1
Preliminaries and literature survey

If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.

-John von Neumann

1.1 INTRODUCTION

Quantum information and computation has emerged as an interdisciplinary research area at the interface of diverse academic disciplines such as computer science and engineering, mathematics and physics. It deals with the study of computational and information processing tasks using the fundamental laws of quantum physics to discover many interesting and exciting capabilities for communication, manipulation and transmission of information. In general, the area analyses preparation, distribution, and control of quantum systems for efficient communication and computation.

With the failure of classical mechanics to explain phenomena such as black-body radiation, photoelectric effect, emission spectra of atoms, and structure of atoms- the first three decades of twentieth century witnessed a period of turmoil, excitement, and creative intellect to accept the need to replace the existent theories and to introduce a new theory for a complete mathematical description of the physical world. Subsequently, Erwin Schrödinger and Werner Heisenberg proposed a mathematical framework of the new quantum theory independently using wave mechanics and matrix mechanics, respectively. This novel theoretical paradigm is based on an algebraic formulation consisting of postulates and principles for accurate but probabilistic description of physical systems. The fact that classical mechanics had to be replaced by quantum mechanics for describing the behaviour of elementary particles at the atomic level naturally took many years to gain acceptance. Based on the assumptions of local realism, Einstein, Podolsky and Rosen in 1935 (EPR), raised the question of completeness of quantum mechanics as a complete physical theory- the EPR paradox paved the way for several open-ended discussions, studies and debates to understand and analyse quantum correlations, described by quantum mechanics as against the description provided by local hidden variable (LHV) theories. In the last three decades, the progress in quantum information and computation clearly suggests that quantum computers based on quantum mechanical laws may solve problems that cannot be solved efficiently on classical computers. The basis for efficient performance of a quantum computer in comparison to a classical computer is laid down in terms of the superposition of quantum states- the fundamental concept in quantum mechanics. Similar to bit which is a fundamental unit of classical computation, qubit or a quantum bit is considered as a fundamental unit of quantum computation. The state of a qubit is fundamentally different from the state of a bit in a sense that a qubit can be represented in any arbitrary linear superposition of two orthonormal basis states. To be precise, a quantum bit can be described using a mathematical framework, know as its state, in a two-dimensional complex vector space- the number of complex numbers required to characterize the state of a quantum system increases exponentially with the increase in the size of the system. Consequently, a classical computer also requires an exponential number of bits of memory to

store and manipulate a quantum state. On the other hand, due to the superposition principle and linearity which is fundamental to the quantum mechanical framework, a quantum computer can store and manipulate all the complex numbers at once. This phenomenon, also known as quantum parallelism, allows quantum computers to efficiently simulate general quantum systems, which are otherwise cannot be efficiently simulated on classical computers. In early 1980, Richard Feynman observed that efficient simulation of certain quantum mechanical effects on classical computer is too difficult; it prompted researchers and experimentalists to visualize computation based on quantum mechanical laws, and hence quantum computers. For example, the advantages offered by Shor's and Grover's algorithm over well known classical algorithms are already established.

From information theoretic perspective, in 1948, Shannon defined the mathematical theory of information to lay the foundations of modern information theory and communication. Shannon's noiseless and noisy channel coding theorems are the two fundamental results of classical information theory. A quantum analogue of noiseless channel coding theorem was proposed by Ben Schumacher which quantifies the resources required to do quantum data compression. Although quantum analogue of Shannon's noisy channel coding is not yet formulated, the concept of quantum error correction is developed to protect information and computation in presence of noise. Another important aspect of quantum information and communication is security, i.e., to protect information from malicious third party intervention. Quantum mechanics offers a solution to eavesdropping through quantum cryptography- the basic premise is to encode the information in a superposition state so that any malicious attempt to intervene can be identified using the very concept of collapse of a wave function. The security of most of the cryptographic protocols, e.g., RSA cryptosystems and Diffie-Hellman are dependent on the computationally hard problems of integer factorization and discrete logarithm. The security of classical cryptographic systems, however, is challenged by the introduction of quantum algorithms such as Shor's algorithm which can be used to break classical cryptosystems, e.g., RSA. Such applications provide support to the use the theoretical foundations of quantum information and computation in experimental prototypes of quantum cryptographic algorithms to be used in real world applications.

In general, at the center of all communication protocols is quantum entanglement which is believed to be responsible for the efficiency and speed-up of quantum computation and information processing in comparison to classical computation and information processing. In fact, there are separable systems exhibiting quantum correlations- as captured by a measure known as quantum discord- which can be used for efficient quantum information and computation. Essentially, nonlocal or quantum correlations existing between the particles are giving an edge to quantum computation over classical computation. Characterization and analysis of nonlocal correlations in bipartite and multipartite systems, therefore, is extremely important to understand the nature and efficiency of entangled systems for quantum information and computation. Since, the complexity in quantum systems increases enormously with the size of the system, the analysis of multiqubit nonlocality is much more intricate in comparison to the analysis of nonlocality in two-qubit systems. The complexity of the problem increases even further once we consider the distribution of entanglement under real conditions, i.e., by considering the effect of decoherence on nonlocal correlations. In principle, the efficiency of a quantum system decreases when subjected to a noise due to the degradation of entanglement and nonlocal correlations. Therefore, it is important to study models to protect nonlocal correlations for an improved efficiency under different noisy channels. Such analysis is not only important to understand the fundamental aspects of entanglement and nonlocality but also helps to design large-scale, efficient information and communication protocols.

For bipartite and multiqubit systems, genuine nonlocality is characterized by the violation of the Bell or Bell-type inequalities. There are instances where the Bell inequality in bipartite mixed entangled systems or Bell-type inequalities even in multiqubit entangled pure systems fails

to identify nonlocal correlations in underlying states. Hence, there is a need for a more generic approach to identify nonlocality in bipartite and multiqubit entangled systems.

In following sections, we first describe basic terminologies and fundamental concepts in quantum information and computation, followed by a brief description regarding scope of this Thesis.

1.2 BASIC CONCEPTS AND TERMINOLOGY

In this section, we will review some basic concepts and terminology related to quantum computing and quantum information processing such as qubits, quantum gates, entanglement, nonlocality, quantum teleportation and quantum dense coding etc.

1.2.1 Qubits

The fundamental units for processing and recording the data or information in classical computation are bits . A classical bit has two distinguishable states 0 and 1, separated by a high energy barrier to ensure that there is no spontaneous transition between these states. One can easily perform a measurement on the state of a bit to deterministically find whether the system is in the state 0 or in the state 1.

Analogues to the fundamental unit of classical computation, a quantum bit or a qubit is a fundamental unit for quantum information and computation [Rieffel and Polak, 2000; Spiller *et al.*, 2005; Nielsen and Chuang, 2010]. The state of a qubit can be described as a mathematical object to develop a general theory of quantum computation. Similar to a bit, a qubit can also be found in two possible states, i.e., $|0\rangle$ and $|1\rangle$. The difference between bits and qubits lies in the fact that a qubit can also be represented as a linear superposition of $|0\rangle$ and $|1\rangle$, resulting in a superposition state represented by $|\psi\rangle = a|0\rangle + b|1\rangle$ where 'a' and 'b' are two complex numbers. There are infinitely many possible representations for $|\psi\rangle$, subject to the normalization condition $|a|^2 + |b|^2 = 1$. Therefore, the state of a qubit can be represented as a vector in a two-dimensional complex vector space where the states $|0\rangle$ and $|1\rangle$ are considered as the orthogonal basis states for the two-dimensional complex vector space, also known as computational basis states. For algebraic convenience, the state $|0\rangle$ can be expressed as a column vector $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and the state $|1\rangle$ can be expressed as a column vector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Clearly, the states satisfy the orthonormality relations, i.e., $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$. Hence, in terms of a column vector, an arbitrary state of a qubit can be represented as $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$. If one tries to measure the state $|\psi\rangle$ of a qubit in a computational basis, then the possible measurement outcomes are either $|0\rangle$ with probability $|a|^2$ or $|1\rangle$ with probability $|b|^2$. Therefore, a measurement to determine the state of a qubit leads to the collapse of a wave function- values of 'a' and 'b' can be ascertained only if one performs infinite number of measurements on infinite number of identically prepared systems.

The atomic model can be used to explain the physical realization of a qubit. For example, one can represent a two-level system by labelling state $|0\rangle$ as the ground state and labelling state $|1\rangle$ as the excited state. A transition of an electron will take place from state $|0\rangle$ to $|1\rangle$ if the ensemble of atoms is irradiated with a light of appropriate energy for an appropriate length of time. The electron can also exist between the state $|0\rangle$ and the state $|1\rangle$ by reducing the time of irradiating the light. Figure 1.1 pictorially represents the existence of a qubit through ground and excited states of an electron in an atom. Equivalently, for geometric representations, an arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$ of a qubit can also be expresses as $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\delta}\sin\left(\frac{\theta}{2}\right)|1\rangle$, where θ and

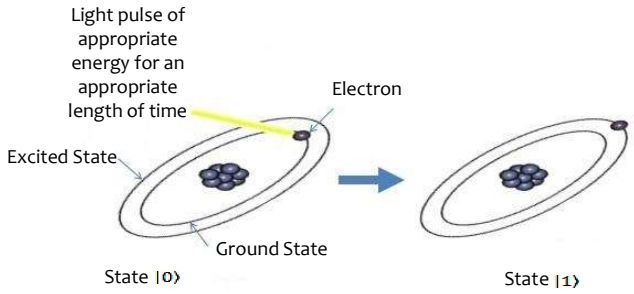

Figure 1.1 : Representation of a qubit using an atomic model.

δ are points in a unit three-dimensional sphere known as Bloch sphere [Jakóbczyk and Siennicki, 2001; Nielsen and Chuang, 2010].

1.2.2 Multiqubit States

Similar to the measurement outcomes of two fair coins, two bits can also exist in four different possible states, namely 00, 01, 10, and 11. Analogously, one of the possible set of orthonormal basis states for a two-qubit system are characterized as $|00\rangle$, $|01\rangle$,$|10\rangle$, and $|11\rangle$. In addition, a two-qubit state can also exist in an arbitrary linear superposition of these four states , i.e., $|\psi\rangle = [a_{00}|00\rangle_{12} + a_{01}|01\rangle_{12} + a_{10}|10\rangle_{12} + a_{11}|11\rangle_{12}]$, subject to the normalization $\sum_{t\varepsilon\{0,1\}}^{2} |a_t|^2 = 1$. A measurement on the state of two qubits in the computational basis $|t\rangle$ will always result in $t = (00, 01, 10 \text{ or } 11)$ with the respective probabilities as $|a_t|^2$. Clearly, a two-bit classical register can store only one out of the four numbers, 00, 01, 10, and 11 at a given moment. Whereas, a two-qubit quantum register can store all the four numbers $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ in a quantum superposition at any given point. Therefore, adding qubits to the register in a superposition state increases its storage capacity exponentially. For example, if we are dealing with $N-$qubit systems, then all possible 2^N basis states can be stored at once, which means that one can perform the same measurement operation on all the basis states stored in a coherent superposition of N qubits in only one single computation. This is known as quantum parallelism, resulting in the essential time and memory advantage in comparison to classical computing [Rieffel and Polak, 2000; Spiller *et al.*, 2005; Nielsen and Chuang, 2010].

1.2.3 Quantum Gates

A classical computer is built from electrical circuits consisting of wires and logical gates. In classical computation bits represent information which is manipulated from one form to another using logic gates while wires are used to carry data or information around the circuit. An example of a single-bit logical gate is a NOT gate that turns 0 to 1 and 1 to 0. In general, two-bit logical gates such as OR, AND, NOR and NAND use two input bits for a computation and give only one output bit as a result of that computation. Such gates are therefore termed as irreversible gates-the irreversibility is interpreted in terms of dissipating energy as the computation is performed. This should not be surprising as deleting information requires work to be performed and hence energy is wasted in terms of heat. Alternately, a logical gate is called irreversible, if one cannot determine the input from the given set of output for the gate.

Similar to a classical computer, quantum computer circuits are also built from wires and elementary quantum gates- following the fundamental laws of quantum mechanics- for carrying and manipulating the quantum information [Barenco *et al.*, 1995a,b; Zhou *et al.*, 2000; Hammerer

et al., 2002; Brylinski and Brylinski, 2002]. Algebraically, quantum gates can be represented as operators acting on a quantum state to transform it from one form to another. In fact, the matrix form is found to be a very convenient way for representing quantum gates, e.g., all single-qubit gates can be represented by 2×2 matrices. However, quantum gates can be represented by an operator if and only if it is a unitary operator. Clearly, the inverse of a unitary operator is also a unitary operator, and hence quantum gates are reversible. In this sub-section, we describe some important single and multiqubit gates and discuss their properties.

The quantum analogue of a classical NOT gate is known as X gate. The operation of an X gate is to flip the computational basis state $|0\rangle$ to $|1\rangle$, and $|1\rangle$ to $|0\rangle$. Since these are quantum gates, their action on quantum states is linear, thus, the X gate flips the basis states of a qubit, i.e., it transforms the state $|\psi\rangle = a|0\rangle + b|1\rangle$ to $|\psi'\rangle = a|1\rangle + b|0\rangle$. Algebraically, $X|\psi\rangle = a(X|0\rangle) + b(X|1\rangle) = |\psi'\rangle$. Therefore, the matrix representation of an X gate is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Since, the X gate is unitary, it is also reversible, i.e., $X|\psi'\rangle = |\psi\rangle$. Interestingly, in classical computation, we have only one reversible logic gate- the NOT gate- whereas there are several 2×2 unitary operators that can be defined as single-qubit quantum gates. For example, another important single-qubit quantum gate used frequently in quantum information and computation is the Z gate. When it operates on the state of a qubit, it leaves the spin up state unchanged and flips the sign of spin down state, such that the state $|\psi\rangle = a|0\rangle + b|1\rangle$ transforms into $|\psi'\rangle = a|0\rangle - b|1\rangle$. This clearly suggests that the matrix representation for the Z gate is $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The third important single-qubit gate we must consider to discuss here is the Hadamard gate. It acts on the state of a qubit in such a way that the initial state $|0\rangle$ transforms to the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, halfway between $|0\rangle$ and $|1\rangle$, and the initial state $|1\rangle$ transforms to the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ which is also half way between $|0\rangle$ and $|1\rangle$. Therefore, the matrix representation for a Hadamard gate is $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$. Although there are infinitely many single-qubit quantum gates due to the existence of the infinitely many 2×2 unitary matrices, we have only discussed three fundamental single-qubit gates frequently used in quantum information and computation.

For multiple qubit gates, we consider two-qubit Controlled Not (CNOT) and three-qubit Toffoli gates. The action of a standard two-qubit CNOT gate is described as $|x, y\rangle \rightarrow |x, y \oplus x\rangle$ where $\oplus$ is addition modulo two. In this case, the two qubits are known as control and target qubit, respectively. If the state of control qubit is $|0\rangle$ then it leaves the target qubit unchanged, but if the state of control qubit is $|1\rangle$, it flips the state of target qubit. Considering this, an appropriate matrix representation for the CNOT gate is $U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, where suffix *CN* stands for a CNOT gate such that $U_{CN}U_{CN}^{\dagger} = I$. Similarly, a three-qubit quantum gate is a Controlled-Controlled-Not

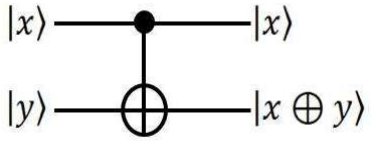

Figure 1.2 : Circuit representation of a CNOT gate.

or Toffoli gate whose action can be described as $|x, y, z\rangle \rightarrow |x, y, z \oplus xy\rangle$. In terms of an operator, it is easy to visualize that the Toffoli gate can be represented by a (8×8) unitary matrix. That Toffoli gate is sufficient to simulate irreversible classical logic gates, is an important evidence to prove that quantum computers are strictly capable of performing any computation which a classical computer may do [Fredkin, 1982; Barenco *et al.*, 1995a].

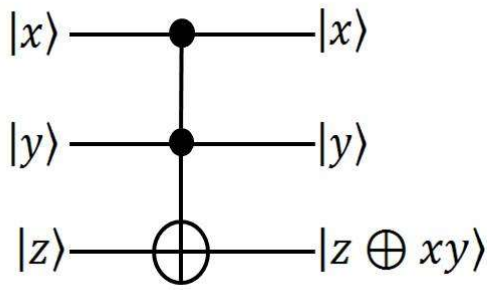

Figure 1.3 : Circuit representation of a Toffoli gate.

These gates have been realized experimentally for optical implementations in quantum information and computation [Milburn, 1989; Knill *et al.*, 2001; Koashi *et al.*, 2001; Ralph *et al.*, 2001]. Considering their importance for quantum computing, elementary quantum gates have been studied and used extensively for manipulation and transfer of information. [Sleator and Weinfurter, 1995; Gottesman and Chuang, 1999; Bartlett and Munro, 2003; Protopopescu *et al.*, 2003; Duan and Raussendorf, 2005; Grigorenko and Khveshchenko, 2005; Walther and Zeilinger, 2005; Isenhower *et al.*, 2010; Ukai *et al.*, 2011; Crespi *et al.*, 2011; Mičuda *et al.*, 2013, 2015; Babazadeh *et al.*, 2017; Russ *et al.*, 2018]

1.2.4 Density Operators in quantum information processing

In classical mechanics, the dynamical state of a system can be completely described if one has the knowledge of types of interactions, i.e., forces acting on the system responsible for the dynamical evolution of the system in addition to the values of initial position and momentum of all particles at a given instance. Therefore, using the complete set of initial conditions and classical equations of motion, it is possible to predict the future motion of a system at a given time. However, in quantum mechanics, due to the restrictions imposed by Heisenberg Uncertainty Principle, such a complete description of maximal information is not possible [Heisenberg, 1958]. Since not all the conjugate variables of interest can be measured simultaneously with precision, quantum mechanics offers only restricted information as against a classical system where all the information is accessible. Clearly, the accessible information in a quantum world is always less than the maximum due to the lack of existence of a complete experiment with a unique predetermined outcome [Fano, 1957]. A mathematical description of the state of a quantum system satisfying the Schrödinger equation, and known as wave function, can be described for only those observables whose operators have common set of eigen functions. Therefore, a wave function can be used to obtain precise values for the properties whose associated operators commute with each other.

Quantum states which can be completely described by a single wave function, are called pure states. In all the other cases, quantum states are known as mixed states. When the system is described to be in a mixed state , then the measurement process introduces a statistical character to the outcome. Thus, a system whose state is not completely known can conveniently be described by a statistical operator known as density operator [Fano, 1957; McWeeny, 1960; Fano, 1983; Blum, 2013]. Density operator can thus be regarded as an alternative mathematical tool to describe

quantum mechanical systems in pure as well as mixed states. Mathematically, the density operator for a quantum system is defined as $\rho = \sum_i p_i |\psi\rangle_i \langle\psi|_i$ where p_i indicates the probability of finding the system in the $|\psi_i\rangle$ state, and $\{p_i, |\psi\rangle_i\}$ represents an ensemble of pure states. When all the p_i's are zero except for a state for which $p_i = 1$, then the system is said to be in a pure state, i.e., in a state with maximal information. Therefore, in case of pure states, the density operator can be represented as $\rho = |\psi\rangle \langle\psi|$. In all other cases, the system is said to be in a mixed state. Thus, the density operator is a possible tool for determining whether an underlying quantum state can be represented by a pure or a mixed state- algebraically this can be ascertained by analysing the inequality $Tr\left(\rho^2\right) \leq 1$ where the equality confirms that the state is a pure state, else it is a mixed state. The importance of density operator description lies in the fact that density operator is a descriptive tool for a composite system in which correlations exist between different sub-systems. The density operator ρ contains all possible information about a system, and describes a statistical ensemble. Density operator has the following properties,

(1) The trace of a density matrix is always equal to one, e.g., for $\rho = \sum_i p_i |\psi\rangle_i \langle\psi|_i$, $Tr(\rho) = \sum_i p_i Tr |\psi\rangle_i \langle\psi|_i = \sum_i p_i = 1$, which is also known as its normalization condition.
(2) It is a Hermitian positive semi-definite operator.
(3) The diagonal elements of a density operator are non-negative and they represent the population of the system in different states.
(4) The density operator for a single-qubit mixed state may be represented as $\rho = \frac{1}{2}\left[I + \overrightarrow{r}.\overrightarrow{\sigma}\right]$ where $\overrightarrow{r}$ is a polarization vector and σ's are Pauli spin operators, and the state is said to be pure if and only if $\|\overrightarrow{r}\| = 1$

One of the important consequences of the density operator formalism is the description of reduced density operators defined as density operators for the sub-systems of a composite system. For example, if the state of a composite system is completely described by a density operator ρ^{AB}, then the reduced density operators for the subsystems A and B are defined by $\rho^A = Tr_B\left(\rho^{AB}\right)$ and $\rho^B = Tr_A\left(\rho^{AB}\right)$, respectively, where Tr_A and Tr_B are partial traces over subsystems A and B, respectively. Due to its properties and physical interpretations, the density operator formalism plays a crucial role in analysing and understanding the nuances of quantum entanglement and information processing [Hughston *et al.*, 1993; Peres, 1996]

1.3 QUANTUM ENTANGLEMENT

In 1935, Einstein, Podolsky and Rosen (EPR) demonstrated a paradox raising the questions regarding completeness of quantum mechanics as a theory [Einstein *et al.*, 1935]. The argument led to the fundamental concept of existence of long-range quantum correlations between entangled particles responsible for achieving efficient, secure and optimal communication in comparison to their classical counterparts. Such correlations not only make the quantum world distinct from their classical analogues, but also provide physical insights into fundamentals of quantum computing and information processing [Bohm and Aharonov, 1957; Bell, 1964; Clauser *et al.*, 1969; Peres, 1990; Gisin, 1991; Home and Selleri, 1991; Khalfin and Tsirelson, 1992; Mermin, 1993; Kwiat *et al.*, 1995; Horodecki *et al.*, 1996; Tittel *et al.*, 1998; Kwiat *et al.*, 2000; Mair *et al.*, 2001; Batle *et al.*, 2002; Babichev *et al.*, 2004; Thew *et al.*, 2004; Genovese, 2005; Özdemir *et al.*, 2007; Zeilinger, 1999; Batle and Casas, 2011; Batle *et al.*, 2016, 2017; Bartkiewicz *et al.*, 2017]. Erwin Schrödinger [Schrödinger, 1926, 1935] first used the term entanglement to define the correlations between the particles, and called it as the characteristic trait of quantum mechanics. David Bohm [Bohm, 1952a,b; Bohm and Aharonov, 1957] defined entanglement in the context of a singlet state of a pair of spin system, which, since then has been essential to investigation the foundations of quantum mechanics and quantum information. Following EPR's argument, John Bell [Bell, 1964] proposed an inequality to understand the fundamental difference between nonlocality and local hidden variable theories.

The Bell inequality based on locality and realism, therefore, distinguishes between the systems which are correlated but whose interactions are local as against to the systems whose correlations are spatially extended and cannot be explained by the assumption of locality.

Algebraically, entanglement can be defined as following: Let us assume a composite system consisting of two subsystems A and B associated with Hilbert spaces H_A and H_B, respectively. We further consider complete sets of orthonormal basis for H_A as $|i\rangle_A$ and for H_B as $|j\rangle_B$ (where $i, j = 1, 2, 3....$). The composite state associated with the Hilbert space $H_A \otimes H_B$ for a system AB is

$$|\psi\rangle_{AB} = \sum_{i,j} c_{ij} |i\rangle_A \otimes |i\rangle_B \tag{1.1}$$

where c_{ij} are complex coefficients and $\sum_{ij} |c_{ij}|^2 = 1$. If the state $|\psi\rangle_{AB}$ cannot be factored into a normalized state $\sum_i^{k=dim(H_A)} c_i |i\rangle_A$ of the subsystem A in H_A and into a normalized state $\sum_j^{k=dim(H_B)} c_j |j\rangle_B$ of the subsystem B in H_B, then the state $|\psi\rangle_{AB}$ is an entangled state, otherwise it is called a separable state. Therefore, the state of a composite quantum system is said to be entangled if it cannot be factored into product states of its sub-systems.

Quantum entanglement is used as a unique and efficient resource for many interesting applications in quantum information and computation [Bennett and Wiesner, 1992; Bennett *et al.*, 1993; Zukowski *et al.*, 1993; Boström and Felbinger, 2002; Gisin *et al.*, 2002]. In comparison to classical resources, entanglement is a purely quantum mechanical phenomenon, with interesting properties such that the measurements performed on one of the sub-systems affect the measurement outcomes of other sub-systems [Einstein *et al.*, 1935]. In general, if users in a protocol share an entangled state with each other, they can transmit the information at remote locations efficiently and securely [Bennett and Wiesner, 1992; Bennett *et al.*, 1993]. Therefore, one of the important aspects of quantum information and computation is to classify and quantify entanglement in bipartite as well as multiqubit systems. In the last three decades, a considerable amount of research has been devoted for the description of entanglement using different entanglement measures. For example, the degree of entanglement in bipartite systems is defined using a measure known as Entanglement of Formation (EoF) or through measures which are physically equivalent to EoF [Schmidt, 1907; Ekert and Knight, 1995; Bennett *et al.*, 1996c; Peres, 1996; Horodecki, 1997; Hill and Wootters, 1997; Wootters, 1998; Vidal and Werner, 2002; Chen *et al.*, 2005b; Buscemi *et al.*, 2007; Gühne *et al.*, 2007; Marian and Marian, 2008; Park *et al.*, 2010; Ganguly *et al.*, 2011; Lastra *et al.*, 2012; Fanchini *et al.*, 2013; Sperling and Vogel, 2013; Ganguly *et al.*, 2014; Streltsov *et al.*, 2015]. In general, there is no unique generalization for a measure to be considered for bipartite as well as multiqubit systems [Wong and Christensen, 2001; Collins *et al.*, 2002a,b; Cereceda, 2002; Wei and Goldbart, 2003; Pan *et al.*, 2003b; Zhao *et al.*, 2003; Eibl *et al.*, 2003, 2004a; Walther *et al.*, 2005a; Eisert *et al.*, 2007; Gühne and Tóth, 2009; Bai *et al.*, 2009; Horodecki *et al.*, 2009; Lavoie *et al.*, 2009; Oliveira and Ramos, 2010; Gühne and Seevinck, 2010; Hou and Qi, 2010; Huber *et al.*, 2010; Bancal *et al.*, 2010; Ghose *et al.*, 2010; Ma *et al.*, 2011; Kay, 2011; Deb, 2011; Prabhu *et al.*, 2012; Spedalieri, 2012; Brandao and Christandl, 2012; Chen *et al.*, 2012; Hyllus *et al.*, 2012; Zhao *et al.*, 2012; Barrett *et al.*, 2013a; Bai *et al.*, 2014; Zhu and Fei, 2014, 2015; Islam *et al.*, 2015; Laflorencie, 2016; Hauke *et al.*, 2016; Zhao *et al.*, 2016; Cianciaruso *et al.*, 2016; Hu *et al.*, 2016; Chen *et al.*, 2016; Buchholz *et al.*, 2016; Luo *et al.*, 2017]. Apparently, the characterization of entanglement in multiqubit systems is much more challenging due to the increased complexity of the system. The different measures to quantify entanglement capture different aspects of the phenomenon and hence do not often agree with one another. In reality, the properties of bipartite mixed entangled systems itself needs a much better physical interpretation [Vedral and Plenio, 1998; Audenaert *et al.*, 2001, 2002; Vidal and Werner, 2002; Lee *et al.*, 2003; Osborne, 2005; Mintert and Buchleitner, 2007; Zhang *et al.*, 2008; Kim *et al.*, 2010]. Further, another important aspect of entangled systems

to be mentioned here is that the spatially separated users, sharing a composite entangled system, can only modify the entanglement properties of the system by performing local operations on their respective subsystems assisted with classical communication, i.e., they may convert one entangled state into another equivalent state with similar entanglement properties, but in no way distant users can generate an entangled state from unentangled states or convert two inequivalent classes of entangled states with certainty by performing sequence of local operations assisted with classical communication [Werner, 1989; Bennett *et al.*, 1996c; Vedral *et al.*, 1997a; Horodecki *et al.*, 2000; Vidal *et al.*, 2002; Horodecki *et al.*, 2003; Plenio and Virmani, 2005; Fan, 2004; de Vicente *et al.*, 2013; Chitambar *et al.*, 2014]. Therefore, the mean entanglement of a system cannot be increased using local operations and classical communication. In general, a measure needs to satisfy the following criteria to be considered as an entanglement measure [Vedral *et al.*, 1997b; Wootters, 1998; Vidal, 2000];

(1) The measure of entanglement for any product state should be zero, i.e., $E(\rho) = 0$, and $E(\rho)$ must attain its maximum value for maximally entangled states.
(2) The amount of entanglement in any state ρ should not increase under local operations and classical communication (LOCC), i.e., $\sum_i p_i E(\rho_i) \leq E(\rho)$.
(3) A certain number n of identical copies of the system ρ must contain n times the entanglement of one copy, i.e., $E(\rho^{\otimes n}) = nE(\rho)$.
(4) The entanglement measure E must be a convex function, i.e.,
$$E(\lambda\rho + (1-\lambda)\rho) \leq \lambda E(\rho) + (1-\lambda)E(\rho)$$
(5) The degree of entanglement of product of two states should not be greater than the sum of degree of entanglement of individual states, i.e.,
$$E(\rho_1 \otimes \rho_2) \leq E(\rho_1) + E(\rho_2)$$
(6) The amount of entanglement in any state ρ should not be affected by any local unitary operation of the form $(U_A \otimes U_B)$, i.e., $E(\rho) = E(U_A \otimes U_B \rho U_A^{\dagger} \otimes U_B^{\dagger})$.

Entanglement measures satisfying the above criteria are called entanglement monotones. For bipartite systems, there are several measures to describe entanglement properties- some of which we will consider in following subsections [Ekert and Knight, 1995; Bennett *et al.*, 1996c,d; Peres, 1996; Horodecki, 1997; Vedral *et al.*, 1997a; Horodecki *et al.*, 1998; Wootters, 1998; Lewenstein *et al.*, 2000; Vidal and Werner, 2002].

1.3.1 Measures of entanglement in pure and mixed two-qubit states

A pure two-qubit state can be expressed as $|\psi\rangle = \alpha|00\rangle + e^{i\delta}\beta|11\rangle_{AB,}$ where δ is relative phase between the qubits. For a maximally entangled two-qubit pure state, one can choose $\alpha = \beta = \frac{1}{\sqrt{2}}$, and $\delta = 0$. The state defined with these parametric values is known as one of the Bell states [Nielsen and Chuang, 2010]. The set of all maximally entangled Bell states are defined as

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle \pm |11\rangle\right], \qquad \left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle \pm |10\rangle\right] \tag{1.2}$$

Moreover, any arbitrary spin-1/2 state can also be represented using a density operator [Horodecki, 1995] as

$$\rho = \frac{1}{4}(I^1 \otimes I^2 + \mathbf{r}^1 \cdot \sigma^1 \otimes I^2 + I^1 \otimes \mathbf{s}^2 \cdot \sigma^2 + \sum_{n,m=1}^{3} t_{nm}\sigma_n^1 \otimes \sigma_m^2) \tag{1.3}$$

where $(1,2)$ represent the qubit index, I is a $2 \otimes 2$ identity operator, $\mathbf{r}$ and $\mathbf{s}$ represent polarization vectors of two spins, respectively, σ^i stands for standard Pauli matrices, and coefficients t_{nm} form a

real matrix which we denote by T_ρ such that $t_{nm} = Tr(\rho.\sigma_n \otimes \sigma_m)$. We now proceed to discuss some important measures of entanglement for pure and mixed states.

(a) Schmidt Number

The possibility of interconversion of two pure bipartite states using local operations and classical communications can be established using a mathematical framework from theory of majorization- leading to an important tool to define separability and entanglement in two-qubit systems known as Schmidt coefficients or Schmidt numbers [Schmidt, 1907; Ekert and Knight, 1995; Bennett *et al.*, 1996c; Sperling and Vogel, 2011a,b; Guo and Fan, 2015]. In order to define Schmidt numbers, we first consider $|\psi\rangle_{AB}$ to be a pure state of a composite system AB in the Hilbert space $H_A \otimes H_B$. If $|i\rangle_A$ and $|i\rangle_B$ represent orthonormal basis for subsystems A and B, respectively, then the state $|\psi\rangle_{AB}$ can be written in form of Schmidt decomposition, such that

$$|\psi\rangle_{AB} = \sum_{i}^{n \leq min\{dim(H_A), dim(H_B)\}} \sqrt{\lambda_i}\, |i\rangle_A \otimes |i\rangle_A \tag{1.4}$$

where λ_i are non-negative real numbers, i.e., $\lambda_i \geq 0$ satisfying $\sum_i \lambda_i = 1$, called as Schmidt coefficients or Schmidt number. Schmidt number can be used to quantify the extent of entanglement between the qubits, e.g., if for the state $|\psi\rangle_{AB}$ only one Schmidt coefficient is non-zero and all others are zero, then $|\psi\rangle_{AB}$ is a separable state otherwise it is an entangled state. In other words, the necessary and sufficient condition for the state $|\psi\rangle_{AB}$ to be a product state is that both the subsystems ρ^A and ρ^B are in pure states. Further, since the eigenvalues of the subsystems are always equal, Schmidt coefficients provide a way to study many interesting properties of the composite system $|\psi\rangle_{AB}$. Evidently, Schmidt coefficients remains invariant under local unitary transformations.

(b) Entanglement of Formation

Using the application of local operations and classical communication, if we generate m copies of a pure state $|\psi\rangle$ starting from n copies of Bell states, then the limiting ratio m/n is defined as Entanglement of Formation (EoF) [Bennett *et al.*, 1996c]. Alternately, it can be defined as the von-Neumann entropy of the reduced density operators associated with either of the two subsystems of a pure two-qubit state [Petz, 2001; Nielsen and Chuang, 2010]. For this, let us assume that Alice and Bob share a two-qubit pure entangled state $|\psi\rangle_{AB,}$ then the entanglement of formation for $|\psi\rangle_{AB}$ is

$$E(|\psi\rangle_{AB}) = S(\rho_A) = S(\rho_B) \tag{1.5}$$

where $S(\rho) = -Tr(\rho log_2 \rho)$ is the von-Neumann entropy, and ρ_A and ρ_B are reduced density operators of the pure two-qubit state $|\psi\rangle_{AB,}$ i.e., $\rho_A = Tr_B(|\psi\rangle_{AB}\langle\psi|_{AB})$, and $\rho_B = Tr_A(|\psi\rangle_{AB}\langle\psi|_{AB})$. The value of EoF monotonically increases from 0 to 1 for product to maximally entangled states, respectively. For a mixed two-qubit state ρ, EoF is defined as

$$E(\rho) := \min \sum_i E(|\psi\rangle_i \langle\psi|_i) \tag{1.6}$$

where $\rho = \sum_i p_i (|\psi\rangle_i \langle\psi|_i)$. Clearly, EoF for pure states is easily computable whereas for mixed states, the computation is extremely difficult [Vedral and Plenio, 1998; Osborne, 2005; Chen *et al.*, 2005b; Gühne *et al.*, 2007; Mintert and Buchleitner, 2007; Zhang *et al.*, 2008; Marian and Marian, 2008; Horodecki *et al.*, 2009; Lastra *et al.*, 2012; Fanchini *et al.*, 2013].

(c) Peres-Horodecki Criterion (Positive Partial Transpose)

Peres-Horodecki criterion is a qualitative approach to analyse the separability in an underlying mixed state. It is also shown to be a necessary and sufficient condition to test the separability of mixed states in $2 \otimes 2$ and $2 \otimes 3$ dimensional systems [Peres, 1996; Horodecki, 1997; Giedke *et al.*, 2001]. The Peres-Horodecki criterion states that if ρ is an arbitrary mixed two-qubit state, then the positivity of the partial transpose operator $\rho_{ij,kl}^{T_B} = \rho_{il,kj}$ with respect to the qubit B ensures the separability of ρ. In other words, we can say that if the state ρ is separable then the partial transpose operator will have all non-negative eigenvalues. The result of Peres-Horodecki criterion is independent of the partial transposed subsystem, as $\rho^{T_A} = (\rho^{T_B})^T$.

(d) Concurrence

Concurrence is a celebrated measure to quantify degree of entanglement in pure and mixed two-qubit systems [Hill and Wootters, 1997; Wootters, 1998, 2001; Chen *et al.*, 2005a; Li *et al.*, 2011; Zhou and Sheng, 2015]. The concurrence for two-qubit states is defined as

$$C(\rho) = max(0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}) \tag{1.7}$$

where λ_i are the eigenvalues of an operator $(\sqrt{\rho}(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)\sqrt{\rho})$ in decreasing order with ρ^* denoting the complex conjugation of the density operator ρ representing a mixed state and σ_y denotes the Pauli spin operator. The value of concurrence for pure states monotonically increases between 0 and 1- it attains the maximum value 1 for maximally entangled states and the minimum value 0 for product states. Alternately, for a general pure two-qubit state $|\psi\rangle_{AB} = [\alpha|00\rangle + \beta|11\rangle]_{AB,}$ $|\alpha|^2 + |\beta|^2 = 1$, the concurrence is given by

$$C = 2\sqrt{\alpha\beta} \tag{1.8}$$

If a pure two-qubit state is described by a density operator ρ, i.e., $\rho_{AB} = (|\psi\rangle_{AB}\langle\psi|_{AB})$, then the concurrence is given by

$$C = \sqrt{2(1 - Tr(\rho_A^2)} \tag{1.9}$$

Although EoF is an entanglement measure and concurrence is a physically equivalent definition through the relation

$$E(\rho) = H\left(1 + \sqrt{1 - C^2}/2\right) \tag{1.10}$$

where $H(p) = -p\log p + (1-p)\log(1-p)$, one tends to use concurrence as an entanglement measure for bipartite mixed states instead of Entanglement of Formation due to the ease of evaluating the concurrence.

There are several other criteria to define bipartite entanglement such as entanglement witness [Lewenstein *et al.*, 2000; Terhal, 2002], von-Neumann relative entropy [Plenio and Vedral, 1998; Vedral *et al.*, 1997a; Vedral, 2002], distillable entanglement [Bennett *et al.*, 1996d; Rains, 1999; Vidal *et al.*, 2002] and bound entanglement [Horodecki *et al.*, 1998; Bennett *et al.*, 1999; Horodecki *et al.*, 1999b; Sanpera *et al.*, 2001; Ishizaka, 2004; Yang *et al.*, 2005; Horodecki *et al.*, 2009; Kaneda *et al.*, 2012; Vértesi and Brunner, 2014].

1.3.2 Measures of entanglement in three-qubit states

The classification and quantification of entanglement in multiqubit systems is a much more interesting and challenging problem due to the very nature of entanglement, i.e., complexity [Cereceda, 2002; Collins *et al.*, 2002b; Eibl *et al.*, 2004a]. For example, for three-qubit pure states, one has to think about establishing a relation between the degree of entanglement shared between qubits A and B, and the degree of entanglement shared between qubits A and C. If the entanglement between A and B is defined to be maximum, i.e., if the joint system of qubits A and B is in one of the Bell states, then AB as a joint entity cannot have any entanglement with the qubit C. However, if the entanglement between A and B is not maximum, i.e., if the joint system of qubits A and B is in a partially entangled state, then the joint system of qubits AB can still share a limited entanglement with the qubit C. In order to facilitate the discussion regarding measures which capture the entanglement between three qubits, we first briefly describe the different classes in which three-qubit pure states can be defined [Dür *et al.*, 1999, 2000], e.g.,

(1) *Product States (Class A-B-C)*- Product states do not possess any entanglement among any of the qubits. Since it is a product state where every subsystem is in a pure state, i.e., in a state of maximal information- the von-Neumann entropy of any of the reduced single-qubit density operators will be 0. A general form of this class can be expressed as

$$|\phi_{A-B-C}\rangle = \left(\sin\theta_1|0\rangle + e^{i\delta_1}\cos\theta_1|1\rangle\right)_A \otimes \left(\sin\theta_2|0\rangle + e^{i\delta_2}\cos\theta_2|1\rangle\right)_B \otimes \left(\sin\theta_3|0\rangle + e^{i\delta_3}\cos\theta_3|1\rangle\right)_C \tag{1.11}$$

(2) *Bi-separable States (Classes A-BC, B-AC, and C-AB)*- As is clear from the representation, these class of states represent three-qubit bi-separable states where any two of the qubits are entangled and the joint state of two entangled qubits forms a product state with the state of third qubit, e.g., a bi-separable state of class $A-BC$ can be written as

$$|\phi_{A-BC}\rangle = \left(\sin\theta_1|0\rangle + e^{i\delta_1}\cos\theta_1|1\rangle\right)_A \otimes \left(\sin\theta_2|00\rangle + e^{i\delta_2}\cos\theta_2|11\rangle\right)_{BC} \tag{1.12}$$

Similarly, bi-separable states can be defined for classes $|\phi_{B-AC}\rangle$ and $|\phi_{C-AB}\rangle$. The von-Neumann entropy in this case will be 0 for reduced density operator of qubit 1 as it is in a pure state, but the von-Neumann entropy of the reduced density operators for qubits 2 and 3 will depend on the parameter θ_2, e.g., maximum uncertainty can be obtained if the joint state of two qubits is a maximally entangled state.

(3) *Genuine tripartite entanglement*- Any three-qubit pure state possessing genuine tripartite entanglement, can be characterized in this category Dur *et al.* [Dür *et al.*, 2000], demonstrated that three-qubit pure states can be classified into two inequivalent classes, namely GHZ class and W class. The states belonging to the two classes cannot be interchanged into one another even with the smallest probability by performing local operations and classical communications. However, they established that any three-qubit pure state can either be converted to GHZ class or W class by performing stochastic local operations and classical communications (SLOCC). The classification and properties of two classes can be described as per the following:

(A) *Greenberg-Horne-Zeilinger (GHZ) States:* In 1989, Daniel Greenberg, Michael Horne, and Anton Zeilinger proposed a general state containing genuine tripartite entanglement [Greenberger *et al.*, 1989], represented as

$$|\psi\rangle_{GGHZ} = \cos\theta|000\rangle_{123} + e^{i\delta}\sin\theta|111\rangle_{123} \tag{1.13}$$

where for $\theta = \pi/4$ and $\delta = 0$, one can define the maximally entangled GHZ state as

$$|\psi\rangle_{GHZ} = \frac{1}{\sqrt{2}}\left[|000\rangle_{123} + \theta|111\rangle_{123}\right] \tag{1.14}$$

These states are not robust in terms of loss of any qubit. In other words, if we trace the state over a subsystem, the remaining state no longer remains entangled, i.e., the

reduced density operator representing the state of two-qubit system contains only classical correlations. GHZ states are shown to be very useful resources for performing many efficient and optimal quantum information processing protocols [Gottesman and Chuang, 1999; Karlsson and Bourennane, 1998; Hillery *et al.*, 1999; Raussendorf *et al.*, 2003; Browne and Rudolph, 2005; Lee *et al.*, 2006].

(B) *W States:* The genuinely entangled three-qubit W class of states can be represented as

$$|W\rangle = x|001\rangle_{123} + y|010\rangle_{123} + z|001\rangle_{123} \tag{1.15}$$

where $|x|^2 + |y|^2 + |z|^2 = 1$, and in the standard case, we consider $x = y = z = \frac{1}{\sqrt{3}}$, hence, the standard W state is given by

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle_{123} + |010\rangle_{123} + |001\rangle_{123}) \tag{1.16}$$

In this case, all the qubits are pairwise entangled, i.e., the von-Neumann entropy of reduced density operators of any of the subsystems is always greater than 0. Unlike GHZ class states, W states are robust against the loss of one qubit, i.e., if one of three qubits is traced out, the remaining qubits will still represent a two-qubit entangled state. For W class states, one can use $min(C_{12}^2, C_{23}^2, C_{31}^2) > 0$ as a measure of entanglement where C_{ij}^2 is the square of concurrence between qubits i and j [Dür *et al.*, 2000; Linden *et al.*, 2002].

We now proceed to discuss entanglement measures capturing the tripartite entanglement in three-qubit entangled classes.

(a) 3-tangle (τ)

A measure of genuine tripartite entanglement, known as three-tangle τ, is used to characterize the nonlocal properties in three-qubit entangled systems [Coffman *et al.*, 2000]. The three-tangle is expressed as

$$\tau = C_{i(jk)}^2 - C_{ij}^2 - C_{ik}^2 \tag{1.17}$$

where concurrence C_{ij} quantifies the bipartite entanglement between qubits i and j, and concurrence $C_{i(jk)}$ measures the entanglement between qubit i and the joint state of qubits j and k [Wootters, 1998]. The three-tangle varies from 0 for product states to 1 for maximally entangled three-qubit states. For example, the three-tangle for generalized GHZ states $|\psi\rangle_{GGHZ} = \cos\theta|000\rangle_{123} + \sin\theta|111\rangle_{123}$ is given by

$$\tau(\rho_{GGHZ}) = \sin^2 2\theta \tag{1.18}$$

For $\theta = 0$, the GGHZ state is a product state of three qubits, and hence, $\tau = 0$. Similarly for $\theta = \pi/4$, the GGHZ state is a maximally entangled standard GHZ state, and hence, $\tau = 1$.

(b) Sigma (σ)

The three-tangle is used to characterize the genuine tripartite entanglement in GHZ class states, but it fails to detect the entanglement in all the W class states. Actually, in three-qubit entangled systems, the distribution of the entanglement among qubits is constrained by the monogamy inequality, such as

$$C_{i(jk)}^2 \geq C_{ij}^2 + C_{jk}^2 \tag{1.19}$$

This equality can be achieved by W class states, therefore three-tangle for W class states is always zero, i.e., $\tau(\rho_W) = 0$. Alternately, degree of entanglement in three-qubit pure states can also be quantified using a measure σ, [Emary and Beenakker, 2004] defined as

$$\sigma = min\left(\frac{C_{i(jk)}^2 + C_{j(ik)}^2}{2} - C_{ij}^2, \frac{C_{j(ik)}^2 + C_{k(ij)}^2}{2} - C_{jk}^2, \frac{C_{i(jk)}^2 + C_{k(ij)}^2}{2} - C_{ik}^2\right) \tag{1.20}$$

where minimum is taken over permutations of three-qubits. The value of σ for the standard GHZ state and the standard W state is 1 and $4/9$, respectively.

(c) Negativity

Another important computable measure for two-qubit and multiqubit entanglement is negativity which can be conveniently used as an entanglement monotone to quantify entanglement in pure and mixed entangled states [Vidal and Werner, 2002; Audenaert *et al.*, 2003; Sabín and García-Alcaine, 2008a; Weinstein, 2010; Eltschka and Siewert, 2013]. For example, negativity for a two-qubit system can be defined in terms of eigen values of the partial transpose of one of the subsystems, i.e.,

$$N(\rho) = \frac{\| \rho^{T_B} \| - 1}{2} \tag{1.21}$$

where $\| \rho^{T_B} \|$ is the trace norm defined as $\| A \| = tr\left(\sqrt{A^{\dagger}A}\right)$ and ρ^{T_B} is the partial transpose of the two-qubit system with respect to the subsystem B. Since negativity is not additive, a more convenient way to define it, is in terms of logarithmic negativity, i.e.,

$$N_L(\rho) = \log_2 \| \rho^{T_B} \| \tag{1.22}$$

Although logarithmic negativity is neither asymptotically continuous nor convex, it is advantageous in terms of its use for ease of calculation and for other operational interpretations. For a three-qubit system, Negativity can be given by

$$N_{ABC}(\rho) = (N_{A-BC} N_{B-AC} N_{C-AB})^{\frac{1}{3}} \tag{1.23}$$

where N_{A-BC} quantifies the amount of entanglement or nonlocal correlations between subsystem A and the joint state of subsystems B and C. Similarly, one can define the negativities N_{B-AC} and N_{C-AB}. The tripartite negativity N_{ABC} is an exciting tool that confirms the distinction between separable, bi-separable, and genuine tripartite entanglement in three-qubit pure states.

One can also use the sum of concurrences of three reduced states, i.e., $\left(C_{ij} + C_{jk} + C_{ki}\right)$ as an entanglement monotone for W-class states [Dür *et al.*, 2000; Linden *et al.*, 2002]. There are several other criteria which measure the entanglement in multiqubit systems as well [Rungta *et al.*, 2001; Verstraete *et al.*, 2002; Meyer and Wallach, 2002; Verstraete *et al.*, 2002; Wei and Goldbart, 2003; Barnum *et al.*, 2004; Osterloh and Siewert, 2005; Gühne *et al.*, 2005; Mandilara *et al.*, 2006; Rigolin *et al.*, 2006; Facchi *et al.*, 2008; Dan *et al.*, 2008; Bai *et al.*, 2009; Huber *et al.*, 2010; Ma *et al.*, 2011; Brandao and Christandl, 2012; Islam *et al.*, 2015; Hu *et al.*, 2016; Chen *et al.*, 2016; Luo *et al.*, 2017]. Therefore, considering the importance of entangled system for quantum information and communication, theoretical as well as the mathematical measures for quantifying the degree of entanglement have been studied in great detail.

Apart from the theoretically driven curiosity, it is imperative to meet the challenges arising during experimental preparation of entangled systems. On these lines, Kwiat [Kwiat, 1995] proposed the first experimental realization to prepare Bell states using polarization-entangled photon pairs and parametric-down conversion. Subsequently, the generation and analysis of Bell states was further strengthened by several groups across the globe [Aspect *et al.*, 1982; Zukowski *et al.*, 1993; Pavičić and Summhammer, 1994; Weinfurter, 1994; Rubin *et al.*, 1994; Cirac and Zoller, 1994; Fry *et al.*, 1995; Braunstein and Mann, 1996; Michler *et al.*, 1996; Hagley *et al.*, 1997; Tittel *et al.*, 1998; Di Giuseppe *et al.*, 2003; Marcikic *et al.*, 2004; Peng *et al.*, 2005; Walther and Zeilinger, 2005; Bernien *et al.*, 2013; Barbieri *et al.*, 2017]. For multiqubit systems, due to the increased complexity, the problem to prepare and characterize multiqubit states increase enormously. Zeilinger *et al.* (1997) and Bouwmeester *et al.* (1999) have proposed a scheme for experimental preparation

of three-qubit Greenberger-Horne-Zeilinger (GHZ) states [Zeilinger *et al.*, 1997; Bouwmeester *et al.*, 1999]. Although dealing with quantum systems experimentally is very challenging, a lot of progress has been made towards experimental realization of multiqubit entangled states for quantum information and computation [Gerry, 1996; Sackett *et al.*, 2000; Rauschenbeutel *et al.*, 2000; Pan *et al.*, 2000; Weinfurter and Żukowski, 2001; Zhao *et al.*, 2004; Kiesel *et al.*, 2005; Bruß *et al.*, 2005; Leibfried *et al.*, 2005; de Oliveira *et al.*, 2006; Prevedel *et al.*, 2007; Lu *et al.*, 2007; Vallone *et al.*, 2007; Tokunaga *et al.*, 2005, 2008; Lavoie *et al.*, 2010; Gao *et al.*, 2010, 2012; Pan *et al.*, 2012; Riedel *et al.*, 2012].

1.4 NONLOCALITY

The potential offered by the efficient use of entangled systems as resources for quantum information, communication, cryptography and quantum computing in comparison to their classical counterparts is based on the existence of long-range correlations between entangled qubits. Bell greatly advanced the investigation of quantum entanglement by deriving an inequality, now known as the Bell inequality which must be obeyed by systems which are correlated but whose interactions are local as against to the systems whose correlations are spatially extended and cannot be explained by the assumption of locality [Bell, 1964]. The Bell inequality, therefore, distinguishes between quantum systems as efficient resources for information processing as against their classical analogues. A more generalized version of the Bell inequality is given by Clauser, Horne, Shimony and Holt- known as the CHSH inequality [Clauser *et al.*, 1969], namely

$$-2 \leq |\langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle| \leq 2 \tag{1.24}$$

where A_0, A_1, B_0 and B_1 are the measurement operators to measure the associated physical properties P_{A_0}, P_{A_1}, P_{B_0} and P_{B_1} of a system, respectively. While deriving the inequality, it was assumed that Alice and Bob are located sufficiently far apart from each other so that their measurement outcomes are not affected by one another, and that both Alice and Bob choose their measurements independently. In the ideal case, Alice and Bob choose their measurements as A_0 or A_1 and B_0 or B_1 with an equal probability of $\frac{1}{2}$. Since the measurement outcomes of operators A_0, A_1, B_0 or B_1 are ± 1, the CHSH inequality is valid for all different measurement outcomes. Clearly, following the EPR argument under the assumption of locality and realism, all two-qubit states must satisfy the Bell inequality. However, for a two-qubit antisymmetric singlet state $|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]_{12}$ shared between Alice and Bob, the Bell inequality is violated and for a specific set of measurements, it attains a maximum value of $2\sqrt{2}$ which is clearly greater than 2. Therefore, the Bell inequality definitely identifies states with correlations which cannot be explained on the basis of locality and realism, hence, creating a boundary between quantum and classical correlations. The singlet states, for violating the inequality to the maximum, are known as maximally entangled two-qubit states. Using simple single-qubit unitary transformations, one can identify a set of four maximally entangled two-qubit states, defined as $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]$, and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$, and known as Bell states. For a system with classical as well as quantum correlations, it is only the quantum correlations that are considered for describing the nonlocal properties of the system. For an entangled pair, measurement outcomes on the first particle depends on the measurement outcomes of the second- this interdependence between the measurement outcomes for two particles is known as nonlocality.

To summarize, there were two assumptions made to derive the Bell inequality:

(1) Assumption of realism: measurements A_0, A_1, B_0 and B_1 exist independent of observations

and are definite values of physical properties $P_{A_0}, P_{A_1}, P_{B_0}$ and P_{B_1}, respectively.

(2) Assumption of locality: Alice's measurement cannot have any effect on the result of Bob's measurement.

The violation of Bell inequality evidently suggests that either or both the assumptions of locality and realism are not correct in the quantum regime. Hence, the violations of Bell or Bell-type inequalities reveal the presence of nonlocal correlations between qubits, and shed light on the deep structure of nonlocality in quantum systems [Leggett and Garg, 1985; Toner and Bacon, 2003; Acín *et al.*, 2005; Gröblacher *et al.*, 2007; Souza *et al.*, 2008; Barbieri, 2009; Goggin *et al.*, 2011; Xu *et al.*, 2011; Knee *et al.*, 2012; Castillo *et al.*, 2013; Epping *et al.*, 2013; Zhou *et al.*, 2015; Chaves *et al.*, 2015; Montina and Wolf, 2016; Chaves and Budroni, 2016; Ringbauer *et al.*, 2016; Brito *et al.*, 2018]. A quantum resource exhibiting nonlocal correlation has been shown to perform information processing tasks which are otherwise found to be difficult or impossible to achieve using classical resources [Bennett and Wiesner, 1992; Bennett *et al.*, 1993; Zukowski *et al.*, 1993; Boström and Felbinger, 2002; Gisin *et al.*, 2002].

1.4.1 Bell-type inequalities for three-qubit states

Similar to two-qubit systems, N. D. Mermin proposed a Bell-type inequality to confirm the nonlocal correlation in tripartite systems [Mermin, 1990], given as

$$|M| = |\langle A_0B_0C_0\rangle - \langle A_0B_1C_1\rangle - \langle A_1B_0C_1\rangle - \langle A_1B_1C_0\rangle| \leq 2. \tag{1.25}$$

Here the additional measurements C and C′ correspond to the measurements performed by a third user, say Charlie, in addition to the measurements performed by Alice and Bob as in the case of Bell-CHSH inequality. The Mermin inequality is violated by genuinely entangled three-qubit states, confirming the presence of nonlocal correlations between three qubits. The inequality is maximally violated by a set of maximally entangled three-qubit Greenberger-Horne-Zeilinger states, with the maximum value as 4. This violation, however, is marred by the violation of inequality by bi-separable states as well. This makes it difficult to distinguish between bi-separable vs genuine tripartite nonlocality. On the other hand, Svetlichny derived an inequality which is satisfied by separable as well as bi-separable states and violated by genuinely entangled three-qubit states only [Svetlichny, 1987]. Hence, the violation of Svetlichny inequality is a necessary and sufficient condition to ensure the presence of genuine tripartite nonlocality. The Svetlichny inequality can be expressed as

$$|S_v| = |\langle A_0B_0K_0\rangle + \langle A_0B_1K_1\rangle + \langle A_1B_0K_1\rangle - \langle A_1B_1K_0\rangle| \leq 4. \tag{1.26}$$

where, $K_0 = (C_0 + C_1)$ and $K_1 = (C_0 - C_1)$, and operators have the usual representation as defined above. Similar to the Mermin inequality, the Sveltichny inequality is maximally violated by GHZ states with the maximum violation as $4\sqrt{2}$. The inequality, however, is violated by set of GHZ states with $\tau > 1/2$ only, i.e., the inequality fails to identify nonlocal correlations in GHZ states with $\tau < 1/2$ as show in Figure 1.4. Interestingly, the Svetlichny inequality is violated by a set of all states, known as Slice states [Carteret and Sudbery, 2000]. Svetlichny inequality can also be generalized to multiqubit GHZ and W class of states to distinguish between local and nonlocal correlations [Seevinck and Svetlichny, 2002]. Since, multiqubit correlations are important not only for understanding the foundations of quantum information, but they also for providing a way to multi-scale quantum information and computation, therefore, in the last two decades, a lot of research has been devoted to detect nonlocal correlations in multiqubit systems using Bell-type inequalities [Svetlichny, 1987; Seevinck and Svetlichny, 2002; Collins *et al.*, 2002a,b; Cereceda, 2002; Pan *et al.*, 2003b; Zhao *et al.*, 2003; Eibl *et al.*, 2003, 2004a; Walther *et al.*, 2005a; Lavoie *et al.*, 2009; Ghose *et al.*, 2009, 2010; Bancal *et al.*, 2010; Ajoy and Rungta, 2010; Liu *et al.*, 2010; Pál and Vértesi,

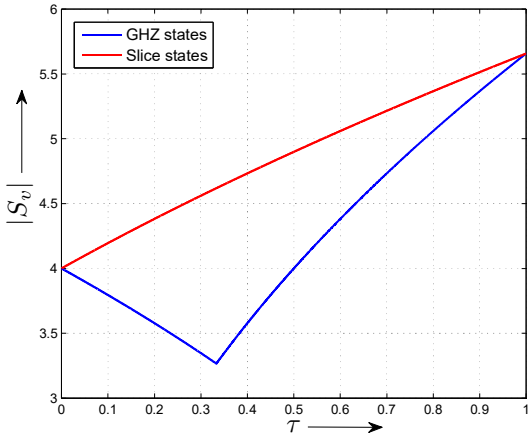

Figure 1.4 : A plot of maximum expectation value of the three-qubit Svetlichny operator versus three-tangle for GHZ and Slice states.

2011; Lu *et al.*, 2011a; Bancal *et al.*, 2011; Chen *et al.*, 2011; Lu *et al.*, 2011b; Chen *et al.*, 2011; Zhao *et al.*, 2012; Chaves *et al.*, 2012; Vértesi and Brunner, 2012; Reid *et al.*, 2012; Chaves *et al.*, 2012; Pramanik and Majumdar, 2012; Tian *et al.*, 2012; Bancal *et al.*, 2013; He and Reid, 2013; Barrett *et al.*, 2013a; Brunner *et al.*, 2014; Lanyon *et al.*, 2014; Chaves *et al.*, 2014; Sohbi *et al.*, 2015; Caban *et al.*, 2015; Fonseca and Parisio, 2015; Alsina and Latorre, 2016; Jebaratnam, 2016; Tavakoli, 2016; Paul *et al.*, 2016; Sharma *et al.*, 2016; Vallins *et al.*, 2017; de Rosier *et al.*, 2017].

1.4.2 Quantum Discord

Due to the general belief that entanglement is the key ingredient for speed-up and efficiency of quantum computation in comparison to classical computation, entanglement and nonlocality have been the subjects of intensive studies since 1935. Although entangled systems are established as efficient resources for several quantum information processing tasks, separable systems (non entangled systems) were thought to be classical systems not useful for quantum information, i.e., the description of quantum correlations was mainly associated with entanglement and nonlocality. This perception has been questioned with the identification of few separable systems exhibiting quantum correlations and for showing potential to be used as resources for quantum information processing. Quantum discord, for example, is a measure of nonlocal correlations and captures the nonlocality in entangled as well as separable bipartite systems [Luo, 2008a; Ollivier and Zurek, 2001; Henderson and Vedral, 2001; Zhang *et al.*, 2012].

Therefore, the theoretical and experimental investigations suggesting the importance of nonlocal correlations in separable systems derive the need to classify correlations beyond the boundaries of Bell-type inequalities [Dakić *et al.*, 2010; Xi *et al.*, 2012; Shi *et al.*, 2012; Gheorghiu *et al.*, 2015; Liu *et al.*, 2015a; Namkung *et al.*, 2015; Chuan-Mei *et al.*, 2015; Mahdian and Arjmandi, 2016; Gerasev and Kuznetsova, 2016; Moreva *et al.*, 2017; Vedral, 2017; De Chiara and Sanpera, 2017; Bera *et al.*, 2017; Christ and Hinrichsen, 2017; Braun *et al.*, 2017; Domínguez-Serna *et al.*, 2017; Zhang *et al.*, 2017; Zalys-Geller *et al.*, 2018]. In this sub-section, we briefly discuss the definition and importance of discord to identify quantum correlations in an underlying quantum state. The total correlation in a bipartite system consists of both classical and quantum correlation, and can be measured by quantum mutual information. For example, if ρ^{AB} is a composite bipartite system,

then the quantum mutual information is defined as

$$I(\rho^{AB}) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \tag{1.27}$$

where $S(\rho) = -Tr(\rho log_2 \rho)$ is the von-Neumann entropy, and ρ_A and ρ_B are reduced density operators for two subsystems A and B, respectively. Using the definition of quantum mutual information, one can define discord as a measure of nonlocal correlations as

$$D_A(\rho^{AB}) = I(\rho^{AB}) - \max_{\left\{\Pi_j^A\right\}} J_{\left\{\Pi_j^A\right\}}(\rho^{AB}) \tag{1.28}$$

where $J_A(\rho^{AB})$ is measurement based mutual information representing classical correlations between two subsystems, given by

$$J_A(\rho^{AB}) = S(\rho^B) - S(\rho^B|\rho^A) \tag{1.29}$$

Here $S(\rho^B|\rho^A)$ is the conditional quantum entropy. Some salient features of quantum discord can be summarized as below

(1) Since the conditional entropy is not symmetric, quantum discord is also not symmetric, i.e., $D_A(\rho) \neq D_B(\rho)$.
(2) Quantum discord is always non-negative, i.e $D(\rho^{AB}) \geq 0$.
(3) Quantum discord of any state ρ is invariant under any local unitary operations of the form $(U_A \otimes U_B)$, i.e., $D(\rho) = D(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger)$.
(4) If a state has only classical correlations then quantum discord is zero, i.e., $D = 0$.

Recently, both theoretical and experimental aspects of quantum discord have been studied. However, due to the optimization procedure, it is difficult to obtain an analytical expression for arbitrary two-qubit states- discord was analytically computed only for a few families of two-qubit states [Girolami and Adesso, 2011; Luo, 2008a]. In order to overcome this difficulty, a measure to quantify the amount of nonclassical correlations in an arbitrary two-qubit system is introduced in terms of its minimal distance from the set of classical states- geometric discord [Dakić *et al.*, 2010; Luo and Fu, 2010; Qiang *et al.*, 2015; Wu and Zhou, 2015; Qiang *et al.*, 2016; Roga *et al.*, 2016], which can be defined as

$$D_G(\rho) = \frac{1}{4}\left[\|T_\rho\|^2 + \|\vec{r}\|^2 - \lambda_{max}(\vec{r}.\vec{r}^T + T_\rho.T_\rho^T)\right] \tag{1.30}$$

where $\vec{r}$ represents a Bloch vector, T_ρ represents a matrix such that the elements of T_ρ are $t_{nm} = Tr(\rho.\sigma_n \otimes \sigma_m)$ and $\vec{r}^T$, T_ρ^T are transpose of $\vec{r}$ and T_ρ, respectively. Moreover, $\|\vec{r}\|^2$ and $\|T_\rho\|^2$ are square norms in Hilbert-Schmidt space and $\lambda_{max}(\vec{r}.\vec{r}^T + T_\rho.T_\rho^T)$ is the maximum eigenvalue of matrix $(\vec{r}.\vec{r}^T + T_\rho.T_\rho^T)$. The formulation of geometric discord was further generalized to the case of d⊗d dimensional systems [Luo and Fu, 2010]. Quantum discord has also received much attention in studies involving fuzzy measurement [Vedral, 2003], broadcasting [Piani *et al.*, 2008; Luo and Sun, 2010], complementarity and monogamy relationship between classical and quantum correlations [Oppenheim *et al.*, 2003; Badziag *et al.*, 2003; Koashi and Winter, 2004], dynamics of discord [Maziero *et al.*, 2009; Mazzola *et al.*, 2010], operational interpretations of quantum discord in terms of state merging [Madhok and Datta, 2011; Cavalcanti *et al.*, 2011] and teleportation fidelity [Adhikari and Banerjee, 2012], and the relation between discord and entanglement [Yang *et al.*,

2005; Streltsov *et al.*, 2011; Cornelio *et al.*, 2011; Piani *et al.*, 2011; Seshadreesan *et al.*, 2015; Zou and Fang, 2016; Lee and Li, 2017; Yuan *et al.*, 2018]. The concept of discord is also extended for multi-dimensional, tripartite or multipartite systems for studying the nature of nonlocal correlations in different multi-dimentional and multiqubit entangled classes [Liu *et al.*, 2015b; Chanda *et al.*, 2015; Beggi *et al.*, 2015; Jakóbczyk *et al.*, 2016; Cheng and Hall, 2017; Jebaratnam *et al.*, 2017].

1.5 QUANTUM INFORMATION PROCESSING: APPLICATIONS

A lot of protocols and techniques are developed using the laws of quantum mechanics that can be used to solve a variety of interesting problems in the area of computer science and information technology. Using these protocols assisted by entangled resources, one can achieve efficient, secure and optimal communication in comparison to the use of classical resources. Some of interesting problems of computer science and engineering are order-finding problem, factoring problem, optimum searching, and information security etc. which can be efficiently solved using quantum algorithms. Similarly, there are efficient protocols to transmit classical and quantum information from one remote location to another, or to exchange cryptographic keys- some of which we will discuss in the following sub-sections.

1.5.1 Quantum Teleportation

Quantum teleportation is a quantum mechanical phenomenon to transport an unknown quantum state from one remote location to another using a previously shared entanglement assisted with classical communication between a sender and a receiver. It can be considered as a very efficient and secure process to transfer quantum information between the users in a protocol as the possibility of intercepting the information by an eavesdropper after a secure distribution of entanglement is negligible. The security, therefore, is very fundamental to the basic concept of teleportation as the quantum information is sent without physically transporting the information through a medium or without measuring the information content on either side of the transport.

The teleportation protocol was proposed by Bennett *et al.* to teleport the state of a single-qubit using a shared two-qubit antisymmetric singlet state. In the original protocol [Bennett *et al.*, 1993], Alice wants to communicate an unknown information encoded in a single-qubit state $|\phi\rangle_1 = [\alpha|0\rangle + \beta|1\rangle]_1$, to Bob. The laws of quantum mechanics prevent Alice to perform any measurement on the unknown state to determine the information as the measurements will lead to collapse of wave function and the information will be lost. Therefore, in order to teleport an unknown state, Alice shares a two-qubit Bell state $|\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]_{23}$ with Bob such that qubit 2 is with Alice and qubit 3 is with Bob. Now, Alice performs a two-qubit Bell state measurement on the joint state of her qubits, i.e., qubit containing the unknown information and her share of the qubit forming the singlet state. The joint state of three-qubit system in terms of Alice's measurement basis can be written as

$$\begin{aligned} |\psi\rangle_{123} &= \frac{1}{2}\left[|\psi^-\rangle_{12}(-\alpha|0\rangle_3 - \beta|1\rangle_3) + |\psi^+\rangle_{12}(-\alpha|0\rangle_3 + \beta|1\rangle_3) + |\phi^-\rangle_{12}(\alpha|1\rangle_3 + \beta|0\rangle_3)\right. \\ &+ \left.|\phi^+\rangle_{12}(\alpha|1\rangle_3 - \beta|0\rangle_3)\right] \end{aligned} \tag{1.31}$$

Clearly, if Alice's measurement outcome is $|\psi^-\rangle_{12}$ then Bob's qubit will be projected onto the state $\alpha|0\rangle_3 + \beta|1\rangle_3$, which is exactly the same state that Alice wanted to communicate. In all other cases, Bob requires to perform a standard single qubit unitary operation to retrieve the teleported state. For example, if Alice's measurement outcome is $|\psi^+\rangle_{12,}$ then Bob will have to perform a σ_z operation on his qubit to recover the original state. In this way, Alice can transmit an

unknown single-qubit state to Bob.

There are two important aspects, that one needs to consider for the teleportation protocol:

(1) Teleportation does not allow faster than light communication as the sender requires classical communication regarding her measurements to be transmitted to the receiver; and
(2) Teleportation does not violate the No-Cloning theorem as the teleported state is not a copy of the original state since the original state is destroyed at the sender's end.

Bennett *et al.* have further generalized the teleportation protocol to teleport an unknown qudit state using a maximally entangled state in $d \otimes d$ dimensional Hilbert space assisted with $2\log_2 d$ bits of classical communication. In addition, teleportation protocol under real experimental set-ups was also described, where the sender and receiver do not share a perfect Bell pair as the entangled pair is distributed through a noisy channel [Bennett *et al.*, 1996b]. Furthermore, the protocol was also demonstrated to be successful for continuous variables [Furusawa *et al.*, 1998].

The efficiency of an entangled resource to teleport an unknown state can be ascertained by using a measure that accounts for the extent of similarity between the unknown state to be teleported and the teleported state. Therefore, a measure of successful teleportation is formulated in terms of fidelity of teleportation which is an indicator of the overlap between input and output states, namely $F = \langle \psi_{in} | \rho_{out} | \psi_{in} \rangle$ [Horodecki *et al.*, 1996, 1999a; Yeo, 2006a; Kay *et al.*, 2009]. For example, only if the fidelity of teleportation $F > 2/3$, a two-qubit state is considered as a useful resource for quantum teleportation [Horodecki *et al.*, 1996; Bouwmeester *et al.*, 2000; Badzia g *et al.*, 2000; Verstraete and Verschelde, 2002; Bandyopadhyay, 2002; Oh *et al.*, 2002; Adesso and Illuminati, 2005; Hu *et al.*, 2010; Taketani *et al.*, 2012; Pramanik and Majumdar, 2013; Qiu *et al.*, 2014; Adhikari and Kumar, 2016]. Clearly, for a perfect teleportation, the value of fidelity is unity and, in general, if two users in a protocol share a maximally entangled state, a unit fidelity teleportation can be achieved. For multiqubit systems, one can consider maximally entangled GHZ states [Greenberger *et al.*, 1989] to be useful resources for single-qubit teleportation [Karlsson and Bourennane, 1998]. However, if the shared entangled state is non-maximally entangled, teleportation may lead to fidelity less that the unity [Hillery *et al.*, 1999; Karlsson *et al.*, 1999; Shi *et al.*, 2000; Fang *et al.*, 2003; Xiao *et al.*, 2004; Shi and Tomita, 2002; Wang *et al.*, 2007b]. In multiqubit cases, one also encounters situations where a controller controls the amount of information between a sender and a receiver, e.g., if GHZ states are used as resources, Charlie can act as a controller for information transfer between Alice and Bob. For non-maximally entangled resources, such as W states, the teleportation is probabilistic and fidelity of teleportation depends on the parameters of the unknown state to be teleported [Shi and Tomita, 2002; Agrawal and Pati, 2002]. On the other hand, Agrawal and Pati proposed a new class of three-qubit W-type states for deterministic teleportation of a single-qubit by performing three-qubit joint measurements [Agrawal and Pati, 2006]. Moreover, non-maximally entangled states such as W and W_n -type states have been used extensively for teleportation of single as well as multiqubit information [Shi *et al.*, 2000; Li *et al.*, 2000; Agrawal and Pati, 2002; Albeverio *et al.*, 2002a; Yan and Wang, 2003; Gorbachev *et al.*, 2003; Fang *et al.*, 2003; Cao and Song, 2005; Gordon and Rigolin, 2006; Singh *et al.*, 2016]. Rigolin (2005), demonstrated a teleportation scheme for teleporting an arbitrary two-qubit state using direct product of two Bell states as a quantum channel [Rigolin, 2005]. A lot of other theoretical schemes of teleportation have been proposed in last three decades to teleport the single or multiqubit information using ideal as well as noisy channels [Braunstein, 1993; Brassard, 1996; Bandyopadhyay, 2000; Gorbachev and Trubilko, 2000; Henderson *et al.*, 2000; Hao *et al.*, 2000; Lee, 2001; Lloyd *et al.*, 2001; Joo *et al.*, 2003; Verstraete and Verschelde, 2003; Dai *et al.*, 2004; Deng, 2005; Deng *et al.*, 2005a; Leuenberger *et al.*, 2005; Dantan *et al.*, 2005; Yeo and Chua, 2006; Yeo, 2006b; Chen *et al.*, 2006; Zhang, 2006; Agrawal and Pati, 2006; Man *et al.*, 2007; Muralidharan and Panigrahi, 2008; Jung *et al.*, 2008a,b; Kumar and Krishnan, 2009; Hu, 2011; Qiu *et al.*, 2014; Li and Jin, 2016; Xiao *et al.*,

2016; Li *et al.*, 2016b; Mozrzymas *et al.*, 2018; Xu *et al.*, 2018].

In 1997, Bouwmeester demonstrated the first experimental realization of original teleportation scheme using parametric down-conversion technique to produce a pair polarization entangled photons. One of the major challenges in experimental teleportation is to identify and distinguish all the orthogonal set of states at the sender's end [Bouwmeester *et al.*, 1997]. The identification of all the four Bell states in teleportation protocol was proposed by Boschi *et al.* [Boschi *et al.*, 1998]. Further, teleportaion over inter-atomic distance was realized using solution state Nuclear Magnetic Resonance (NMR) [Nielsen *et al.*, 1998]. The protocol was also generalized for teleportation of atomic qubits [Barrett *et al.*, 2004]. Moreover, teleportation between objects of a different nature, i.e., light and matter was demonstrated by Sherson *et al.* (2006) [Sherson *et al.*, 2006]. Zhang *et al.* (2006) took a step forward to propose experimental teleportation of an arbitrary two-qubit state from a sender to a receiver [Zhang *et al.*, 2006]. In general, a number of experiments have been proposed to realize quantum teleportation of single as well as multiqubit information with higher fidelity and unit probability. [Bouwmeester *et al.*, 1997; Braunstein and Kimble, 1998; Kok and Braunstein, 2000; Shih, 2001; Kim *et al.*, 2001a; Lombardi *et al.*, 2002; Bowen *et al.*, 2003; Pan *et al.*, 2003a; Fattal *et al.*, 2004; Yonezawa *et al.*, 2004; Huang *et al.*, 2004; Zhang *et al.*, 2006; Herbst *et al.*, 2015; Takesue *et al.*, 2015a; Pirandola *et al.*, 2015; Wang *et al.*, 2015; Sun *et al.*, 2016; Valivarthi *et al.*, 2016; Singh *et al.*, 2016]

1.5.2 Quantum dense Coding

Quantum dense coding is one of the simplest and elementary application of quantum information processing which utilizes quantum entanglement to enhance the information content, communicated between two distant users. Hence, quantum dense coding is an efficient protocol to prove that entanglement is not only the fundamental resource in quantum communication but it also enhances the channel capacity for classical communication. For example, in dense coding if Alice and Bob share a bipartite entangled state, then by locally manipulating only her qubit, Alice can send two-bit information to Bob. In the original protocol [Bennett and Wiesner, 1992], Alice shares a two-qubit Bell state $|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]_{12}$ with Bob such that qubit 1 is with Alice and qubit 2 is with Bob. In order to communicate a two-bit information, Alice performs one of the four unitary operations given by identity I^1, or Pauli operators $(\sigma_x^1, \sigma_y^1, \sigma_z^1)$ locally on her qubit. Using these four unitary operations, Alice essentially maps the originally shared state with Bob to one of the four maximally entangled two-qubit states depending on what information she wants to communicate. For example, depending on whether she wants to transmit 00, 01, 10, or 11, Alice will transform $|\phi^+\rangle_{12}$ into different Bell states as represented in Table 1.1. After

Table 1.1 : A scheme to map the originality shared state to four Bell states

$00 : \|\phi^+\rangle_{12} \xrightarrow{I^1} \|\phi^+\rangle_{12} = \frac{\|00\rangle_{12}+\|11\rangle_{12}}{\sqrt{2}}$	$01 : \|\phi^+\rangle_{12} \xrightarrow{\sigma_z^1} \|\phi^-\rangle_{12} = \frac{\|00\rangle_{12}-\|11\rangle_{12}}{\sqrt{2}}$
$10 : \|\phi^+\rangle_{12} \xrightarrow{\sigma_x^1} \|\psi^+\rangle_{12} = \frac{\|01\rangle_{12}+\|10\rangle_{12}}{\sqrt{2}}$	$11 : \|\psi^+\rangle_{12} \xrightarrow{\sigma_y^1} \|\phi^-\rangle_{12} = \frac{\|01\rangle_{12}-\|10\rangle_{12}}{\sqrt{2}}$

performing the requisite operation, Alice sends her qubit to Bob. After receiving her qubit, Bob performs a joint measurement in Bell basis on qubits 1 and 2, to distinguish the four Bell states. By performing Bell state measurements (BSM), Bob determines the state which Alice has prepared, and thus decodes the two-bit classical information which Alice wanted to communicate. In general, if Alice and Bob share a $2N$ qubit entangled state, then Alice can map the original state to 2^{2N} entangled states. This will allow her to transmit $2N$ bits of classical information by creating 2^{2N} distinct messages for Bob who can, in principle, distinguish between the messages as the entangled states will be orthogonal to each other. More generally, a sender can transmit $2log_2 d$ classical bits to

a receiver using quantum dense coding protocol using a shared maximally entangled state of $d \otimes d$ dimensional Hilbert space. It is important to note that using the classical protocol one can only transmit N-bit information if the sender has a N bit state. Quantum dense coding is also known as super dense coding if single qubit unitary operations are restricted to identity and Pauli operators.

The first experimental realization of quantum dense coding for sending the classical information was demonstrated in 1997 by Mattle *et al.* [Mattle *et al.*, 1996]. Subsequently, Fang *et al.* (2000) proposed experimental dense coding using NMR techniques [Fang *et al.*, 2000]. In addition, Bose *et al.*, proposed an experimental quantum dense coding scheme with non-maximally entangled resources and they further analysed a case where the shared entangled state is a mixed state [Bose *et al.*, 2000]. For multiqubit systems, Alice can transmit 3-bit information to Bob by locally manipulating her two qubits of the shared three-qubit GHZ state [Lee *et al.*, 2002; Wójcik and Grudka, 2003]. Further, Hao *et al.* (2000) proposed a theoretical scheme for controlled superdense coding in which a controller named Charlie, controls the amount of information communicated between Alice and Bob [Hao *et al.*, 2001]. There are several theoretical and experimental schemes for optimum communication involving dense coding using different entangled systems [Mattle *et al.*, 1996; Shimizu *et al.*, 1999; Hao *et al.*, 2001; Choi, 2001; Cereceda, 2001; Ralph and Huntington, 2002; Hiroshima, 2002; Lee *et al.*, 2002; Mermin, 2002; Gorbachev *et al.*, 2002; Liu *et al.*, 2002; Jing *et al.*, 2003; Wójcik and Grudka, 2003; Akhavan and Rezakhani, 2003; Bruß *et al.*, 2004; Rigolin, 2004; Schaetz *et al.*, 2004; Mozes *et al.*, 2005; Pati *et al.*, 2005; Mozes *et al.*, 2005; Wang *et al.*, 2007a; Hwang *et al.*, 2011; Shadman *et al.*, 2011; Tsai *et al.*, 2011; Li, 2012; Saha and Panigrahi, 2012; Horodecki and Piani, 2012; Shadman *et al.*, 2012, 2013; Prabhu *et al.*, 2013; Sazim and Chakrabarty, 2013; Das *et al.*, 2014; Lee *et al.*, 2014; Das *et al.*, 2015; Roy and Ghosh, 2015; Kögler and Neves, 2017; Roy *et al.*, 2017]. For evaluating the dense coding capacity of a quantum state, Barenco *et al.* derived an analytical expression [Barenco and Ekert, 1995; Hausladen *et al.*, 1996; Bowen, 2001] such that the maximum amount of information that can be sent using an entangled state is given as

$$C_{max} = log_2 D_A + S(\rho^B) - S(\rho^{AB}) \tag{1.32}$$

where D_A is the dimension of Alice's subsystem, ρ^{AB} is the density operator of the shared entangled state, ρ^B is reduced density operator corresponding to Bob's qubit, and $S(\rho)$ is the von-Neumann entropy.

1.5.3 Entanglement Swapping

Entanglement swapping is a protocol for entangling qubits that have neither come through the same source nor interacted with each other in the past [Bennett *et al.*, 1993; Zukowski *et al.*, 1993]. It can be regarded as an elementary application of quantum mechanics for mutual exchange of entanglement between qubits associated with different entangled states. In order to understand the basic premise, let us assume that Alice has a two-qubit entangled state $|\psi^-\rangle_{14} = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]_{14}$. In addition, Alice also shares an entangled pair $|\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]_{23}$ with Bob such that qubit 2 is with Alice and qubit 3 is with Bob. Now if Alice performs a Bell state measurement on her qubits 1 and 2 then the joint state of qubits 3 and 4 will be projected onto one of the four possible Bell states with a given probability. For example, the joint state of four qubits can be expressed in terms of Alice's measurement basis as $|\psi\rangle_{1234} = \frac{1}{2}[|\psi^+\rangle_{12}|\psi^+\rangle_{43} - |\psi^-\rangle_{12}|\psi^-\rangle_{43} - |\phi^+\rangle_{12}|\phi^+\rangle_{43} + |\phi^-\rangle_{12}|\phi^-\rangle_{43}]$, i.e., if Alice's measurement outcome is $|\psi^-\rangle_{12}$ with a probability of 1/4, then she will share $|\psi^-\rangle_{43}$ state with Bob. Interestingly, qubits 3 and 4 belong to two different entangled states, but after a standard BSM, these qubits are now entangled with each other even without interacting with each other. Hence, the entanglement which was between qubits 1 and 4 and qubits 2 and 3 is now swapped between qubits 1 and 2 and qubits 3 and 4. Thus, the process of entangling qubits which neither came from

the same source nor interacted with each other in the past is termed as entanglement swapping. Entanglement swapping protocol to manipulate a multipartite system has been proposed by Bose *et al.* in 1997 [Bose *et al.*, 2000]. The concept finds its applications in quantum repeaters [Briegel *et al.*, 1998], quantum secret sharing [Hillery *et al.*, 1999; Karimipour *et al.*, 2002; Zhang and Man, 2005], generation of Greenberger-Horne-Zeilinger (GHZ) states [Zeilinger *et al.*, 1997; Bose *et al.*, 1998], and other quantum communication protocols [Zhong-Xiao *et al.*, 2005; Zhou *et al.*, 2005; Man *et al.*, 2006; Dong *et al.*, 2008]. Similar to quantum teleportation, continuous variable entanglement swapping [Polkinghorne and Ralph, 1999; Abdi *et al.*, 2014; Takeda *et al.*, 2015], and probabilistic entanglement swapping using non-maximally entangled resources have also been suggested [Polkinghorne and Ralph, 1999]. Experimental realization of entanglement swapping was first demonstrated by Pan *et al.* in 1998 using two pairs of EPR states [Pan *et al.*, 1998]. A number of experimental implementations have been suggested since then by different groups, using nuclear magnetic resonance (NMR) [Boulant *et al.*, 2003], trapped ions [Riebe *et al.*, 2008], and photons of the telecom wavelength range [Jin *et al.*, 2015]. Furthermore, a lot of development has happened in the area of entanglement swapping on theoretical as well as experimental front [Lu and Guo, 2000; Boulant *et al.*, 2003; Song, 2003; Glöckl *et al.*, 2003; Zhang and Man, 2005; Short *et al.*, 2006; Riebe *et al.*, 2008; Hu and Rarity, 2011; Sangouard *et al.*, 2011; Chen and She, 2011; Qu *et al.*, 2011; Gao *et al.*, 2011; Ma *et al.*, 2012; Lin and Hwang, 2013; Wang *et al.*, 2013; Megidish *et al.*, 2013; Khalique *et al.*, 2013; Song *et al.*, 2014; Torres *et al.*, 2014; Roa *et al.*, 2014; Khalique and Sanders, 2014; Jin *et al.*, 2015; Ye, 2015; Kirby *et al.*, 2016; Pakniat *et al.*, 2017]

1.5.4 Quantum Algorithms

Quantum algorithms offer an increase in computational speed and space with the size of system over classical algorithms [Montanaro, 2016]. In early 1982, Richard Feynman observed that efficient simulation of certain quantum mechanical effects on classical computer is far too difficult [Feynman, 1982]; it prompted researchers and experimentalists to formulate and analyse quantum algorithms than can run on a quantum computer [Deutsch, 1989; Shor, 1994; Grover, 1996; Ekert and Jozsa, 1998; Zalka, 1999; Aharonov and Ta-Shma, 2003; Chi *et al.*, 2006; Hallgren, 2007; Childs and van Dam, 2010; Jordan *et al.*, 2012; Hen, 2014; Wiebe *et al.*, 2015]. Such algorithms are difficult to design but can be efficiently used to solve the computation problems which are not feasible on a classical computer with increasing problem size, and by considering the measures such as time or memory usage. In general, quantum algorithms are classified in three different classes [Nielsen and Chuang, 2010; Bacon and van Dam, 2010; Smith and Mosca, 2012; Montanaro, 2016]. First class of algorithms is based on the Fourier transformation and used to solve many complex problems over classical computers. Deutsch-Jozsa algorithm was first well defined quantum algorithm that uses the Fourier transformation to achieve a speed-up of a quantum computer over classical computers [Deutsch, 1989; Jozsa, 1998; Schulte-Herbrüggen *et al.*, 2005; Adcock *et al.*, 2009]. Deutsch-Jozsa algorithm solves the balancing problem with one evaluation, whereas any deterministic classical algorithm requires $2^N/2 + 1$ evaluations to solve the same problem [Deutsch, 1989; Deutsch and Jozsa, 1992]. Similarly, in 1994, Peter Shor also demonstrated a quantum algorithm to solve the problem of discrete logarithm and integer factorization in polynomial time [Shor, 1994, 1999]. The second class of quantum algorithms is quantum search algorithm. A quantum search algorithm, also known as Grover's algorithm, takes $O(\sqrt{N})$ evaluations to search an element from unordered set of elements, whereas the best classical algorithm takes $O(N)$ evaluations [Grover, 1996, 1997; Zalka, 1999]. The third class of algorithms is known as quantum simulations- many algorithms for quantum simulation have been proposed for Hamiltonians [Aharonov and Ta-Shma, 2003; Wiebe and Childs, 2012], open quantum systems [Kliesch *et al.*, 2011], and quantum field theory [Jordan *et al.*, 2014].

There are several other algorithms proposed by different groups for the development of theoretical and experimental quantum computation in diverse academic spaces [Abrams and

Lloyd, 1997; Chi *et al.*, 2006; Berry *et al.*, 2007; Aminian *et al.*, 2008; Bacon and van Dam, 2010; Bruß and Macchiavello, 2011; Chang *et al.*, 2015; Lloyd *et al.*, 2016; Ambainis, 2016].

1.5.5 Quantum Cryptography

Cryptography can be considered as a branch of a broader discipline known as Cryptology. In general, cryptography can be classified into symmetric and asymmetric cryptography [Stallings, 2003; Forouzan and Mukhopadhyay, 2011]. The two processes can be distinguished from one another in terms of keys used to encrypt and decrypt the data. For example, in symmetric cryptography only one key is used to encrypt and decrypt the data, but in asymmetric cryptography one key is used to encrypt and the another key is used to decrypt the message. For the very reasons of increased key domain and increased complexity, asymmetric cryptography is considered as more secure in comparison to symmetric cryptography [Diffie and Hellman, 1976; Rivest *et al.*, 1978].

Quantum cryptography or quantum key distribution (QKD) uses the fundamental laws of quantum mechanics to ensure secure transmission of private information over the public channel. In 1983, Wiesner proposed the basic concept of quantum cryptography asserting that an entangled state could be used as a kind of inauthentic-proof money if one can store it for a long period of time [Seth *et al.*, 1983]. Following the development, Bennett and Brassard proposed a noble protocol, known as BB84 protocol for creating a key between a sender and a receiver to establish secure communication using the classical private cryptography [Bennett Ch and Brassard, 1984; Bennett and Brassard, 2014]. Bennett, Brassard, and Robert further described the concept of privacy amplification which is used to increase the security of quantum key distribution [Bennett *et al.*, 1988]. Since then, a large number of efficient quantum key distribution protocols have been invented [Ekert, 1991; Bennett, 1992; Goldenberg and Vaidman, 1995; Long and Liu, 2002; Deng *et al.*, 2003; Zhou *et al.*, 2004; Renner, 2008; Scarani *et al.*, 2009; Branciard *et al.*, 2012; Braunstein and Pirandola, 2012; Lo *et al.*, 2014; Chau, 2015]. Moreover, Bennett *et al.* have also implemented quantum cryptography scheme successfully on the experimental front [Bennett *et al.*, 1992]. The experimental demonstration of BB84 protocol was further developed by Bethune and Risk [Bethune and Risk, 2000]. Muller, Zbinden and Gisin demonstrated quantum cryptography using a 23 km long installed standard optical cable under Lake Geneva [Muller *et al.*, 1996]. Several protocols of quantum cryptography have been theoretically and experimentally analysed to establish the validity of such protocols [Buttler *et al.*, 1998; Pan *et al.*, 2001a; Cai and Li, 2004; Lemelle *et al.*, 2006; Noh *et al.*, 2009; Weedbrook *et al.*, 2012; Brida *et al.*, 2012; Barrett *et al.*, 2013b; Shukla *et al.*, 2013; Buhrman *et al.*, 2014; Takesue *et al.*, 2015b; Chau, 2015; Diamanti *et al.*, 2016; Li *et al.*, 2016a; Zhu *et al.*, 2017; Islam *et al.*, 2017; Collins *et al.*, 2017].

1.6 SCOPE OF THE THESIS

As discussed above, quantum entanglement and nonlocal correlations are used as essential ingredients not only for describing and analysing the foundational aspects of quantum mechanics but also as resources to implement many efficient and optimal protocols in quantum information and computation. Considering the importance of entanglement and nonlocality for information and communication protocols, a lot of theoretical and experimental progress has been made in last three decades towards the development of this area. However, there are many aspects which still require a much better physical interpretation to understand the nature of quantum correlations in bipartite and multiqubit systems. For example, there are mixed entangled systems which are entangled but do not violate the Bell inequality or the failure of multiqubit Bell-type inequalities to identify nonlocal correlations in a large set of entangled states- the non-violation of such inequalities definitely raises questions over the usefulness of such resources in quantum information and computation. The nature of quantum correlations becomes even more

complicated under real noisy conditions. This Thesis is an attempt to readdress the question of analysing the usefulness of quantum correlations under noisy conditions using the applications of weak measurements in two- as well as in multiqubit systems. For this, we analyse the Bell inequality for two-qubit systems, and the Svetlichny inequality for three- and four-qubit systems. In the present work, we further modify the Bell and Svetlichny inequality using statistical correlation coefficients to detect and characterize nonlocal correlations in entangled systems where other Bell-type inequalities fail to detect nonlocality. In addition, we also consider to analyse the efficiency of nonlocal correlations under biased experimental set-up, i.e., for a nonlocal game or a class of Bell-CHSH inequalities where both Alice and Bob choose their measurements with a certain probability. Furthermore, we also propose a four-qubit non-maximally entangled state for efficient information transfer and generalize the proposed state to be used as a resource for quantum information processing. This thesis is organized in 7 chapters and the content of each chapter is described briefly as follows.

In **chapter-1**, we discuss some of the basic concepts associated with quantum information and processing and provide a brief review of the literature related to the problems considered in this thesis.

In **chapter-2**, we analyse nonlocal correlations in bipartite entangled systems under different noisy conditions using applications of weak measurement and its reversal operations. In order to compute nonlocality in the evolved two-qubit state under noisy conditions, we establish an analytical result between the Bell-CHSH inequality, the state parameter, noise parameters, and a parameter representing strength of weak measurement and its reversal operations. The analysis also allows us to propose a class of two-qubit mixed entangled states for efficient quantum information processing. We further determine the usefulness of proposed states using various measures such as teleportation fidelity, singlet fraction, linear entropy and dense coding channel capacity. Interestingly, our results show that the proposed states are better resources in comparison to a large set of pure and mixed two-qubit states.

Based on above results we extend our analysis in **chapter-3** to investigate the effect of noise and weak measurements on nonlocal correlations in different classes of multiqubit maximally and non-maximally entangled states. Similar to the two-qubit case, here we derive an analytical expression between the three- and four-qubit Svetlichny inequalities, the state parameter, noise parameters, and strength of weak measurement and its reversal operations. As in the previous case, we use examples of amplitude-damping, phase-damping, and depolarizing noise. Our results indicate that more correlations in the initially prepared state do not always guarantee more correlations in the finally shared state. We further analyse entanglement properties of the finally shared three- and four-qubit states using three- and four-qubit negativity of the finally shared states. In all the above cases our analytical results give excellent agreement with the numerical results.

In **chapter-4**, we modify the two-qubit Bell-CHSH inequality and the three-qubit Svetlichny inequality using correlation coefficients which are considered as indicators of correlations between qubits. Using our approach, we analyse two- and three-qubit pure and mixed entangled states for violation of modified inequalities. We extend our analysis by establishing an analytical relation between the modified Bell inequality and maximum and minimum value of geometric discord. Our results suggest that correlation coefficients can be used as an emerging tool for characterizing nonlocal properties of a quantum system. We demonstrate the utility of modified inequalities as quantifiers of entanglement and nonlocality in bipartite mixed entangled states and three-qubit pure entangled states.

In **chapter-5**, we proceed to analyse the efficiency of nonlocal correlations under biased