that the fundamental unit of classical information, a bit, can have value either 0 or 1. We often allows the receiver to have some prior knowledge about the values, say 0 will be received with probability p0(respectively p1). Shannon's theory in this scenario gives a precise mathematical quantification of information and leads to great practical interest.

One of the most striking difference between classical and quantum information is the role of measurement. Given a classical we can always with certainty tell that if it's value is 0 or 1. No problem. But the scenario is not so simple in case of qubit. Suppose we are given a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 \quad 1$. The orthonormal basis is given by $\{|0\rangle, |1\rangle\}$.

What does it mean? It means that one can find the qubit in the state $|0\rangle$ with probability $|\alpha|^2$ and can find it in the state $|1\rangle$ with probability $|\beta|^2$ respectively.

But to get the information we have to measure the qubit and it will project the state in one of the two orthonormal basis vector and the information about the original qubit will be lost for ever. This type of feature never arise in classical information processing.

Another most striking difference with classical and quantum information is the "No cloning theorem". Given a classical bit we can make as many copies as required of this bit. But in case of qubit quantum mechanics does not allow us to copy an unknown quantum state perfectly!.

Despite of all the interesting feature, the most remarkable feature of quantum mechanics is the nonlocal correlation. Nonlocal correlation comes from the feature of "Quantum Entanglement", the heart of quantum information.

What is mean't by quantum entanglement and nonlocal correlation? Let's begin informally. Suppose Alice and Bob are supplied a joint quantum state $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ [1]. Now it is asked that what are the individual state of Alice and Bob. Simple, both of them having state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (just factorize $|1|$). Now if Alice measure his qubit and gets $|0\rangle$ then what is the state of Bob. Clearly it is either $|0\rangle$ or $|1\rangle$ with probability 0.5 in both cases. So Alice gets no information about Bobs state on average.

Now consider a little different situation. Assume Alice and Bob are supplied state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Now they are asked about there individual state. What will be the answer? Note one can not factorized as before. So conclusion is that Alice and Bob exist together, they can not be separated. They are entangled.

Now let us see how entanglement can interact with information retrieval. Assume Alice and Bob are now separated far far away. Alice measures his qubit and gets $|0\rangle$. Then Alice immediately know that Bob's state is projected into state $|0\rangle$. So though Alice and Bob are separated by any distance nonlocal correlation always exists between them!

Using this type of nonlocal correlation and entanglement Benett and Brassad developed quantum teleportation. It is the quantum teleportation which dramatically changed quantum information theory and information theorists were stunned by the power of quantum mechanics. Informally speaking quantum teleportation is just analogous to classical fax machine. By quantum teleportation an unknown quantum state can be transferred to a distance party using only local operation and classical communication. Beside teleportation another remarkable protocol namely Quantum dense coding have been developed. Since then rate of progress of quantum information is enormous. And today scientists are trying mostly to quantify quantum entanglement more accurately, effort have been going to make quantum information more quantified just as classical information (thanks to Shannon). Lot of progress have been made in this field.

This incredible features of quantum mechanics has started to interact with the world of secured communication, cryptology. As Shor's algorithm can factorize in polynomial time the widely used crypto system like RSA are seems to be already

in trouble. Quantum mechanics has shown the way of designing some incredible crypto protocol which can not be broken even by the use of quantum computer. Some of these protocol have been implemented already. We will come back to all those issues more formally later in this work.

1.2 Future Direction

Clearly the technology must progress a long way before quantum computers are ready to fulfill their destiny as the world's fastest machines. There is a long road ahead. But somewhere at the end of that road, high on a hill, stands a shining castle. We are just beginning to venture down that road. Researcher has started to believe that we will eventually arrive at the gates of the castle though the way may be difficult. But when that will be? difficult to answer at this stage. May be another 5-6yrs we have to wait.

On the other hand the technology for quantum information theory is much more mature than quantum computation. Prototype crypto system has all ready been implemented and almost reached to commercial level. Quantum teleportation has been reported to realized effectively. And from many experimental facts we are now in a position to understand the differen feature of quantum information more correctly.

So the road to road to quantum computation may be a long one, and there is no telling for sure how long, but it certainly has been and will continue to be a fascinating voyage.

We strongly believe this century is going to experience one of the ever fascinating discovery of science and technology - Quantum Computer. It's the challenge for today's engineers and physicist.

Chapter 2

Basic Quantum Mechanics

2.1 Introduction

In this chapter I am going to describe some basic laws and result of quantum mechanics that is required for the study of Quantum information and Quantum computation. In most of the cases I will describe only the required result or some brief proofs that will be useful for our purpose. Intense mathematical treatment will be avoided in some cases. Rather we will rely more on physical and computing technique to describe the results of quantum mechanics.

2.2 Hilbert Space Formulation of Quantum Mechanics

In a word Quantum Mechanics can be described as a mathematical model of physical world. To understand the model properly Hilbert Space formalism was introduced.

Hilbert Space:

1. It is a vector space H defined over $\mathbb{C}$ (space of complex numbers). Vectors will be indicated generally by Dirac notation e.g $|\psi\rangle$.

2. Inner product is defined as $\langle .|. \rangle : H \otimes H -> \mathbb{C}$ has the following property

(i) Positivity: $\langle \psi|\phi\rangle > 0$;

(ii) Linearity: $\langle \phi(a|\psi\rangle + b|\varphi\rangle) = a\langle\phi|\psi\rangle + b\langle\phi|\varphi\rangle$.

(iii) Skew symmetry: $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

3.It is complete in norms:$||\phi|| = \langle\psi|\phi\rangle^{\frac{1}{2}}$

Meaning of quantum state:

Quantum states are encoded version of a physical reality. In Hilbert space they are treated as a vector.

Observables:

Observable is a property of a physical system that in principle can be measured. In quantum mechanics the observable are self adjoint operator.

Let A be an operator. It's adjoint $A^\dagger$ is defined as:

$$\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle.$$

A is said to be self adjoint iff $A = A^\dagger$. Any self adjoint operator has a spectral decomposition in a Hilbert Space. For example A can be written as:

$$A = \Sigma a_n P_n$$

where a_n is the eigen value and P_n is the corresponding orthogonal projector on the space of eigenvectors with the eigen value a_n.

Measurement

In Quantum mechanics measurement of an observable means getting a eigen value of the operator as a outcome with a certain probability. The original quantum state is projected onto a eigen state of the corresponding eigen value. e.g

If $A = \Sigma a_n P_n$ then the probability that the measured outcome will be a_n is given by $P = \langle\phi|P_n|\phi\rangle$ where ϕ is the original quantum state before the measurement. The final state of the system is projected into $\frac{P_n|\phi\rangle}{\langle\phi|P_n\phi\rangle^{1/2}}$.

Dynamics:

The evolution of a quantum state is unitary i.e it's dynamics is given by a self adjoint unitary operator called it's Hamiltonian (H). The dynamics of a state is given by

$$\frac{d}{dt}|\psi\rangle = -iH|\psi(t)\rangle.$$

2.3 Qubit

The fundamental unit of information in classical information theory is a bit. Which can take value either 0 or 1 at a time. The fundamental unit of information in Quantum information theory is qubit. If we consider two dimensional Hilbert space with two orthogonal vectors $|0\rangle, |1\rangle$ then the most general form of a qubit defined over that hilbert space is given by;

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ where } |\alpha|^2 + |\beta|^2 = 1.$$

The meaning of the qubit is that if we measure $|\psi\rangle$ in the basis $|0\rangle, |1\rangle$ then the probability that $|0\rangle$ is obtained is $|\alpha|^2$ and the probability that $|1\rangle$ is obtained is $|\beta|^2$.

2.4 Density Operator

We starts with an example. Let we are given a two particle state $|\psi\rangle = a|00\rangle + b|11\rangle$. Now if first particle is measured in the basis $\{|0\rangle, |1\rangle\}$ then if we get result $|0\rangle$ (with probability $|a|^2$) we know that the state of the second particle is immediately projected to $|0\rangle$. Similar cases arise for the other case. So we see that the first and second particle are highly correlated. If we know the state of one then we can deterministically say about the state of the second particle.

Now let us consider an observable acting M acting on the first particle. This is expressed as $M \otimes I$. The expected value of the observable in the state $|\psi\rangle$ is given by:

$$\langle\psi|M \otimes I|\psi\rangle = (a^*\langle 0| \otimes \langle 0| + b^*\langle 1| \otimes \langle 1|)(M \otimes I)(a|0\rangle \otimes |0\rangle + b|1\rangle \otimes |1\rangle) = |a|^2\langle 0|M|0\rangle + |b|^2\langle 1|M|1\rangle$$

This expression can be written in the form:

$$\langle M\rangle = Tr(M\rho)$$
$$\rho_1 = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|.$$

The operator ρ_1 is called the density operator of the first particle. It is self adjoint, positive, and has unit trace.

2.5 Pure and Mixed state

If the state of a system is a state in the Hilbert space then it is called a pure state otherwise it will be called a mixed state. If a state is pure then the corresponding density operator ρ satisfies $\rho^2 = \rho$. Because this is simple to check for $\rho = |\psi\rangle\langle\psi|$.

In general the density operator can be expressed as:

$\rho = \Sigma_i p_i|\psi_i\rangle\langle\psi_i|$. Where $0 \leq p_i \leq 1$. For mixed state there will be two or more terms. So we see that for a mixed state $\rho^2 \neq \rho$.

Chapter 3

Quantum Information

3.1 Introduction

Before starting discussion on Quantum Information theory let me quickly review classical information theory very briefly. The basic need of information theory is to encode some amount of news (information) by some means and to decode the encoded version to retrieve the news when required.

Whatever paradigm we choose this is the basic objective of studying Information theory. In classical information theory the fundamental unit of information is bit. We encode an amount of information by the classical bits which can be either 0 or 1 at a time but essentially not both.

To decode the information essential strategy of the receiver is to measure the bit which we can always do easily classically.

The receiver can also have some priori knowledge of the outcome. Say the receiver knows that the probability that 0 will occur is p_0 and the priori probability of 1 is p_1. In this scenario Shannon's remarkable theory gives precise mathematical quantification.

These features of classical information differs dramatically in case of quantum information. The fundamental unit of quantum information is a qubit. In a two level system with orthonormal basis $\{|0\rangle, |1\rangle\}$ the most general form of a qubit is given by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. The information is encoded in $\alpha\&\beta$. In contrast to the classical physics, quantum measurement theory places several limitation over the amount of information that we can extract. Most remarkable fact is that although most of the information is inaccessible but still it is useful. And this feature of quantum information makes a huge impact on cryptography and quantum computing.

Another great difference of quantum information with classical information is that like classical information quantum information can not be copied. The fact is guaranteed by one celebrated result of quantum mechanics namely "**No Cloning Theorem**".

The most remarkable difference between classical information and quantum information is due to **Quantum entanglement**. In the chapter 1 I have already described what is meant by quantum entanglement. If two classical system interacts once and then they are kept few light years apart. Can measurement over one of them effect the state of the other? certainly the answer is 'No'. But if we allow two quantum system to interact in such a way that quantum entanglement is estabilised between them, and then we separate them as many light years as we

wish, the measurement on any one of them changes the state of the other. The magical "**Quantum Entanglement**" has no classical counterpart. Quantum entanglement is the heart of quantum information. I will describe two of the major breakthrough results namely "**Quantum Teleportation**" and "**Quantum Dense Coding**" , which was made possible because of entanglement, in the upcoming section.

3.2 Quantum no cloning theorem:

Theorem: **Unknown quantum state can not be copied**

Proof: Let if possible there exists an unitary operator U which is a cloning operator.

$$U(|0\rangle, |\phi\rangle) = |0\rangle|0\rangle$$
$$U(|1\rangle, |\phi\rangle) = |1\rangle|1\rangle$$

In the above expressions $|\phi\rangle$ is the state on which the wanted state will is copied. Now let us apply the linear superposition principle on U. If U exists then the following must be true:

$$U(a|0\rangle + b|1\rangle, |\phi\rangle) = aU(|0\rangle, |\phi\rangle) + bU(|1\rangle, |\phi\rangle) = a|0\rangle|0\rangle + b|1\rangle|1\rangle$$

Which is in general not equal to $(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)$.
Hence universal quantum cloning machine does not exists.

3.3 Unitary Transformation

Before describing further result of quantum information let us first state some useful single qubit & two qubit quantum state transformations.

Single qubit quantum state transformations: {I , X , Y , Z , H }

$$\mathbf{I} : |0\rangle \rightarrow |0\rangle$$
$$\mathbf{I} : |1\rangle \rightarrow |1\rangle$$

$$\mathbf{X} : |0\rangle \rightarrow |1\rangle$$
$$\mathbf{X} : |1\rangle \rightarrow |0\rangle$$

$$\mathbf{Y} : |0\rangle \rightarrow |1\rangle$$
$$\mathbf{Y} : |1\rangle \rightarrow -|0\rangle$$

$$\mathbf{Z} : |0\rangle \rightarrow |0\rangle$$
$$\mathbf{Z} : |1\rangle \rightarrow -|1\rangle$$

$$\mathbf{H} : |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$\mathbf{H} : |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Double qubit quantum state transformations: Controlled Not (CNOT)

CNOT is a two qubit quantum gate where the first bit is taken as control bit. If the control bit is 1 then the gates flips the second bit and if the control bit is 0 the gate keeps the second bit as it is. In both the cases it keeps control bit unchanged.

Mathematically this transformation is given by:

$$C_{not} : |00\rangle \rightarrow |00\rangle$$
$$C_{not} : |01\rangle \rightarrow |01\rangle$$
$$C_{not} : |10\rangle \rightarrow |11\rangle$$
$$C_{not} : |11\rangle \rightarrow |10\rangle$$

3.4 Quantum Dense Coding

Say Alice receives two classical bits, encoding the number 0 to 3. If Alice wants to send this information to a distant separated Bob then he has to send 2 classical bit of information. Surprisingly enough Alice can do the same job by sending only one quantum bit (qubit) through quantum channel if he shares one maximally entangled pair with Bob.

Depending on the information Alice has to send Alice performs one of the transformation $\{I, X, Y, Z\}$ on his qubit of the entangled pair $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The resulting state is shown in the following table.

Value	Transformation	New state
0	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	X	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	Y	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$
3	Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

Alice then sends his qubit to the Bob.
Now Bob applies a controlled not gate to two qubits of entangled pair.

Initial state	Controlled not	First bit	Second bit
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\|1\rangle$

$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|1\rangle + \|0\rangle)$	$\|1\rangle$
$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$-\|0\rangle$

Bob can now measure his qubit without disturbing the quantum state. If the measurement returns $|0\rangle$ then the encoded version was either 0 or 3. And if the measurement returns $|1\rangle$ then it was either 1 or 2.

Then Bob apply Hadamard transform on the first qubit and measures it to distinguish between 0,3 and 1,2.

3.5 Quantum Teleportation

Alice and Bob are two distant separated party share some priori maximally entangled state say $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice has a qubit $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$ which he wants to send to Bob.

What Alice does is that he operates $|\chi\rangle$ with his half of the entangled pair i.e the state is given by:

$|\chi\rangle \otimes |\varphi\rangle = \frac{1}{\sqrt{2}}\{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\} = \frac{1}{2}\{\phi^+(\alpha|0\rangle + \beta|1\rangle) + \phi^-(\alpha|0\rangle - \beta|1\rangle) + \psi^+(\alpha|1\rangle + \beta|0\rangle) + \psi^-(\alpha|1\rangle - \beta|0\rangle)\}$.

Now Alice does bell state measurement on his two qubits and gets outcome either of $\phi^+, \phi^-, \psi^+, \psi^-$ with equal probability. Then Alice makes phone call to Bob to indicate his outcome i.e Alice use two classical bit of information to tell Bob either of the four outcomes .

Bob can now easily retrieve χ accurately by the following decoding process:

Alice's outcome	Bob's state	Decoding
ϕ^+	$\alpha\|0\rangle + \beta\|1\rangle$	I
ϕ^-	$\alpha\|0\rangle - \beta\|1\rangle$	Z
ψ^+	$\alpha\|1\rangle + \beta\|0\rangle$	X
ψ^+	$\alpha\|1\rangle - \beta\|0\rangle$	Y

After the decoding process Bob can successfully retrieve the original state χ to him.

Chapter 4

Quantum Cryptography

4.1 Introduction

Cryptography is the science of encryption and decryption of message. The basic need of cryptology is to encrypt some message using a key to prevent the message from unauthorized intruders. It should be guaranteed that if the intruder does not have the knowledge of the key then it should be absolutely difficult for him to retrieve the original message. Another objective of cryptology is that person having the complete knowledge of key it should be easy for him to decrypt the original message.

The real breakthrough in cryptography came when Rivest, Shamir, Adlemann discovered an amazingly simple scheme for encryption and decryption. Their scheme is popularly known as **RSA**. The basic principle that they used in **RSA**. is the one way property of the factorization problem i.e given a large number there was no polynomial algorithm to find it's prime factors. Otherwise if some body is provided some prime numbers and a large number then it is easy to check that whether the prime numbers are the factors of the large number (just multiply the factors and check).

Things were going right until Peter Shor's came with a polynomial time quantum algorithm for factoring large number in 1994. The algorithm shows if quantum computer can be made in reality then all the **RSA** based crypto system will be evacuated in a moment.

Another important question in classical crypto system is to establish some common key between two distant separated parties. The widely used scheme that classical crypto system use is mainly based on famous **Discrete Log Problem** The problem says that if some body is given α^a and α is known then there is no polynomial time algorithm exists so far to extract a. But it has been also shown that with the help of a quantum computer **D.L.P** can be easily broken.

So the question came how key distribution problem can be solved effectively such that even with the help of quantum computer intruders will not be able to retrieve the key.

Fortunately using the power of quantum mechanics Bennett and Brassard discovered a scheme for key distribution which is secure even against attack by quantum computer. Their scheme is popularly known as **BB84** protocol.

4.2 BB84 Protocol

Alice and Bob, two distant party want to establish a common secret key between them. The communication link between them are one classical communication channel and one quantum communication channel.

The basic steps of the protocol are as follows:

1:Alice sends Bob a sequence of photon randomly and independently chosen from 4 polarization, horizontal (ψ_z), vertical (ψ_{-z}), 45 degree (ψ_x), 135 degree (ψ_{-x}).

2:For each of the photon Bob randomly choose either of the rectilinear bases {horizontal , vertical (i.e in Z basis)} or diagonal bases {45 degree, 135 degree (i.e in X basis)}.

3:Bob records his chosen bases and the outcome of the measurement for each photon.

4:Bob then publicly announces his chosen bases but not the outcome of the measurement.

5:Alice, after receiving Bob's bases compare with his own bases and tells Bob in which of the cases they have used same bases.

6:In the cases they match in the bases they keep the result otherwise they discard the corresponding polarization bit.

7:Alice and Bob now can convert the polarization of the remaining photon into raw bits. They decide horizontal and 45 degree polarized photon as 0 and vertical and 135 degree polarized photon as 1.

Alice	$\|\Psi_z>$	$\|\Psi_{-z}>$	$\|\Psi_x>$	$\|\Psi_z>$	$\|\Psi_{-x}>$	$\|\Psi_x>$	$\|\Psi_{-z}>$
Bob's basis	X	Z	X	X	Z	X	Z
Bob's result	$\|\Psi_x>$	$\|\Psi_{-z}>$	$\|\Psi_x>$	$\|\Psi_{-x}>$	$\|\Psi_z>$	$\|\Psi_x>$	$\|\Psi_{-z}>$
Alice's message	×	√	√	×	×	√	√
Raw key		1	0			1	0

From the table one can see how the key is generated where Alice sends 7 qubits one by one and Bob performs spin measurement randomly in one of the bases.

Now let us consider what a possible eavesdropper can do. Eavesdropper can tap the quantum mechanical channel and can measure the photon in the randomly chosen bases. In the measuring process eve introduces large amount of error because on measurement the state of the photon. Now to detect the presence of eavesdropper Alice and Bob publicly compare some portion of the key. If the error rate exceeds a predefined limit then they detect the presence of eavesdropper and

discard the key string. They then repeat the whole process again to establish a new key.

Chapter 5

Quantum Computation

5.1 Introduction

In the current chapter I am going to describe how the power of quantum mechanics is going to have a huge impact on the classical complexity and computation theory.

The modern idea of computer science first came through Alan Turing. Turing first developed a model of computation that we know current day as programmable computer. Turing shows that if a task can be performed on a piece of hardware then it can be algorithmically computed in a Turing machine. Moreover Turing shows that there exists an Universal Turing Machine (**UTM**) which can in principle simulate any other Turing machine. Everything was going right until randomized algorithm arrived into picture. But the threat to Turing thesis because of randomized algorithm was easily removed by changing it to the following statement:

Any algorithmic process can be simulated efficiently using a probabilistic Turing machine

Another most important issue in computer science since it's birth is whether "$P = NP$?". This question has no answer till today. Intense research in the field of theoretical computer science has been able so far to reveal many facts about the structure of complexity theory.

It is known that P is a subset of NP but it is not known whether the subset is a proper one? It is known that the hardest class of problem in NP is the NP *Complete* problem. It is also known that NP *Complete* problems can be polynomially reduced from one to another. So finding a polynomial time algorithm for one of them is simply mean that $P = NP$. Another very interesting complexity class is NP *Intermediate*(NPI) class. That is there exists some problem for which no polynomial time algorithm is known till today and also this problems are not known to be in NP Complete.

$$NPI = NP - (NPC \cup P)$$

In the classical computation theory NPI problems has no effective solution apparently. Example of NPI problems are factorization, graph isomorphism, quadratic reciprocity etc. It is also not known that whether

These are some of the key issues of computer science. In the next sections I will try to describe few quantum algorithm and associated facts which have major impact in these issues.

Quantum Algorithm

5.2 Deutsch's Problem

Suppose a single variable boolean function $f : \{0,1\} \rightarrow \{0,1\}$ is given. Now it is asked to check whether the function is balanced i.e $\{f(0) \neq f(1)\}$ or constant i.e $\{f(0) = f(1)\}$. Suppose the function needs t second for computation once. So it is clear that classically on a single processor to answer the above query it needs 2t second. Can we do it within t second? Fortunately we use the power of quantum mechanics to solve the problem effectively.

Let us consider a two qubit transformation U_f acting as follows:

$$U_f : \{|x\rangle, |y\rangle\} \rightarrow \{|x\rangle, |y \oplus f(x)\}$$

$$U_f\{|x\rangle, \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} = \tfrac{1}{\sqrt{2}}U_f\{|x\rangle, |0\rangle\} - \tfrac{1}{\sqrt{2}}U_f\{|x\rangle, |0\rangle\} = \tfrac{1}{\sqrt{2}}|x\rangle(-1)^f(x)(|0\rangle - |1\rangle)$$

Hence we have the following:

$$U_f\{\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} = \tfrac{1}{\sqrt{2}}[|0\rangle(-1)^f(0) + |1\rangle(-1)^f(1)] \quad \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Now if the first particle is measured in the $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ basis then if the original function is constant then we will be always getting $|+\rangle$ and if the function is balanced then we will always get $|-\rangle$.

Thus on a single quantum computer the total solution can be found in t seconds as the separate computation of f need not to be done for 0 and 1.

Let me now consider the generalization of the **Deutsch** problem popularly known as **Deutsch Josza Algorithm**

5.3 Deutsch Josza Algorithm

Deutsch Josza Problem:

In a n variable boolean function , the promise is given that the function is either constant or balanced. Now can we decide it in polynomial time whether the function is balanced or constant.

Obviously the problem is of exponential complexity classically. Amazingly this problem can be solved polynomially using Quantum Algorithm.

Let us take a n bit quantum register and apply n Hadamard gates in parallel. We define the parallel Hadamard transform $H^{(n)}$ as:

$$H^{(n)} = H \otimes H \otimes ..... \otimes H$$

The n qubit state is transformed to :

$$H^{(n)} : |x\rangle \rightarrow \prod_{i=1}^{n}(\frac{1}{2}\sum_{y_i=\{0,1\}}(-1)^{x_i y_i}|y_i\rangle) = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x.y}|y\rangle$$

Where $x.y$ means bit by bit multiplication(mod 2) of two n bit binary string and then mod 2 addition.

Applying $H^{(n)}$ on the initial state $(|0\rangle)^n|1\rangle$ transforms it into $\frac{1}{2^n}(\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f}(x)(-1)^{x.y}|y\rangle)\frac{1}{\sqrt{(2)}}(|0\rangle - |1\rangle)$.

Now if we observe the term

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x.y}$$

If f is a constant function the sum is $(-1)^{f(x)}\delta_{y,0}$; which vanishes unless y=0. Hence if we measure n bit register we obtain the result $|y=0\rangle$ with probability 1.

But if the function is balanced then the sum is zero. Hence the probability of obtaining the measurement outcome $|y=0\rangle$ is zero.

Hence we can easily decide the promise of the function in polynomial time , in fact the time complexity is a constant and the space complexity is $O(n)$.

5.4 Shor's Factorization Algorithm

Problem: Given an integer N which has two prime factor p , q such that N=pq.

So far this problem has no known polynomial time classical algorithm but it has been shown by Shor's in 1993 that the problem can be solved efficiently using quantum algorithm.

Step 1: It's a number theoretic fact that the problem of finding prime factors of N is equivalent in finding the period of the function

$$f_{a,N}(x) = a^x mod N$$

Where a is a randomly chosen integer less than N and such that $g.c.d(a,N) = 1$.

Step 2: If the period r is such that r is even and $a^{\frac{r}{2}} \neq -1(mod N)$ then it is possible to find the factor of f.

Step 3: It's a mathematical fact, the probability that r satisfies the condition of **Step 2** is greater than $\frac{1}{2}$.

Step 4: Once r satisfies the above mentioned condition the the $g.c.d(a^{\frac{r}{2}}+1, N)$ and $g.c.d(a^{\frac{r}{2}}-1, N)$ give the two factors of N.

Step 5: All the steps except finding r can be done in polynomial time in classical computer. We can now use quantum algorithm to find r in polynomial time. Let L bits are required to store N where $L \simeq log_2(N)$. The quantum algorithm runs in time polynomial in L.

Let me now briefly explain the basic strategy of Shor's algorithm. Let us take two L bit register. Both register is loaded with initial value 0. So the total state is $|0\rangle|0\rangle$. Let us now apply Hadamard transform on the first register to make the state $\frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}|x\rangle|0\rangle$. Now let us apply $U_{f_{a,N}}$ to this state, to obtain the following state.

$$\frac{1}{2^L}\sum_{x=0}^{2^{2L}-1}|x\rangle|f_{a,N}(x)\rangle$$

At this stage all the possible values of $f_{a,N}$ are encoded in the state of the second register, but they are not all accessible at the same time. Also we are interested only on the periodicity of the function. If it was possible that we could dictate the outcome of the second register, then repeating the process a few times we can get easily the value of the period.

But unfortunately quantum mechanics does not allow the dictation over second register.

Now let us use the main strategy used by Shor to extract the period. The tool Shor used is Quantum version of Discrete Fourier transform popularly known as quantum fourier transform.

What ever be the outcome of the second register the outcome of the first register is of the form $|\psi\rangle = \xi\sum_{j=0}^{\lfloor 2^{2L}/r\rfloor}|jr+l\rangle$ where r is the period of $f_{a,N}(x)$, l is an offset value and ξ is a normalization factor.

Now let us apply D.F.T on the value of the first register.

$$U_{DFT}|x\rangle = \frac{1}{2^L}\sum_{y}^{2^{2L}-1} exp(2\pi i\frac{xy}{2^{2L}}|y\rangle$$

The advantage of applying Q.F.T is to eliminate the offset l and make it is a phase factor. The output of the first register can be written as:

$$|\phi_{out}\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} exp(2\pi ilj/r)|j2^{2L}/r\rangle$$

Now on measuring the first register we can easily find out the value of r as L is known.

Complexity

The computation of the function $f_{a,N}$ can be done in $O(L^3)$. The time complexity of the computation of D.F.T is $O(Llog(L))$. Hence total algorithm runs in polynomial time in L.

5.5 Discussion

I have here mentioned three quantum algorithm. Beside those there also exists some incredible quantum algorithm, one among them is due to **Grover**. In his algorithm Grover has shown that the searching in a unstructured database can be done quantum mechanically in time $O(\sqrt{(N)})$ where as it's classical counterpart needs $O(N)$.

We have seen that quantum algorithm can solve at least one NPI problem. But the main question regarding the solution of NP Complete problems still remains as open challenge. Although there is some weak indication that even quantum computer can not solve these problem efficiently.

But some researcher still believe the challenge still alive for future.

Chapter 6

Sharing of secret quantum information

6.1 Our Goal

In a distributed computer network suppose Alice wants to distribute a secret information to some distant parties B_i's. B_i's can operate locally on his part of information and can communicate between them using classical communication. Alice needs guarantee that any of the B_i's should not be able to reconstruct the total secret information to him using LOCC with others. In case of classical computer network this problem has apparently no solution. Here we discuss how this problem can be tackled with the help of quantum mechanics in a distributed quantum network.

6.2 Introduction:

In a distributed computer network say machine A has a secret information (Key) which he wants to keep distributed in some distant machine $B_1, B_2.....,B_n$. Moreover the distribution should be such that if A or some other person authorized by A wants to get back the information, he should be able to do that. Now all the B_i's can use their part of total information for some local use. But it should be confirmed that none of them should get the total information of the key when B_i are allowed to operate only locally and can communicate classically within them. This is a reasonable assumption in case of distributed network. This problem has apparently no solution in case of classical computer network. Because individually each of the B_i's can read their part and then make phone call to each other to reconstruct the total information to any of them. Can we solve the problem using quantum network?

Fortunately we can, if we replace the classical links of the network by proper entangled quantum channels, classical machines by quantum machines.

First question that arises in case of security issue is that can any B_i recreate the the total information about the key without having any help from others. Essentially he can not. Because if the information (pure state) is distributed through proper quantum entangled channel then the individual state of any B_i is a mixed state. And we know there exists no unitary operation which can transform mixed state to pure state.

The next immediate question is that can they do it by taking only distant help from others via classical communication. Essentially that is dependent on how good the channel is. In a recent work T.Brune has shown a large class of pure state multiparty channel, which he called web state, are useful for the distribution and

concentration of quantum information in a distributed quantum network. But this states are not useful for our purpose. Because if information is distributed by these states then any of the B_i can reconstruct the information to him using only LOCC with others.

In this current work we have investigated a class of pure multiparty state that can be used for our purpose. We mainly discussed the case of a 4 party network. We hope that the result can be extended to a multiparty network.

Pure state are generally costly to prepare and it is also difficult to prevent them from natural decoherence. So one solution is to use proper mixed entangled state. In case of a 4 party network if we distribute the information by Smolin's 4 party unlockable bound entangled state then it is impossible for the B_i's to concentrate the total information to one of them using only LOCC. We have generalized this idea where we have a class of mixed channel for general multiparty network from which it is impossible for B_i's to reconstruct the whole information to one of them using only LOCC.

In **section 2** we have discussed the structure of the entangled pure channel that can be used for distribution and concentration of quantum information in a general multiparty network and the corresponding protocol. In **section 3** we have discussed about the level of secrecy that we can achieve with this channels. And finally we have made a short discussion of overall work and left few open question in the **section 4**.

6.3 Protocol for distribution and concentration of quantum information:

Say we have (N+1) parties where N is odd. Let Alice, one among them, has a secret information in the form of a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\alpha|^2 + |\beta|^2 = 1$.

The channel they share is given by $|\chi_{1,2,\ldots N+1}\rangle = |0\rangle \otimes \sum_i a_i S_i + |1\rangle \otimes \sum_i a_i \bar{S}_i$. Where $\bar{S}$ is the bit by bit complement of S. The state is properly normalized, i.e $\sum_i a_i * a_i = \frac{1}{2}$. Where $\bar{a}$ is the complex conjugate of a. In each S_i the no of 0's is odd.

The protocol has two phase. The first one we call Distribution phase and the next one we call Concentration phase. In the Distribution phase Alice perform bell state measurement on his two qubits $|\psi\rangle$ and the first qubit of $|\chi_{1,2,\ldots N+1}\rangle$. Depending on his outcome $\phi^+, \phi^-, \psi^+, \psi^-$ Alice makes phone call to other N parties to perform unitary operation $I, \sigma_x, \sigma_y, \sigma_z$ respectively on their qubit i.e parties 2,3,4,....,N will individually apply I for measurement result ϕ^+, σ_z for ϕ^-, σ_x for ψ^+, σ_y for ψ^-. The state of the N parties become $\alpha \sum_i a_i S_i + \beta \sum_i a_i \bar{S}_i$. Distribution phase is over.

Now let Claire who is authorized to Alice wants to concentrate the information to him. If claire shares a properly normalized state $|\chi_{1,2,\ldots N+1}\rangle = (\sum_i b_i S_i) \otimes |0\rangle + (\sum_i b_i \bar{S}_i) \otimes |1\rangle$ with the parties among whom the original state was distributed.

Let the parties among whom the state is distributed are $B_1, B_2, ..., B_n$.

In the concentration phase each of the B_i's performs bell measurement on their two qubits. They then inform Claire their measurement results by phone call. Claire then perform unitary operation on his qubit given by $\prod_{i=1} \otimes O_i$. Where O_i's are either I if the outcome of Bi is ϕ^+ or σ_x if the outcome is ϕ^- or σ_y if the outcome is ψ^+ and otherwise σ_z. Claire thus can recover the state $|\psi\rangle$ exactly. Concentration phase is over.

In the protocol we can also use an eqivalent channel given by $|\chi_{1,2,....N+1}\rangle = |0\rangle \otimes \sum_i a_i S_i + |1\rangle \otimes \sum_i a_i' \bar{S}_i$. Where $a_i = a_i' \exp(i\theta_i)$.

6.4 Proof of security

Let us first discuss the case of pure state channel in a 1:3:1 system i.e $A : \{B_1, B_2, B_3\} : C$. The shared channel is given by:

$$|\chi_{A,B_1,B_2,B_3}\rangle = |0\rangle \otimes (a_1|000\rangle + a_2|011\rangle + a_3|101\rangle + a_4|110\rangle) +$$
$$|1\rangle \otimes (a_1|111\rangle + a_2|100\rangle + a_3|010\rangle + a_4|001\rangle).$$

Now we note that this state can be written in any $\{A, B_i\} : \{B_j, B_k\}$ cut as a linear combination of $\phi^+ \otimes \phi^+, \phi^- \otimes \phi^-, \psi^+ \otimes \psi^+, \psi^- \otimes \phi^-$. As for example $|\chi_{A,B_1,B_2,B_3}\rangle = (a_1 + a_2)\phi^+ \otimes \phi^+ + (a_1 - a_2)\phi^- \otimes \phi^- + (a_3 + a_4)\psi^+ \otimes \psi^+ + (a_3 - a_4)\psi^- \otimes \phi^-$.....(i).

Now if information can be reconstructed in any of the Bi's using LOCC that equivalently mean that Bi's can distill 1 ebit between A and any of them using LOCC only.

Now we investigate different possible strategy by Bi's to distill 1 ebit between A and any of them.

case I:

Let us consider a possible decomposition of $|\chi_{A,B_1,B_2,B_3}\rangle$ as:

$|\chi_{A,B_1,B_2,B_3}\rangle = \lambda\psi_{max1} \otimes \psi_{ent} + \mu\psi_{max2} \otimes \psi_{pr1} + \eta\psi_{max3} \otimes \psi_{pr2}$.....(2)

Where $\psi_{max1}, \psi_{max2}, \psi_{max3}$ are three maximally entangled state between A and B_1 and $\psi_{ent}, \psi_{pr1}, \psi_{pr2}$ are three pairwise orthogonal states between B_2 and B_3 where ψ_{ent} is a entangled state and ψ_{pr1}, ψ_{pr2} are two product state. Now if B_2 and B_3 can discriminate using LOCC only these three orthogonal states then they can distill 1 ebit of entanglement between A and B_1. Now if we trace out A and B_1 in the representation of $|\chi_{A,B_1,B_2,B_3}\rangle$ then the state of other two parties is given by $\rho_{A,B1} = |a_1 + a_2|^2 P[\psi^+] + |a_1 - a_2|^2 P[\psi^-] + |a_3 + a_4|^2 P[\phi^+] + |a_3 - a_4|^2 P[\phi^-]$. We note that the rank of $\rho_{A,B_1} \leq 4$. Now in representation (2) if we trace out B_2 , B_3 the state between A and B_1 is given by $\rho 1_{A,B_1} = |\lambda|^2 P[\psi_{max1}] + |\mu|^2 P[\psi_{max2}] + |\eta|^2 P[\psi_{max3}]$. The rank of $\rho 1 \leq 3$. So in general $\rho_{A,B_1} \& \rho 1_{A,B_1}$ are not equal. So this decomposition is not allowed, in general.

case II:

Let if possible $|\chi_{A,B_1,B_2,B_3}\rangle = \sum_1^4 \lambda_i \psi_{max_i} \otimes \psi_{pr_i}$.....(3). Where ψ_{max_i}'s are pairwise orthogonal and ψ_{pr_i} are pairwise orthogonal. Now if we trace out the first two parties from (3) the state between other two party B_1 and B_2 is a separable state where as from (1) we know after trace out of A and B_1 the state between B_2 and B_3 is a entangled state. So in general this decomposition is not allowed.

case III: If it is possible that $|\chi_{A,B_1,B_2,B_3}\rangle = \sum_1^4 \lambda_i \psi_{max_i} \otimes \psi_{pr_i}$.....(3) where ψ_{max_i}'s are in general not pairwise orthogonal the argument of **case II** generally does not hold.

It is in general looking difficult to discard the situation although we can show some convincing argument regarding the impossibility of decomposition of the state $|\chi_{A,B_1,B_2,B_3}\rangle$ in the above mentioned from.

We know that 1-ebit between two party can be distilled out from a three party $|GHZ\rangle$ state effectively using only LOCC. And so far we don't have effective general procedure to distill 1-ebit from a three party $|W\rangle$ state. So it might be interesting to see if the state $|\chi_{A,B_1,B_2,B_3}\rangle$ can be transformed into a 3 party $|GHZ\rangle$ in general.

Let us check if 3 party $|GHZ\rangle$ can be distilled between say A, B_1, B_2. The state $|\chi_{A,B_1,B_2,B_3}\rangle$ can be written as $|\chi_{A,B_1,B_2,B_3}\rangle = (a_1|000\rangle + a_4|011\rangle + a_2|110\rangle + a_3|101\rangle)\otimes|0\rangle + (a_2|001\rangle + a_3|010\rangle + a_1|111\rangle + a_4|100\rangle)\otimes|1\rangle$. Now if B_3 can measure his qubit in preparation basis i.e $\{|0\rangle, |1\rangle\}$ basis the state between A, B_1, B_2 is either $(a_1|000\rangle + a_4|011\rangle + a_2|110\rangle + a_3|101\rangle)$ or $(a_2|001\rangle + a_3|010\rangle + a_1|111\rangle + a_4|100\rangle)$. Now A can measure his qubit in $\{(x|0'\rangle + y|1'\rangle), (y^*|0'\rangle - x^*|1'\rangle)\}$ basis. So the joint state of B_1, B_2 will be either $\{x(a_1|00\rangle + a_4|11\rangle) + y^*(a_2|10\rangle + a_3|01\rangle)\}$ or $\{y(a_1|00\rangle + a_4|11\rangle) - x^*(a_2|10\rangle + a_3|01\rangle)\}$. If we consider the first state then $\rho_{B1} = P[xa_1|0\rangle + y^*a_2|1\rangle] + P[xa_4|1\rangle + y^*a_3|0\rangle]$. Now if 3 party GHZ state has to be distilled between A, B_1, B_2 then it must be satisfied $(xa_1/y^*a_3) = (y^*a_2/xa_4)\&(ya_1/x^*a_3) = (x^*a_2/ya_4)$. From this two relation we get $|a_2a_3|^2 = |a_1a_4|^2$ which is in general not satisfied for any choice of a_i's.

Otherwise if B_3 measures his qubit in $\{(x_1|0''\rangle + y_1|1''\rangle)\ (y_1^*|0''\rangle - x_1^*|1''\rangle)\}$ basis then the joint state of A, B_1, B_2 either $|0\rangle\otimes(xa_1|00\rangle + xa_4|11\rangle + y^*a_2|01\rangle + y^*a_3|10\rangle) + |1\rangle\otimes(xa_2|10\rangle + xa_3|01\rangle + y^*a_1|11\rangle + y^*a_4|00\rangle)$ or $|0\rangle\otimes(ya_1|00\rangle + ya_4|11\rangle - x^*a_2|01\rangle - x^*a_3|10\rangle) + |1\rangle\otimes(ya_2|10\rangle + ya_3|01\rangle - x^*a_1|11\rangle - x^*a_4|00\rangle)$. If the state is to be a GHZ state between A, B_1, B_2 then from the first state we have $xy(Re(a_1a_4^*)) = -x^*y^*(Re(a_3a_2^*))$ which implies $|Re(a_3a_2^*)/Re(a_1a_4^*)| = 1$. Which is not possible in general.

Now we look forward to implement the shared channel by mixed state. It is easy to check that distribution and concentration of information can be done

using mixed state of the form $\chi_{mixed_{1,2,....N+1}} = \sum_i P[|0\rangle \otimes S_i + |1\rangle \otimes S_i|$. Where S is the bit by bit complement of S and P[ ] is the projector operator . The state is properly normalized, i,e $\sum_i a_i * \bar{a}_i = \frac{1}{2}$. Where $\bar{a}$ is the complex conjugate of a. In each S_i the no of 0's is odd.

We claim the following lemma:

The state given by $\chi_{mixed_{1,2,....N+1}}$ is a PPT state in any (1,i):(2,3,...,i-1,i+1,...N+1) cut for all i.

Proof:

We observe in the mixed state the projector $P[|0\rangle \otimes S_i + |1\rangle \otimes \bar{S}_i]$ is present iff S contains odd no of 0's. Now if we take the indicated cut then the form of a projector will be either $P[|00\rangle \otimes S1_i + |11\rangle \otimes \bar{S}1_i]$ where $S1_i$ contains even no of 0's or $P[|01\rangle \otimes S2_i + |10\rangle \otimes \bar{S}2_i]$ where $S2_i$ contains odd no of 0's. Now for the first form we note that the projector $P[|0 \otimes 0\bar{S}1_i + |1 \otimes 1S1_i]$ is always present because this form falls under the form of projector we have chosen for the mixed state. Similar argument holds for the second form of the projector. And the original mixed state is invariant under all such 2:(N-2) cut because we have exhausted all such projector in the preparation of the original mixed state. Hence clearly this state is a PPT in the above mentioned cut and hence not distillable in the above cut.

From the above mentioned lemma we conclude that 1 ebit entanglement can not be distilled between first party and one of rest N-1 parties by other N-2 party using only LOCC. Hence if the 1st party say Alice distribute the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ among the rest N parties then the complete information of $|\psi\rangle$ can not be concentrated to any of the intermediate party using only LOCC with others.

6.5 Discussion:

In the current work effort has been made to develop a protocol for distribution of secured information in a distributed environment. We have first discussed the possible structure of pure entangled state used as channel to achieve the secrecy. The problem has been discussed for a 4 party network. We have given some convincing argument about the usefulness of pure state for the purpose although the rigorous proof of secrecy remains open. We hope the result will motivate our reader to prove formally the possibility of using pure state as a secret channel in the distributed environment. Result can be also extended to a N party general distributed network and will be investigated elsewhere.

We have solved the problem completely using mixed state channel for general multiparty distributed environment. The N+1 party channel that we have used, is a PPT in (2:N-2) cut and hence 1 ebit can not be distilled between Alice and

any B_i using LOCC.

We have presented here a class of pure and mixed state useful as secret channel. The question about the most general form of the channel remains open. The problem suggest that a more insight into characterization of entanglement in a multiparty system might be useful in generalization of the problem.

Chapter 7

Bibliography

For Further reading:

[1] *Quantum computation and Quantum information* by Michael A. Nielsen and Isacc L. chuang.

[2] *Introduction to quantum computation and information* edited by T Spliller, H.-K. Lo and S.Popescu.

[3] *Quantum computing* by J.Gruska.

[4] John Preskill's lecture notes in quantum information and quantum computation available at http://www.theory.caltech.edu/people/preskill/ph229.

[5] Umesh Vazirani's lecture notes in quantum computation available at http://www.cs.berkeley.edu/ vazirani.

[6] Many useful papers are available regularly at http://xxx.lanl.gov/archive/quant-ph.

[7] R.P. Feynman, Int. J. Theor. Phys. 21,467 (1982).

For our problem

[8] Todd A. Brun, quant-ph/0102046

[9] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K Wotters, Phys. Rev. Lett. 70,1895 (1993).

[10] C.H. Bennett and S. Wiesner, Phys. Rev. Lett.69,2881(1992)

[11] J.A. Smolin, quant-ph/0001001

[12] A.Cabello, quant-ph/0203119

[13] W.K. Wootters and W.H. Zurek, *Nature* 299, 802 (1982)

[14] C.H. Bennett, F.Bessette, G. Brassard, L. Salvail and J. Smolin, *J. Cryptology* 5,3 (1992)