1
Preliminaries and literature survey

Do not worry about your difficulties in Mathematics. I can assure you mine are still greater.

—Albert Einstein

Young man, in mathematics you don't understand things. You just get used to them.

— Von Neumann

1.1 INTRODUCTION

The discussions surrounding quantum computing gained momentum with the proposal of a quantum computer coined by Richard Feynman in 1982. Since then, the theoretical proposal has evolved into several practical and useful quantum algorithms, secure cryptographic protocols, and potential applications in quantum information and computation leading to a competing research in the development of a practical quantum computer. Soon after Feynman's proposal, the analysis of quantum money proposed by Wiesner in 1983 merged two diverse fields of game theory and quantum computation, which further inspired the scientific community to explore various dimensions of quantum game theory. In fact the first instance of investigating a relation between quantum mechanics and game theory was discussed by Blaquiere in 1980. The basis of theory probably received inspiration from the algorithmic advantages offered by quantum computing over classical computers. The introduction of Shor's algorithm for efficient factorization of prime numbers, Grover's algorithm for faster database search as against the best classical search algorithms, and quantum error correction paved a way for the realization of a feasible quantum computer. In last two decades, quantum games and quantum algorithms are being witnessed as similar concepts with varied outlook. In fact, the discovery of newer quantum games became an easier way of visualizing and formulating novel quantum algorithms, leading to further advancement in quantum computation.

The research domain of quantum game theory found a very strong base probably in 1999 with the seminal contribution from Eisert *et al.* and Meyer. The theory is an extension of classical game theory in quantum realm aided with superposition principle, entanglement between qubits, and superposition of strategies performed by players in a game. In general, the theory analyses situations where quantum strategies result either in a clear win for quantum players or studies inherent benefits to quantum players, which are otherwise not possible using classical strategies. Apparently, the presence of entanglement and nonlocality, and availability of superposition of strategies offered by quantum mechanics to quantum players lead to the dominant performance of quantum players in a game in comparison to classical players. The physical interpretation of advantages obtained using quantum theory has always been a subject of interesting discussions and debates among physicists and a matter of *weirdness* to non-physicists. Moreover, complexity being central to the basic premise of quantum theory further increases the degree of intricacy to analyse a protocol or situation enormously, with the increase in number of qubits, quantum operations, and interventions in a scenario. This increased degree of complexity with the evolution of quantum systems and strategies can be dealt efficiently with the notion of a quantum game. Therefore, the idea of representing nonlocality, quantum cryptographic protocols, eavesdropping, and cloning as games is gaining significant interest in the community with an aim to effectively understand and analyse such quantum phenomena. For example, the game-theoretic perspective of BB84 protocol- an important quantum key distribution protocol- led to examine mixed strategy Nash equilibrium strategies and payoffs of players (sender, receiver, eavesdropper) involved in the communication protocol. The analysis further arose intrigue to study other communication protocols in the framework of game theory, and thus paved a way for evaluating stable equilibrium points for these protocols. In addition, the game-theoretic analysis also finds its application in investigating the adverse affects of decoherence during distribution of entanglement, thereby contributing towards characterizing the efficiency of a quantum resource for practical implementations.

One of the important dimensions of game theory is Bayesian games- games with incomplete information- which have shown to possess direct correspondence with Bell-type inequalities. Therefore, the element of incompleteness in a Bayesian game setting has a direct relation with the local hidden variable theories. In view of the above, Bayesian games play an important role in representation of non-local correlations in quantum systems. On similar lines, various nonlocal games have been proposed and analysed to enhance the basic understanding and role played by entanglement and nonlocality in quantum computing. Bayesian games can be categorized as of two different types- ones where players possess common interests and others where players possess conflicting interests in a game. Interestingly, both type of games showcase the correspondence of non-local game settings with different bipartite and multi-qubit Bell-type inequalities; and also demonstrate the usefulness of quantum strategies over their classical counterparts.

In general, maximal entanglement, nonlocality and quantum strategies offer an edge to quantum players over classical players. However, different classes of entangled states may or may not offer quantum benefit as resources in different games. This may be attributed to different parameters, rules and settings of a game. For example, the use of a quantum state may be useful in winning a particular game; the similar analysis however may be very different for another game set-up. Hence, studying the role of different maximally and non-maximally entangled pure and mixed states for quantum games or quantum cryptography protocols will be a worthwhile contribution for understanding the fundamentals of theory and designing large-scale efficient quantum communication protocols.

1.2 BASIC TERMINOLOGIES AND CONCEPTS IN QUANTUM INFORMATION PROCESSING

In this section, we describe basic terminology and fundamental concepts to facilitate the discussion of the results obtained in this Thesis from Chapter 2 onwards.

1.2.1 Qubits and quantum states

The fundamental unit of classical computation and information processing is a bit. In quantum information and computation, there is an analogous concept known as a quantum bit or qubit in short for convenience [Rieffel and Polak, 2000; Spiller *et al.*, 2005; Nielsen and Chuang, 2011]- Qubit is the fundamental unit of all quantum information processing tasks, and inherently very different from a bit. For example, a classical bit can be in one of the two possible states, either 0 or 1; whereas a qubit in addition to its existence in states $|0\rangle$ and $|1\rangle$ can also exist in an arbitrary linear superposition of $|0\rangle$ and $|1\rangle$, such that

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

where α and β are two complex numbers. The wave function ψ in Eq. (1.1) is a mathematical representation of the state of a qubit and it contains all the information about the preparation of the qubit. Due to the measurement problem and statistical nature of quantum mechanics, if one measures the state of a qubit, the outcome is not deterministic. In fact the outcome is probabilistic, determined by the value of coefficients α and β. Clearly, if a measurement is performed on the qubit $|\psi\rangle$, one can find it to be either in the state $|0\rangle$ with a probability of $|\alpha|^2$ or in the state $|1\rangle$ with a probability of $|\beta|^2$. Since, the sum of total probability should be 1, one requires $|\alpha|^2 + |\beta|^2 = 1$ for all qubits. The above condition further ensures that qubit is always normalized to unit length.

In the above description for the state of a qubit, "$|\ \rangle$"- following the Dirac's notation- represents a ket vector which is an algebraic representation of a quantum state under study [Sakurai and Napolitano, 2017]. Precisely, a ket represents a column vector, and in its standard form, $|0\rangle$ and $|1\rangle$, which are also known as computational basis states represented as a 2×1 column vectors as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{1.2}$$

Therefore, the state of a qubit can be defined as a vector in a two-dimensional complex vector space. Such representations facilitate a smooth transition of wave mechanics to matrix mechanics, and the algebra can be easily done on a vector space, following similar mathematics of vector addition and scalar multiplication that any basic vector would follow. For example, the state of a qubit represented in Eq. (1.1) can alternatively be re-expressed as $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$. Similarly, an operator can be represented by a matrix to transform one form of the vector to other. In order to represent multiqubit systems, one requires to switch to higher dimensional vector spaces. The representation of vectors in a high dimensional space can be obtained by mathematically performing a tensor product of basis vectors in the lower dimensional space. For instance, two-qubit states $|jk\rangle$ can be represented as a tensor product of $|j\rangle$ and $|k\rangle$ where $|j\rangle$ and $|k\rangle$ are single qubit states expressed in Eq. (1.2), such that

$$\begin{aligned} |00\rangle &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\ |10\rangle &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned} \tag{1.3}$$

Similarly, one can obtain quantum states in higher dimensional vector spaces. In order to denote any n-qubit state, it can be written as a superposition of 2^n basis states

The general state for a two-qubit system can be expressed as $|\psi\rangle_{12} = \alpha|00\rangle_{12} + \beta|01\rangle_{12} + \gamma|10\rangle_{12} + \delta|11\rangle_{12}$. In a similar fashion, one can evaluate the representation of all basis states associated with higher dimensional vector spaces. An N-qubit state can be represented by a linear superposition of all 2^N basis states in N-dimensional vector space with the help of 2^N coefficients for each basis state. One of the celebrated consequences of the superposition principle is quantum parallelism [Lanzagorta and Uhlmann, 2008]. The fundamental concept of superposition allows one to store same amount of information that can be embedded in 2^N different classical numbers or coefficients using a single N-qibit quantum state in quantum registers, thus rendering exponential advantage in terms of time and space [Rieffel and Polak, 2000; Spiller *et al.*, 2005; Nielsen and Chuang, 2011].

As discussed above for a single qubit, the state can be defined as a linear superposition of computational basis states $|0\rangle$ and $|1\rangle$, where a basis set can be defined as to comprise of linearly independent orthogonal vectors spanning the vector space. Clearly, there can be more than one basis using which a two-level system can be defined. For instance, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ as shown in Eq. (1.2) and (1.4), respectively, can be two different basis sets for the representation of a single qubit system such that

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{1.4}$$

Therefore, if an arbitrary quantum state is measured in computational basis, then the qubit is measured in the basis $|0\rangle$ and $|1\rangle$ with respective probabilities $|\alpha|^2$ and $|\beta|^2$. However, if the same quantum state is measured in the basis set represented in Eq. (1.4), then the qubit is found to exist in $|+\rangle$ state with probability $\frac{|\alpha+\beta|^2}{2}$ or in $|-\rangle$ state with probability $\frac{|\alpha-\beta|^2}{2}$.

In order to represent a system, one requires a complete set of information regarding the initial conditions at a given instance and the forces acting on the system- such a complete description is represented by a wave function; and is possible only for observables whose operators have common set of eigen functions. If it is possible to represent a quantum system using a wave function, then the state of system is termed as a pure state. However, due to the restrictions imposed by Heisenberg Uncertainty Principle such a description of quantum systems with maximal information is not always possible. In all such cases, it is convenient to describe the state of a system using a statistical operator known as density operator ρ. Such statistical mixture can be expressed in form of a density operator [Fano, 1957, 1983; Blum, 2012], as

$$\rho = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i| \tag{1.5}$$

where "$\langle\ |$" is the Dirac notation for the transpose conjugate of a *ket* vector. A state enclosed in this notation is called a *bra*, which by definition can be represented using a row vector. Therefore, the representation of a density operator for a n-qubit state is nothing but a $n \times n$ square matrix. A pure quantum state is a special case of mixed state where $i = 1$, thus it is simply of the form $|\psi_1\rangle\langle\psi_1|$. Algebraically, a state ρ is defined as a pure state if $\mathrm{Tr}(\rho^2) = 1$. On the other hand, if $\mathrm{Tr}(\rho^2) < 1$, then the state is a mixed state. Here $\mathrm{Tr}(M)$ is the trace (sum of diagonal elements) of a matrix M. Hence, a density operator can be visualized as an effective mathematical tool to understand the properties and dynamics of a composite statistical ensemble. The representation further allows one to study and characterize the properties and correlation between the individual subsystems, which in general is not possible using a wave function approach. The density operator of a system has the following properties,

(i) The trace of a density operator is 1;

(ii) Its diagonal elements are non-negative real numbers; and

(iii) It is a positive semi-definite hermitian operator.

For example, the density operator for a single qubit system can be represented as $\rho = \frac{1}{2}\left[I + \overrightarrow{r}.\overrightarrow{\sigma}\right]$ where $\overrightarrow{r}$ is the polarization vector and $\overrightarrow{\sigma}$ are the Pauli spin projection operators. Clearly, the state is a pure state iff $\|r\| = 1$. By definition, the complete density operator of a quantum system contains all the information of its subsystems. A quantum state however may be distributed or shared between more than one parties. In order to know the state of a subsystem (let A) in a composite quantum system (let AB), partial trace is taken over the state of the remaining subsystem (let B).

For instance, consider the state of composite system to be represented by a density operator ρ_{AB}, then the reduced density operators for subsystems A can be defined as $\rho_A = \text{Tr}_B(\rho_{AB})$, where Tr_B represents the partial trace over subsystem B. 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 [Hall, 2013].

1.2.2 Quantum gates and circuits

The fundamental unit of classical computation is bits, i.e., 0 or 1. The information is represented and processed in forms of string of bits; and then there are logic gates and digital circuits to manipulate and transfer the information. The standard examples include NOT, AND, OR, XOR, NAND, NOR, and Toffoli gate. Similar to classical computation, a quantum computer works on an analogous concept where information is represented using qubits and manipulated using quantum gates and circuit diagrams. These gates are represented using operators which act on the state of a qubit to transform it from one form to another. Therefore, algebraically, gates or operators corresponding to them are represented by matrices. The only restriction quantum mechanics puts on these operators is to be unitary, i.e., if an operator is represented by a matrix U, then it can be represented by a quantum gate iff $UU^\dagger = 1$. In addition, quantum operators representing physical observables should have real eigen values, and therefore must be Hermitian. By definition, an operator $\widehat{O}$ is Hermitian if $\widehat{O} = \widehat{O}^\dagger$. Unlike the classical gates where one gives two inputs to receive one output (except for NOT gate)- resulting in irreversibility of these gates- quantum gates are reversible in nature due to the very property of being unitary. In this sub-section, we describe some important single and multiqubit gates and discuss their properties.

As discussed above, in a striking difference to classical gates where there is only one gate (NOT) which is reversible in nature, quantum computation comprises of many single and multiqubit gates which are reversible in nature. A single qubit gate can be represented by a 2×2 matrix that can map one form of the state of a qubit to another. Some standard single and two-qubit gates are as follows,

- **X Gate**: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ The X Gate is a quantum analogue of classical NOT gate, and is also known as the bit flip operator. As the name suggests, it flips the state of a qubit from $|0\rangle$ to $|1\rangle$ and from $|1\rangle$ to $|0\rangle$. For example, if a X Gate acts on the state of a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$, then it transforms the original state to $|\psi'\rangle = a|1\rangle + b|0\rangle$.

- **Z Gate**: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ The Z Gate is also known as a phase flip gate as it flips the phase of qubit $|1\rangle$ to $-|1\rangle$ while keeping the qubit $|0\rangle$ invariant. For example, if a Z Gate acts on the state of a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$, then it transforms the original state to $|\psi'\rangle = a|0\rangle - b|1\rangle$.

- **Y Gate**: $Y = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}$ The Y Gate is defined by a bit phase flip operator as it is a combination of X and Z operator i.e., if a Y Gate acts on the state of a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$, then it transforms the original state to $|\psi'\rangle = -a|1\rangle + b|0\rangle$; neglecting the overall phase.

- **Hadamard Gate**: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ Hadamard gate is considered as one of the most important single qubit gates as it can be used to create superposition of basis states. Precisely, the gate changes the qubits from computational basis to Hadamard basis as represented in Eq. (1.4), i.e., converts $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$.

Apart from single qubit gates, there are multi-qubit gates used for higher dimensional complex quantum systems. One of the prominent examples of a two-qubit gate is the 4×4 swap operator $SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ where the the basis states $|01\rangle$ and $|10\rangle$ are interchanged among themselves once the gate is operated on a two-qubit computational basis set. Further, another special class of two-qubit gates are the controlled gates. The controlled gates have two input bits-control bit and target bit. On the operation of the gate, the target bit remains unchanged if control bit is 0. On the other hand when control bit is 1, the specified unitary operator acts on the target bit, for the defined controlled-unitary operation. Few controlled gates that are commonly used for quantum computations are defined as follows:

- **Controlled NOT Gate :** $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
- **Controlled Pauli Z Gate :** $CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
- **Controlled Phase shift Gate :** $CS = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\imath\theta} \end{bmatrix}$

Here, we will briefly explain the action of controlled-NOT gate. It acts on the state of two qubits such that it leaves the target qubit as it is if the state of the control qubit is 0, but flips the state of the target qubit if the state of the control qubit is 1. For example, if a C-NOT gate operates on an arbitrary two-qubit state $\psi = a|00> +b|01> +c|10> +d|11>$, then the state evolves as $\psi' = a|00> +b|01> +c|11> +d|10>$. Clearly, the operation of a C-NOT gate can be summarized as $|x,y\rangle \rightarrow |x,x+y\rangle$.

Similarly, a *Toffoli* gate which is equivalent to Controlled-Controlled NOT operation, is an instance of a three-qubit gate. Its operation is defined as $|x,y,z\rangle \rightarrow |x,y,z \oplus xy\rangle$. Mathematically, the gate can be represented as a 8×8 unitary matrix. Toffoli gate along with Hadamard gate form a universal set of gates for quantum computations, thus making their experimental realization very crucial for implementing any quantum or classical operator [Barenco *et al.*, 1995a; Monz *et al.*, 2009; Huang *et al.*, 2017a; Cao *et al.*, 2018].

Considering their importance in quantum computation and information, quantum gates can be physically realized as quantum circuits operating on qubits in the same way as wired logic gates operating on classical bits [Barenco *et al.*, 1995a,b; Zhou *et al.*, 2000; Hammerer *et al.*, 2002; Brylinski and Brylinski, 2002]. The first realization of universal quantum logic gates was based on cavity quantum electrodynamics techniques [Sleator and Weinfurter, 1995]. Since then many quantum circuits have been designed using optical devices for feasible quantum computations [Milburn, 1989; Knill *et al.*, 2001; Koashi *et al.*, 2001; Ralph *et al.*, 2001]. Further, efficient teleportation method was utilized for designing various quantum gates [Gottesman and Chuang, 1999; Bartlett and Munro, 2003; Walther and Zeilinger, 2005]. Other important issues addressed were controlling decoherence in quantum gates [Protopopescu *et al.*, 2003; Zhao *et al.*, 2017] and designing circuits with high noise tolerance [Duan and Raussendorf, 2005]. This further led to different experimental demonstrations of high fidelity controlled NOT, controlled phase, controlled Z, Toffoli, and swap gates [Grigorenko and Khveshchenko, 2005; Isenhower *et al.*, 2010; Ukai *et al.*, 2011; Crespi *et al.*, 2011; Mičuda *et al.*, 2013, 2015; Meany *et al.*, 2016; Ferrando-Soria *et al.*, 2016; Bataille and Luque, 2019]. Moreover, successful experiments for multi-qubit quantum gates have also been performed [Babazadeh *et al.*, 2017; Russ *et al.*, 2018]. Recently, high fidelity single and two-qubit gates have been realized using quantum dots [Devra *et al.*, 2018], diamond defects [Huang *et al.*, 2019], and nanodiamonds [Chen and Yin, 2019].

1.3 ENTANGLEMENT AND NONLOCALITY

Ever since Einstein, Podolsky and Rosen raised the issue of completeness of quantum mechanics as a physical theory in 1935 [Einstein *et al.*, 1935], the nuances and fundamentals of quantum mechanics in the form of entanglement and nonlocality is being discussed, debated, and celebrated across diverse academic spaces throughout the globe. The concept of entanglement is very fundamental to the foundations of quantum mechanics, and is described as the characteristic trait of the complexity [Schrödinger, 1935, 1936]. It describes the correlations between the subsystem of a composite system. For example, if two or more than two qubits are entangled, then the properties of any of the subsystems depend on the properties of all other subsystems. Therefore, in an entangled system, the state of an individual subsystem cannot be defined with certainty, i.e., there is always an uncertainty associated with the states of individual subsystems- the state of individual subsystems will therefore be characterized using a mixed state density operator. David Bohm described correlations using a two-qubit antisymmetric state which was further characterized and used as a resource to understand many fundamental concepts in theory and to implement many potential applications in quantum information and computation [Bohm, 1952; Bohm and Aharonov, 1957]. Based on the EPR's arguement of locality and realism, John S. Bell designed an inequality which must be satisfied by systems whose correlations are local such that the properties of individual subsystems are not dependent on each other [Bell, 1964]. The inequality however was violated by systems whose correlations are spatially extended and hence, cannot be explained on the basis of locality and realism. The inequality was maximally violated by the two-qubit antisymmetric state, and therefore, the state is considered as a maximally entangled state. The violation of Bell inequality raised questions over the assumptions of elements of reality and locality, and clearly distinguished quantum systems as against their classical counterparts.

Therefore, entanglement can be described as a phenomena where the physical properties such as position, momentum, spin, or polarization of a particle are correlated with the properties of another particle even if they are spatially separated and do not interact with each other anymore.

1.3.1 Entanglement and its witnesses

Mathematically, a quantum state $|\psi\rangle_{AB}$ is entangled when it can be factorized as a tensor product of lower dimensional subsystems $|x\rangle_A$ and $|y\rangle_B$. For example, a system comprising two particles can be defined as

$$|\psi\rangle_{AB} = \sum_{xy} c_{xy} |x\rangle_A \otimes |y\rangle_B \tag{1.6}$$

where c_{xy} are complex numbers satisfying $\sum_{xy} |c_{xy}|^2 = 1$, and $|x\rangle_A$ is a subsystem associated with the Hilbert space H_A and $|y\rangle_B$ is a subsystem associated with the Hilbert space H_B. On the other hand, if a system can be factorized as a tensor product of individual subsystems of lower dimensions, then the state is termed as a product or a separable state. If $|\psi\rangle_{AB}$ cannot be factorized into the tensor product of $\sum_x c_x |x\rangle$ and $\sum_y c_y |y\rangle$ of subsystems x and y, respectively; then it is considered as an entangled state. Therefore, in an entangled sate, the variables of one of the subsystems depend on the variables of the other subsystem. Due to the very fundamental distinction of entangled systems in terms of nonlocal correlations as against classically correlated systems, such systems are used as resources to achieve tasks which are otherwise impossible by classical means. In last three decades, entangled systems have been used extensively for proposing and implementing many potential applications offered by quantum information and computation. Therefore, the classification and quantification of entanglement and nonlocal correlations become an integral part of the theory itself [Bennett, 1998]. Considering the technological challenges in generating and identifying different entangled systems, it is definitely expansive. Moreover, the entanglement cannot be increased by performing local operations and classical communication (LOCC), but it can be manipulated [Popescu, 1995; Bennett *et al.*, 1996b,c; Gisin, 1996; Raimond *et al.*, 2001] so as to aid performing certain tasks efficiently [Bennett and Wiesner, 1992; Bennett *et al.*, 1993; Żukowski *et al.*, 1993; Boström and Felbinger, 2002; Gisin *et al.*, 2002; Gisin and Fröwis, 2018]. Furthermore, entanglement also has its roots in the origin of important quantum cryptography protocols [Ekert, 1991], in addition to its connection with classical cryptography schemes such as secret key agreement [Gisin and Wolf, 1999; Collins and Popescu, 2002].

In general, a pure maximally entangled state possess maximum correlations between the qubits, which gets adversely affected once the state passes through a noisy channel. Therefore, once a quantum state is subjected to noisy environment, there is an inevitable need to protect it from decoherence by distilling a pure state from manipulated noisy entanglement [Popescu, 1995; Bennett *et al.*, 1996b]. The studies that evaluate mechanisms to protect correlations against noise further led to the discovery of error correcting codes [Shor, 1995; Steane, 1996a,b]. Moreover, a relation between entanglement distillation and quantum error correction was also established [Bennett *et al.*, 1996c]. Further, entanglement was also measured in terms of entanglement distillation [Bennett *et al.*, 1996a,b,c; Rains, 1999; Vidal *et al.*, 2002], and entanglement cost [Bennett *et al.*, 1996c; Hayden *et al.*, 2001], where entanglement cost describes number of bits that can be obtained as a private key by LOCC operations in the presence of a mischievous third party. Based on the distillation of entanglement, entanglement can also be defined as free and bound entanglement where free entanglement is the one which can be distilled and bound entanglement is the one that cannot be distilled. There are many instances in the literature where bound entanglement is studied in detail [Horodecki *et al.*, 1997, 1998; Bennett *et al.*, 1999b; Horodecki *et al.*, 1999; Bruß and Peres, 2000; Werner and Wolf, 2001; Sanpera *et al.*, 2001; Ishizaka, 2004; Yang *et al.*, 2005; Clarisse, 2006; Bruß and Leuchs, 2007; Horodecki *et al.*, 2009; Kaneda *et al.*, 2012; Vértesi and Brunner, 2014].

In order to quantify entanglement in a quantum state ρ, an acceptable measure of entanglement $E(\rho)$ must satisfy the following criteria [Vedral *et al.*, 1997; Wootters, 1998; Vidal, 2000; Bennett *et al.*, 1996c; Horodecki *et al.*, 2009],

(1) If ρ is a product state then $E(\rho) = 0$ and if ρ is a maximally entangled then $E(\rho) = 1$, i.e., the measure must vary between 0 and 1, for no entanglement and maximal entanglement, respectively.

(2) Monotonicity condition: The degree of entanglement in any state ρ should not increase under local operations and classical communication (LOCC)

(3) Convexity: The measure of entanglement must be a convex function, i.e., $E(\mu\rho + (1-\mu)\rho) \leq \mu E(\rho) + (1-\mu)E(\rho)$

(4) Additivity property: Amount of entanglement in n identical copies of the system must contain n times the amount of entanglement in the individual quantum state, i.e., $E(\chi^{\otimes n}) = nE(\chi)$

(5) The degree of entanglement must remain invariant of local unitary transformations, i.e., $E(\rho) = E(U\rho U^{\dagger})$

(6) The amount of entanglement of tensor product of two states should not be greater than the sum of entanglement of individual states, i.e., $E(\mu \otimes \nu) \leq E(\mu) + E(\nu)$

In addition to pure states, instances of mixed states possessing only classical correlations, mixed states which are not entangled but violate the Bell inequality [Modi *et al.*, 2012], and mixed states which are entangled but do not violate Bell inequalities [Werner, 1989; Horodecki *et al.*, 1995] elevated the importance of distinction between mixed states and separable ones. For this, Peres defined a criterion such that if the partial transpose of a quantum state ρ_{AB} with respect to qubit B

results in a positive operator having all non-negative eigenvalues, then the state ρ_{AB} is a separable state [Peres, 1996]. This criterion was considered as a necessary and sufficient condition to test separability in a $2 \otimes 2$ and $2 \otimes 3$ dimension quantum system [Peres, 1996; Horodecki *et al.*, 1996]. Even though the condition was experimentally challenging, the technique of partial transpose being a positive map is considered to be a good detector of entanglement. The experimental creation and detection of entanglement, however, are crucial ingredients in many information processing tasks. Therefore, one needs to consider efficient experimental ways to generate and detect entanglement. Interestingly, there exist class of entanglement witnesses which provide necessary and sufficient conditions to analyse entanglement present in an underlying system. These are Hermitian operators with at least one negative eigen value. The experimental detection of entanglement is facilitated by the fact that such witnesses can be decomposed in form of Pauli spin operators or Gell-Mann matrices (for higher dimensions) which are in fact experimentally realizable quantities. The concept of "entanglement witness" to detect entanglement was first introduced by Terhal [Terhal, 2000]. The entanglement present in a quantum state ρ can be detected by a witness operator W iff $\text{Tr}(W\rho) < 0$. Terhal further demonstrated a relation between the Bell inequality and entanglement witness; and described the Bell inequality as a non-optimal entanglement witness detecting entanglement as well as nonlocality [Terhal, 2000]. We now discuss some of the standard measures used for entanglement detection and characterization.

Entanglement measure based on distance

This classification is based on the premise that closeness of a state to a separable state is inversely related to the degree of entanglement. Therefore, minimum distance between the given state from a set of separable states is considered as a measure of entanglement [Vedral *et al.*, 1997; Vedral and Plenio, 1998], i.e.,

$$E_{D,S}(\rho) = \inf_{\sigma \in S} D(\rho, \sigma) \tag{1.7}$$

Here, the distance D between two states can also be interpreted in terms of fidelity for calculation of entanglement in mixed states using maximal success probability of Grover's search algorithm [Shapira *et al.*, 2006].

Convex roof measures

In general, using an entanglement measure, the entanglement for a pure state is first evaluated, and then the evaluation is extended to mixed states using the method of convex roofs [Uhlmann, 1998].

(a) The first convex roof measure we consider here is **Entanglement of Formation (EoF)** [Wootters, 2001]where the measure is defined in terms of a limiting ratio $\frac{n}{m}$ such that m copies of Bell states generate n copies of the pure state ψ [Bennett *et al.*, 1996c]. Alternately, EoF can also be defined as the von-Neumann entropy of any of the subsystems associated with the two-qubit pure state. For example, if $|\psi\rangle_{AB}$ is a two-qubit entangled state of qubits A and B then the EoF for the state $|\psi\rangle_{AB}$ can be given as $\text{EoF} = S(\rho_A) = S(\rho_B)$ where ρ_i is the reduced density operator for the i^{th} qubit and $S(\rho_i) = -\text{Tr}(\rho_i log_2 \rho_i)$ [Petz, 2001; Nielsen and Chuang, 2011]. Although the evaluation of EoF for a pure state is easy, and it can be extended for mixed states by the method of convex roofs, the calculation for mixed states is fairly complex [Chen *et al.*, 2005; Gühne *et al.*, 2007].

(b) Another important tool that distinguishes separable two-qubit states from entangled ones is **Schmidt numbers** or **Schmidt coefficients** [Schmidt, 1907; Ekert and Knight, 1995; Bennett *et al.*, 1996c; Terhal and Horodecki, 2000; Sanpera *et al.*, 2001; Sperling and Vogel, 2011a,b; Guo and Fan, 2015]. A pure two-qubit state $|\psi\rangle_{AB}$ in the composite Hilbert state $H_A \otimes H_B$ can be written in the Schmidt decomposition form as

$$|\psi\rangle_{AB} = \sum_{i}^{min(dim(H_A),dim(H_B))} \sqrt{\gamma_i}|i\rangle_A \otimes |i\rangle_B \tag{1.8}$$

where $\gamma_i \geq 0$ such that $\sum_i \gamma_i = 1$. These γ_i's are known as the Schmidt coefficients or numbers. For a separable state $|\psi\rangle_{AB}$, the Schmidt decomposition yields only one non-zero Schmidt number, which is not true for an entangled state. Thus, the mathematical framework of Schmidt decomposition and numbers is an efficient means to quantify the entanglement present in quantum states.

(c) We finally consider one of the most commonly used measures of entanglement namely, **Concurrence** [Hill and Wootters, 1997; Wootters, 1998, 2001]. The degree of entanglement in a two-qubit pure state using concurrence can be defined as

$$C(|\psi\rangle) = |\langle\psi|\sigma_y \otimes \sigma_y|\psi^*\rangle| \tag{1.9}$$

Here, ψ^* denotes the complex conjugate of the wave function representing the two-qubit entangled state. For example, the concurrence for a two-qubit state represented as $|\psi\rangle = cos\theta|00\rangle + sin\theta|11\rangle$ can be easily evaluated as $sin2\theta$. If the state of a system is represented by a density operator, i.e., $\rho = |\psi\rangle\langle\psi|$, then the concurrence can be re-expressed as $C(\rho) = \sqrt{2(1 - Tr(\rho_a^2))}$. Alternatively, for mixed quantum state ρ concurrence is also described as

$$C(\rho) = max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4) \tag{1.10}$$

where λ_i are the singular values of $\sqrt{\rho}\sqrt{\widetilde{\rho}}$ with $\widetilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$; and $\lambda_k > \lambda_{k+1}$ Concurrence can also be extended to characterize degree of entanglement in higher dimensional systems [Audenaert *et al.*, 2001b; Rungta *et al.*, 2001; Badziag *et al.*, 2002].

Various other measures of entanglement involving mixed state evaluation by convex roof means were also studied in detail [Sinolecka *et al.*, 2002; Fan *et al.*, 2003; Gour, 2005].

Apart from this, several methods of quantification of entanglement have been proposed, such as robustness measure [Vidal and Tarrach, 1999], and squashed entanglement [Tucci, 2002; Christandl and Winter, 2004]. Optimization of entanglement witness operators [Lewenstein *et al.*, 2000, 2001] and their minimization [Eisert *et al.*, 2007; Gühne *et al.*, 2007] was studied. Later, general numerical techniques of finding genuine multipartite entanglement were presented [Tóth *et al.*, 2009]. An optimal witness operator for bipartite mixed states could be further extended to multi-qubit quantum states [Park *et al.*, 2010].

Multipartite entanglement measures

Although few entanglement measures such as relative entropy [Vidal and Tarrach, 1999] can be generalized to multiqubit systems, classification and quantification of multipartite entanglement is a very complex yet an interesting problem [Cereceda, 2002; Collins *et al.*, 2002b]. The fact that the measures for two-qubit systems cannot be directly generalized to multiqubit systems can be attributed to the very nature of increased complexity in multiqubit systems with increasing number of qubits. For example, in a two-qubit entangled system, one needs to worry only about the entanglement between qubits A and B. However for a three qubit system, one not only needs to inquire regarding the entanglement between qubits A and B, but also needs to know the entanglement shared between AB as one single entity and the qubit C. One of the seminal contributions in this direction began with global entanglement, which is the sum of concurrences between a qubit and all other qubits [Meyer and Wallach, 2002]. Moreover, considering the importance of multiqubit systems several other measures were proposed to classify and quantify entanglement in such systems [Barnum and Linden, 2001; Eisert and Briegel, 2001; Wei and Goldbart, 2003; Herbut, 2004; Roscilde *et al.*, 2004, 2005; Facchi *et al.*, 2006; Yang *et al.*, 2009; Facchi *et al.*, 2009, 2010; Chen *et al.*, 2010; Modi *et al.*, 2010; Eltschka *et al.*, 2012; Eltschka and Siewert, 2012; Borsten, 2013; Wilde *et al.*, 2014; Gerke *et al.*, 2015; Li *et al.*, 2015; Pezzè *et al.*, 2017].

In this sub-section, we will consider few standard entanglement measures for three-qubit systems. The first measure to quantify degree of entanglement in a pure three-qubit system- a signature of genuine tripartite entanglement- is known as three-tangle (τ) or residual tangle. The three-tangle can be defined using a two-qubit entanglement measure, concurrence, as

$$\tau(P:Q:R) = C^2_{P:QR} - C^2_{PQ} - C^2_{PR} \tag{1.11}$$

where $C_{P:QR}$ represents the concurrence between the qubit P, with qubits Q and R taken together as one entity [Hill and Wootters, 1997; Wootters, 1998, 2001]. Moreover, entanglement followed another fundamental property of monogamy, which states that if two qubits P and Q share maximum amount of entanglement, then qubits P and Q cannot be entangled at all with a third qubit R [Coffman *et al.*, 2000; Bennett *et al.*, 1996c; Fanchini *et al.*, 2013; Farooq *et al.*, 2018; Gour and Guo, 2018; Guo and Gour, 2019].

In order to facilitate the discussions of three-tangle, we first briefly describe the two inequivalent classes of three-qubit entangled systems. Based on the propertied and classification, three-qubit entangled systems can be classified in two distinct and inequivalent classes, namely GHZ class and W class, represented as

$$|\psi_{GHZ}\rangle = sin\theta|000\rangle + cos\theta|111\rangle \tag{1.12}$$

and

$$|\psi_W\rangle = a|100\rangle + b|010\rangle + c|001\rangle, \tag{1.13}$$

respectively where $\theta \in (0, \pi/4)$ and $|a|^2 + |b|^2 + |c|^2 = 1$. The above two classes are termed as inequivalent as a state belonging to one of the classes cannot be converted to a state belonging to the other class by performing any number of local operations and classical communication (LOCC). Clearly, the nonequivalence between these two classes is a result of different entanglement properties of two classes. As a genuine tripartite entanglement measure, the value of three-tangle [Coffman *et al.*, 2000] varies between 0 for product states to 1 for states having maximum entanglement. For example, the three-tangle for a bi-separable state represented as $(a|0\rangle + b|1\rangle) \otimes (c|00\rangle + d|11\rangle)$ is 0 and for a standard GHZ state represented as

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{1.14}$$

is 1. In general, for the generalized GHZ state represented in Eq. (1.12), the three-tangle is $\sin^2 2\theta$. Therefore, as discussed above, for $\theta = 0$, the state is a product state, and hence τ is 0; and for $\theta = \frac{\pi}{4}$, the state is a maximally entangled state thus τ is 1. Similar to the standard GHZ state, the standard state in W class is represented by

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |001\rangle) \tag{1.15}$$

Although the standard W state possesses genuine three-qubit entanglement, the entanglement cannot be quantified using the three-tangle as an entanglement measure since for W class states $C^2_{A:BC} = C^2_{AB} + C^2_{AC}$ resulting in the value of three-tangle being 0 for this class. Thus, in order to capture and quantify entanglement in W class states, one can use an alternate measure of entanglement known as sigma [Emary and Beenakker, 2004], so that

$$\sigma(P:Q:R) = min\left(\frac{C^2_{P:QR}+C^2_{Q:PR}}{2}-C^2_{PQ}, \frac{C^2_{Q:PR}+C^2_{R:PQ}}{2}-C^2_{QR}, \frac{C^2_{P:QR}+C^2_{R:PQ}}{2}-C^2_{PR}\right) \tag{1.16}$$

On similar lines, another measure of entanglement, named negativity was introduced [Zyczkowski *et al.*, 1998]. It is expressed as the sum of negative eigen values of partial transpose of the two-qubit state in system AB with respect to a subsystem A or B. It is given as,

$$N(\rho_{AB}) = \frac{\|\rho^{T_B}\| - 1}{2} \tag{1.17}$$

where $\|\rho^{T_B}\| = \mathrm{Tr}(\sqrt{\rho^{T_B\dagger}\rho^{T_B}})$ is the trace norm and ρ^{T_B} is the partial transpose of the two-qubit state ρ_{AB} with respect to subsystem B. In order to make calculations and interpretations convenient, logarithmic negativity, which is $N_L(\rho_{AB})$ =log $_2\|\rho^{T_B}\|$ is used instead of standard negativity [Vidal and Werner, 2002]. Moreover, tripartite negativity can be evaluated to distinguish between separable, bi-separable, and genuine three-qubit entangled pure states [Sabín and García-Alcaine, 2008]. Further, the concept of negativity can also be extended to mixed states by convex roof method [Lee *et al.*, 2003].

In addition to the above measures, Lohmayer *et al.* further introduced a convex roof measure for evaluating entanglement in a mixture of GHZ and W type states [Lohmayer *et al.*, 2006]. Moreover, three-tangle was also generalized via hyperdeterminants for computing entanglement in multiparty systems [Miyake, 2003]. Miyake demonstrated that concurrence is a hyperdeterminant of first order, and similarly three-tangle is a hyperdeterminant of second order. Although finding hyperdeterminants of higher order is a complex procedure, this method results in entanglement measures which obey monotonicity condition [Miyake, 2004]. Lévay further elaborated the subject by deriving expression for hyperdeterminant entanglement measure for four qubit entangled systems [Lévay, 2006]. Although, there is no general methodology to compute degree of entanglement in an n-particle quantum states, there are several important contributions towards classification and quantification of multiqubit entanglement [Wong and Christensen, 2001; Collins *et al.*, 2002a,b; Cereceda, 2002; Wei and Goldbart, 2003; Pan *et al.*, 2003; Zhao *et al.*, 2003; Eibl *et al.*, 2003, 2004; Walther *et al.*, 2005; Eisert *et al.*, 2007; Bai *et al.*, 2009; Gühne and Tóth, 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; Brandão and Christandl, 2012; Chen *et al.*, 2012; Hyllus *et al.*, 2012; Zhao *et al.*, 2012; Barrett *et al.*, 2013; Sperling and Vogel, 2013; Bai *et al.*, 2014; Zhu and Fei, 2014, 2015; Islam *et al.*, 2015; Laflorencie, 2016; Hauke *et al.*, 2016; Zhao *et al.*, 2016; Hu *et al.*, 2016b; Cianciaruso *et al.*, 2016; Chen *et al.*, 2016; Buchholz *et al.*, 2016; Luo *et al.*, 2017; Gerke *et al.*, 2018; Che *et al.*, 2018; Deng and Deng, 2018; Haddadi and Bohloul, 2018]. In comparison to pure states, quantification of entanglement in mixed states is evidently a much more challenging task. However, despite the challenges due to increased complexity in this direction, a lot of significant studies have also been reported [Vedral and Plenio, 1998; Audenaert *et al.*, 2001a, 2002; Vidal and Werner, 2002; Lee *et al.*, 2003; Osborne, 2005; Mintert and Buchleitner, 2007; Zhang *et al.*, 2008; Park *et al.*, 2010; Ganguly *et al.*, 2014; Eltschka and Siewert, 2014; Deng and Deng, 2018].

1.3.2 Nonlocality

Quantum theory allows correlations between spatially separated particles that are fundamentally different from classical correlations. As the Bell inequality [Bell, 1964] puts an upper bound on the correlations compatible with local realistic theories, the violation of Bell inequality by pure two-qubit states confirms the presence of genuine nonlocal correlations between the two qubits. Moreover, studies in last few decades have confirmed that entangled quantum systems exhibit nonlocal correlations between qubits, which provide entangled resources an edge over classical resources for their efficient use in information processing, communication, and cryptography tasks. Therefore, the analysis of entanglement and nonlocality has gained significant interest from different quarters not only from the perspective of analysing the foundational aspects of theory, but also to design large-scale efficient quantum information and computation tasks.

The Bell inequality was later generalized to a much simpler form known as the Clauser, Horne, Shimony, and Holt (CHSH) inequality [Clauser *et al.*, 1969] as shown in Eq. (1.18).

$$|\langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle| \leq 2 \tag{1.18}$$

where A_1, A_2, B_1, and B_2 are the measurement operators, each associated to different physical observable. Here, A_i and B_i are the measurements performed on qubits 1 and 2, respectively; and can be defined as $A_1 = \sigma_1.\hat{a}$, $A_2 = \sigma_1.\hat{a'}$, $B_1 = \sigma_2.\hat{b}$, and $B_2 = \sigma_2.\hat{b'}$ where σ_i's are spin projection operators on respective qubits and $\hat{a}$, $\hat{a'}$, $\hat{b}$, $\hat{b'}$ are unit vectors. Clearly, the measurement outcomes of these operators yield values $+1$ or -1. Further, the CHSH inequality represented in Eq. (1.18) is an unbiased inequality, i.e., an inequality where measurement operators (A_1,A_2) and (B_1,B_2) are chosen with equal probability of $\frac{1}{2}$ each with respect to individual qubits. In order to incorporate locality and realism, the inequality was designed with assumptions that the measurement outcomes are independent of observation and the measurements performed on one of the qubits does not affect the measurement outcomes on the other qubit. As represented in Eq. (1.18), the expectation value of the CHSH operator under the assumptions of locality and realism must not exceed 2, i.e. all bipartite quantum states must satisfy the inequality. Interestingly, set of quantum states defined as

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle] \qquad\qquad |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle] \tag{1.19}$$

violate the CHSH inequality for a certain set of measurement operations, and with $2sqrt2$ as the expectation value of the CHSH operator. Thus, Bell or CHSH inequality enables identification of quantum states whose correlations cannot be explained by the assumption of locality and realism, thus delimiting a boundary between classical (local) and quantum (nonlocal) correlations. For a general two-qubit state $|\psi\rangle = sin\theta|00\rangle + cos\theta|11\rangle$, the maximum violation of CHSH operator is $2sqrt1 + sin^2 2\theta$ [Popescu and Rohrlich, 1992]. Thus the value of CHSH operator ranges from 0 to $2sqrt2$ for a product state of the form $|11\rangle$ to a state of the form $|\phi^+\rangle$ for $\theta = \frac{\pi}{4}$ as represented in Eq. (1.19). Since the quantum states in Eq. (1.19) violate the inequality to the maximum, they are known as maximally entangled two-qubit states; and play a central role in the advantages offered by quantum computation over classical computation. Clearly all pure two-qubit states violate the Bell-CHSH inequality, and all general two-qubit pure states where $0 < \theta < \frac{\pi}{4}$ are termed as non-maximally entangled states. Therefore, the violation of Bell inequality suggests that either one or both the assumptions forming the basis of Bell inequality are wrong in the quantum realm. The discussion further led to the discovery of other Bell-type inequalities which unveiled nonlocal correlations in quantum systems, shedding light on the complex nature of nonlocality in quantum realm [Leggett and Garg, 1985; Toner and Bacon, 2003; Acín *et al.*, 2005; Gröblacher *et al.*, 2007; Souza *et al.*, 2008; Barbieri, 2009; Xu *et al.*, 2011; Knee *et al.*, 2012; Epping *et al.*, 2013; Brunner *et al.*, 2014; Zhou *et al.*, 2015; Montina and Wolf, 2016; Chaves and Budroni, 2016; Brito *et al.*, 2018].

In order to identify nonlocal correlations in three-qubit systems, various Bell-type inequalities were also proposed and analysed [Mermin, 1990a; Svetlichny, 1987]. Although Mermin's inequality is violated by genuinely entangled three-qubit states, it is also violated by bi-separable entangled states making it difficult to distinguish between bi-partite and genuine tri-partite nonlocality. On the other hand, Svetlichny designed an inequality bearing the signature of genuine tripartite nonlocality as the inequality is only violated by genuinely entangled three-qubit states [Svetlichny, 1987]. Like Bell states violating the Bell inequality maximally, the Svetlichny inequality is also maximally violated by maximally entangled GHZ states. However, for a general three-qubit GHZ class as represented in Eq. (1.12), the inequality is only violated by the set of GHZ states with $\tau > \frac{1}{2}$. Later, the inequality was further generalized to identify non local correlations in multiqubit GHZ and W class of states [Seevinck and Svetlichny, 2002]. Furthermore, the vast application of extended multiqubit quantum systems in quantum information and computation has lead to the discovery of several significant Bell-type inequalities including n-party generalization to identify nonlocal quantum correlations in complex multipartite systems [Collins *et al.*, 2002a,b; Cereceda, 2002; Zhao *et al.*, 2003; Eibl *et al.*, 2003, 2004; Walther *et al.*, 2005; Lavoie *et al.*, 2009; Ghose *et al.*, 2009, 2010; Bancal *et al.*, 2010; Ajoy and Rungta, 2010; Liu *et al.*, 2010; Pál and Vértesi, 2011; Lu *et al.*, 2011a,b; Bancal *et al.*, 2011; Chen *et al.*, 2011; Zhao *et al.*, 2012; Vértesi and Brunner, 2012; Reid *et al.*, 2012; Pramanik and Majumdar, 2012; Tian *et al.*, 2012; He and Reid, 2013; 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; Zhao *et al.*, 2018; Riccardi *et al.*, 2018; Barasiński, 2018].

Since the advent of EPR paradox, quantum correlations have been the subject of intensive studies due to the general belief that they are fundamental resources for quantum information processing and other potential applications in quantum technology. The analysis and description of nonlocal correlations was therefore a subject of characterizing entanglement and nonlocality in quantum systems. Initially separable systems were thought to possess only classical correlations and hence were marked as not useful resources for quantum information and computation. This notion, however, was surprisingly challenged with the discovery of few separable states useful for quantum information processing. These separable systems were shown to evince quantum correlations, thus creating the need to find appropriate ways of quantifying these correlations [Modi *et al.*, 2012; Adesso *et al.*, 2016]. Quantum discord is one such measure that evaluates the amount of quantum correlations in both entangled and separable states [Ollivier and Zurek, 2001; Henderson and Vedral, 2001; Luo, 2008]. The importance of distinction between classical and quantum regime; and identification on nonlocal correlations in separable states on theoretical as well as experimental from led to study of quantum correlations beyond the paradigm of entanglement and Bell inequality. [Dakić *et al.*, 2010; Xi *et al.*, 2012; Gheorghiu *et al.*, 2015; Mahdian and Arjmandi, 2016; Bera *et al.*, 2017; Zhang *et al.*, 2017a].

Due to its importance in distinguishing classical and quantum correlations of all type, here, we briefly discuss the definition and significance of discord. A quantum state comprises of both classical and quantum correlations, which is measured using quantum mutual information where the quantum mutual information of a bipartite quantum state ρ^{AB} is defined as

$$I(\rho^{AB}) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \tag{1.20}$$

where $S(\sigma) = -\mathrm{Tr}(\sigma log_2 \sigma)$ is the von-Neumann entropy, ρ^A and ρ^B are reduced density operators for the subsystems A and B, respectively. On the other hand, classical correlations can be defined using measurement based mutual information as

$$J_A(\rho^{AB}) = S(\rho^B) - S(\rho^B|\rho^A) \tag{1.21}$$

where $S(\rho^B|\rho^A)$ is the conditional von-Neumann entropy. Quantum mutual information and amount of classical correlations in a system enables one to determine the amount of quantum correlations in a quantum system using the definition of discord as depicted in Eq. (1.22).

$$D_A(\rho^{AB}) = I(\rho^{AB}) - \underset{\{\pi_j^A\}}{max} J_{\{\pi_j^A\}}(\rho^{AB}) \tag{1.22}$$

Moreover, quantum discord has the following essential properties,

(a) Quantum discord is not symmetric i.e., $D_A(\rho) \neq D_B(\rho)$;

(b) Quantum discord always takes non-negative value;

(c) Quantum discord of any state is invariant under local unitary operations i.e., $D(\rho) = D((U_A \otimes U_B)\rho(U_A^\dagger \otimes U_B^\dagger))$; and

(d) The value of quantum discord is zero for any state that has only classical correlations.

Although quantum discord has been proved to be essential for describing nonlocal correlations in quantum states, the optimization procedure involved in the determination of quantum discord makes its evaluation difficult in different classes of bipartite states [Girolami and Adesso, 2011; Luo, 2008]. In view of the above, another measure known as "geometric discord" was introduced that quantifies nonlocal correlations using minimum distance from classical states [Dakić *et al.*, 2010; Luo and Fu, 2010; Qiang *et al.*, 2016; Roga *et al.*, 2016]; and can be defined as

$$D_G = \frac{1}{4}[\|x\|^2 + \|T\|^2 - K] \tag{1.23}$$

where K is the maximum eigenvalue of $xx^T + TT^T$; x is a 3×1 vector with elements $x_i = \langle \sigma_i \otimes I \rangle$; T is a 3×3 correlation matrix with elements $T_{ij} = \langle \sigma_i \otimes \sigma_j \rangle$; and σ_1, σ_2, and σ_3 are the Pauli spin operators. In order to calculate quantum correlations in higher dimensional multi-qubit quantum states, the formulation of discord is also studied for multi-dimensional multipartite systems [Liu *et al.*, 2015; Chanda *et al.*, 2015; Beggi *et al.*, 2015; Jakóbczyk *et al.*, 2016; Cheng and Hall, 2017; Jebaratnam *et al.*, 2018]. Due to its importance, quantum discord finds many applications in diverse domains [Vedral, 2003; Oppenheim *et al.*, 2003; Badziag *et al.*, 2003; Koashi and Winter, 2004; Yang *et al.*, 2005; Piani *et al.*, 2008; Maziero *et al.*, 2009; Mazzola *et al.*, 2010; Luo and Sun, 2010; Madhok and Datta, 2011; Cavalcanti *et al.*, 2011; Streltsov *et al.*, 2011; Cornelio *et al.*, 2011; Piani *et al.*, 2011; Adhikari and Banerjee, 2012; Seshadreesan *et al.*, 2015; Zou and Fang, 2016; Lee and Li, 2017; Yuan *et al.*, 2018]

1.3.3 Applications of entanglement

Apart from being central to several debates and discussions to investigate the foundations of quantum mechanics, entanglement and nonlocality have been used as key resources to design and characterize several potential applications in quantum information and computation. Quantum correlations, being the primary reason for out-performance of several tasks in quantum realm over their classical counterparts, have been used efficiently in various domains of information processing, computing, security, and games. For example, the users in a communication protocol share an entangled state for establishing a quantum channel for information transfer. Using this channel, the properties of an entangled quantum system are efficiently employed for secure quantum communication. In the following subsections, we discuss some of the major applications of entangled resources for efficiently sharing classical and quantum information.

- **Teleportation :** Quantum teleportation is a quantum mechanical process to transport the state of a system from one location to another arbitrary location, without sending the quantum system through any medium, or without measuring the state of the system on either side of the transport. The teleportation of the quantum state is facilitated by a shared entangled resource between the parties in the protocol. Since no medium is used to teleport the information, the protocol cannot be used to teleport the particle or qubit but rather its physical state. However, considering that the state of a system contains all information regarding the system, the recreation of original state at an arbitrary location suffices. The very reason that the information is not sent through a medium, prevents an eavesdropper to intervene and eavesdrop, once a secure quantum channel is established. The original protocol was proposed for teleporting a single qubit arbitrary state by sharing two-qubit anti-symmetric singlet state [Bennett *et al.*, 1993]. Alice, in possession of the unknown information, can neither perform a measurement to identify the unknown state due to the problem of measurement in quantum mechanics, nor send the qubit through any medium as it may adversely affect the necessary quantum coherence in the state. Therefore, in order to teleport a single qubit arbitrary state $|\chi\rangle_1 = [\alpha|0\rangle + \beta|1\rangle]_1$ to Bob, Alice establishes a quantum channel in the form of a shared two-qubit Bell state $|\phi^+\rangle_{23}$ as shown in Eq. (1.19). The shared state is distributed between the two in a way such that qubit 2 is with Alice and qubit 3 is with Bob. Alice then performs a Bell state measurement to identify the joint state of her qubits 1 and 2. Algebraically, the joint state of three-qubit system just before the Bell state measurement can be represented as

$$\begin{aligned}|\chi\rangle_1|\phi^+\rangle_{23} = |\phi^+\rangle_{12}(\alpha|0\rangle + \beta|1\rangle)_3 + |\phi^-\rangle_{12}(\alpha|0\rangle - \beta|1\rangle)_3 \\ + |\psi^+\rangle_{12}(\alpha|1\rangle + \beta|0\rangle)_3 + |\psi^-\rangle_{12}(\alpha|1\rangle - \beta|0\rangle)_3\end{aligned} \tag{1.24}$$

If Alice's outcome is $|\phi^+\rangle_{12}$, then the state of Bob's qubit gets instantaneously projected onto the original unknown state teleported by Alice i.e., $\alpha|0\rangle + \beta|1\rangle$. However, for all other measurement outcomes of Alice, Bob will have to perform a single qubit unitary transformation to get the desired state. For example, if Alice's measurement outcomes are $|\phi^-\rangle_{12}$, $|\psi^+\rangle_{12}$, or $|\psi^-\rangle_{12}$, then Bob needs to perform σ_z, σ_x, or $\sigma_z\sigma_x$ operations respectively. For Bob to know which unitary transformation has to be performed on his qubits to retrieve the original state, Alice must communicate her measurement outcome via a classical channel, thus restricting faster than light communication through teleportation. Moreover, the teleported state is not a copy or clone of the original state because the original state gets destroyed during the Bell state measurement at Alice's end.

The original protocol was also generalized to teleport an arbitrary qudit using a maximally entangled state in $d \otimes d$ dimensional Hilbert space [Bennett *et al.*, 1993]. Bennett *et al.* showed the faithful teleportation of an unknown state even when the Bell state is shared via a noisy channel [Bennett *et al.*, 1996b]. Similar to the shared two-qubit state, tripartite entangled resource was also considered as an efficient resource for teleprtation [Karlsson and Bourennane, 1998]. In general, when the shared resource is a non-maximally entangled state, then the teleportation of the unknown state was found to be probabilistic [Hillery *et al.*, 1999; Karlsson *et al.*, 1999; Shi *et al.*, 2000; Shi and Tomita, 2002; Agrawal and Pati, 2002; Fang *et al.*, 2003; Xiao *et al.*, 2004; yin Wang *et al.*, 2007; Wang *et al.*, 2018]. However, Agrawal and Pati have proposed an efficient three-qubit partially entangled resource for perfect teleportation [Agrawal and Pati, 2006]. In order to teleport an arbitrary two qubit state across distant locations, Rigolin used direct product of two Bell states as resources for deterministic teleportation [Rigolin, 2005]. The first instance of experimental teleportation of a single qubit came across in 1997 using photons [Bouwmeester *et al.*, 1997]. This was immediately followed by another successful teleportation along with identification of the four Bell states [Boschi *et al.*, 1998]. From the perspective of Nuclear Magnetic Resonance (NMR), teleportation protocol was first implemented over the space between atoms using solution state NMR [Nielsen *et al.*, 1998]. Moreover, implementation of teleportation protocol was also reported in ion-trap atomic systems [Barrett *et al.*, 2004]. Furthermore, different variants of the protocol were proposed, which showed teleportation between light and matter

[Sherson *et al.*, 2006], and deterministic quantum teleportation using a hybrid technique [Takeda *et al.*, 2013]. In the multiqubit regime, open-destination protocol was carried out using four-photon entanglement [Zhao *et al.*, 2004]. In addition, a six-photon interferometer was also employed for teleportation of a two-qubit quantum system [Zhang *et al.*, 2006]. The teleportation protocol was further accomplished over a distance of 600 meters using linear optics [Ursin *et al.*, 2004], then in free-space over 16 km [Jin *et al.*, 2010], and later over 143 km [Ma *et al.*, 2012]. Furthermore, teleportation across 102 km optical fiber was performed using superconducting nanowire detectors [Takesue *et al.*, 2015]. Latest reports show that satellite-based teleportation of six input states in unbiased bases has been accomplished over 1400 km [Ren *et al.*, 2017].

- **Entanglement Swapping :** Entanglement swapping, as the name suggests, is the mutual interchange of entanglement from a pair of qubits to another, thus entangling two qubits that have neither interacted nor generated from a common source in the past [Bennett *et al.*, 1993; Żukowski *et al.*, 1993]. Here, we consider a simple example of a swapping protocol using two Bell pairs. For this, we further consider that Alice and Bob share two Bell pairs $|\phi^+\rangle_{12}$ and $|\phi^+\rangle_{34}$ where qubits 1 and 4 are with Alice and qubits 2 and 3 are with Bob. It is assumed that once the entanglement is established or distributed, both Alice and Bob take their respective qubits to distant locations. Alice performs a Bell state measurement on her qubits 1 and 4. The measurement destroys the entanglement between qubits 1 and 2 and between qubits 3 and 4. In fact, two qubits which had never interacted, i.e., qubits 2 and 3 get entangled. Algebraically, this can be represented as

$$|\phi^+\rangle_{12}|\phi^+\rangle_{34} = \frac{1}{2}\Big[|\phi^+\rangle_{14}|\phi^+\rangle_{23} + |\phi^-\rangle_{14}|\phi^-\rangle_{23} + |\psi^+\rangle_{14}|\psi^+\rangle_{23} + |\psi^-\rangle_{14}|\psi^-\rangle_{23}\Big] \quad (1.25)$$

  Thus, the entanglement between qubits 1 and 2 and qubits 3 and 4 gets swapped so as to entangle qubit 1 with 4 and qubit 2 with 3. The basic settings of this protocol are used in designing quantum repeaters [Briegel *et al.*, 1998], and preparation of GHZ states [Zeilinger *et al.*, 1997; Bose *et al.*, 1998]. In addition, entanglement swapping holds application in quantum secret sharing [Hillery *et al.*, 1999; Karimipour *et al.*, 2002; Zhang and Man, 2005], and various other quantum secure communication schemes [Man *et al.*, 2005; Zhou *et al.*, 2005; Man *et al.*, 2006; Dong *et al.*, 2008]. The first experimental realization of entanglement swapping protocol was performed using two EPR pairs [Pan *et al.*, 1998]. This was followed by realizations using nuclear magnetic resonance [Boulant *et al.*, 2003], trapped ions [Riebe *et al.*, 2008], and photons with specific wavelength [Jin *et al.*, 2015].

- **Superdense coding :** Dense coding is a simple communication protocol to send 2 bits of classical message by locally manipulating a single qubit. It is probably the most elementary protocol by far to understand and analyse the importance of entangled systems over classical resources. For example, using a classical bit, a sender can send only one bit of information to a distant receiver. Whereas if the sender shares an entangled state with the receiver, then the sender can send two bits of information using her single qubit. In that sense, superdense coding protocol is a good example to demonstrate the use of quantum entanglement in enhancing the communication channel capacity. In the original protocol for dense coding [Bennett and Wiesner, 1992], Alice and Bob shared a two-qubit Bell state $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]_{AB}$, where qubit A is with Alice and qubit B is with Bob. For encoding two bit classical information (00, 01, 10, or 11) Alice performs single qubit unitary operations on her qubit locally. For example, in order to send 00, 01, 10, or 11, Alice performs I^A, σ_x^A, σ_y^A, or σ_z^A, respectively. Alice's operations either leaves originally shared Bell state $|\psi^-\rangle_{AB}$ unchanged or map it to other Bell states $|\phi^-\rangle_{AB}$, $|\phi^+\rangle_{AB}$, or $|\psi^+\rangle_{AB}$, respectively. After encoding her message by locally manipulating her qubit, Alice sends the qubit containing the encoded information to Bob, who then performs a Bell measurement to identify the joint state of two qubits. In principle, since the four Bell states are orthogonal to each other, Bob is able to distinguish between the four Bell states; hence decoding the required message. In general, a sender sharing a maximally entangled state in $d \otimes d$ dimensional Hilbert space with the receiver, can send $2\log_2 d$ bits of classical information to him/her with the help of superdense coding protocol.

On the experimental front, the first realization of the dense coding protocol was proposed by Mattle *et al.* using entangled photon pairs in 1996 [Mattle *et al.*, 1996]. This was followed by implementations of dense coding using the technique of nuclear magnetic resonance [Fang *et al.*, 2000]. Moreover, use of non-maximally entangled states and mixed states as resources for sending classical information was demonstrated in theory and experiments [Bose *et al.*, 2000]. For multi-qubit systems, GHZ states can be efficiently used to transfer three-bit classical information by performing local unitary operations on two qubits of the shared entangled states [Lee *et al.*, 2002; Wójcik and Grudka, 2003]. Experimentally, the techniques of NMR has been used to demonstrate the principles of dense coding including three users [Wei *et al.*, 2004]. Apart from this, an interesting theoretical scheme known as controlled dense coding was also proposed, in which a controller can control the amount of information between a sender and a receiver [Hao *et al.*, 2001]. Furthermore for making quantification simple, an analytical expression for evaluation of dense coding capacity of an entangled state was derived [Barenco and Ekert, 1995; Hausladen *et al.*, 1996; Bowen, 2001]. In addition, various experimental efforts were made to design dense coding protocol with non-integer channel capacities as well [Schaetz *et al.*, 2004; Williams *et al.*, 2017].

1.3.4 Quantum cryptography

Cryptography is the art of transforming a useful message into garbage/ cipher text (i.e. encryption), and later retrieving it back (i.e. decryption) in order to securely communicate private information between two parties in presence of adversaries. There are two types of encryption schemes: private-key cryptography and public-key cryptography [Stallings, 2003; Forouzan and Mukhopadhyay, 2011]. In private-key or symmetric cryptography, the same key is used to encrypt and decrypt the secret message. On the other hand, public-key cryptography protocols make use of different keys, a public key for encryption, and a private key for decryption. The basic premise of any cryptography technique depends on the secure sharing of key between the sender and the receiver, so that desired private information remains concealed from the third party. Considering the increased key domain and complexity, public-key cryptography is known to be more secure in comparison to private-key cryptography [Diffie and Hellman, 1976; Rivest *et al.*, 1978]. Quantum mechanics further assists the theory of cryptography for safe transmission of the key in several ways as described further.

- **Quantum Key Distribution (QKD):** The discussions surrounding quantum-mechanical means of secure key transmission probably took a flight with the noble proposal of BB84 protocol where the security relied on the problem of distinguishability of non-orthogonal basis states [Bennett and Brassard, 1984, 2014]. Another seminal contribution in formulating a secure method for safe transmission of key was proposed by Ekert using Bell's theorem and nonlocal properties of two-qubit entangled states [Ekert, 1991]. Since then, various protocols have been discussed for secure QKD [Bruß, 1998; Gisin *et al.*, 2002; Bennett, 1992; Bennett *et al.*, 1992; Beige *et al.*, 2002; Long and Liu, 2002; Deng *et al.*, 2003; Scarani *et al.*, 2009; Noh, 2009; Branciard *et al.*, 2012; Braunstein and Pirandola, 2012; Lo *et al.*, 2014; Chau, 2015]. Experimentally, quantum cryptography based on BB84 protocol was implemented over 10 km optical fiber [Bethune and Risk, 2000]. In addition to this, several other noticeable attempts have been made for practical and secure key transfer over longer distances [Muller *et al.*, 1996; Buttler *et al.*, 1998; Lemelle *et al.*, 2006; Brida *et al.*, 2012; Takesue *et al.*, 2015; Diamanti *et al.*, 2016; Collins *et al.*, 2016].

- **Quantum Secure Direct Communication (QSDC):** The fundamental laws of quantum mechanics also enable secure direct transmission of message without sharing any secret key in advance [Long and Liu, 2002; Boström and Felbinger, 2002; Deng *et al.*, 2003; Deng and Long, 2004b; Lucamarini and Mancini, 2005]. The first QSDC protocol was based on block transmission of the four encoded EPR states to send two bits of classical information [Long and Liu, 2002]. A two-way QSDC was also proposed using the similar concept of sharing encoded EPR pairs to communicate the message [Deng *et al.*, 2003]. These two schemes have recently been applied for long-distance transmission of secret message [Zhang *et al.*, 2017b; Zhu *et al.*, 2017]. Further, an interesting two-way asymptotically secure key distribution and quasi-secure direct communication protocol, named Ping-Pong Protocol (PPP) was proposed [Boström and Felbinger, 2002]. The prototype implementation of PPP using polarised entangled photons was demonstrated by Ostermeyer and Walenta [Ostermeyer and Walenta, 2008], followed by an experimental demonstration of a loss-tolerant QKD protocol based on a modified PPP [H. Chen *et al.*, 2016]. Deng and Long showed the protocol to be secure by encoding two-bit information using two unitary operations [Deng and Long, 2004b], which was experimentally implemented using single-photon frequency coding [Hu *et al.*, 2016a] and was also tested for communication at a distance of 1.5 kilometers [Qi *et al.*, 2019]. Another two-way deterministic communication protocol was proposed, as a special case of the scheme proposed by Deng and Long as it did not use entanglement for encoding the message [Lucamarini and Mancini, 2005]. This protocol has also been practically implemented using faint laser pulses containing not more than two single photons [Deng and Long, 2004a]. Lately, the advent of measurement device-independent QSDC protocols using EPR pairs and single photons have shown hopes for even more secure quantum communication [Niu *et al.*, 2018; Zhou *et al.*, 2018].

- **Quantum Secret Sharing (QSS):** Secret sharing is the mechanism of dividing or splitting a secret message into parts, such that none of the parts are sufficient enough to know the entire original message [Hillery *et al.*, 1999]. The motivation of QSS protocol is to split the information between the two receivers, one of which may be dishonest. The protocol is based on the assumption that the honest recipient will not let the dishonest recipient to cheat or break the protocol, hence splitting parts of message between the two. Only when the two recipients cooperate with each other, they recover the original message.

  Classically, Alice can produce a cipher text by adding the original message to a random bit string bitwise and modulo 2. She then communicates the cipher text to one of the recipient and a copy of the random bit string to the another recipient. Clearly the individual communications to the recipients are of no use for them unless they cooperate with each other to retrieve the original message. The protocol, however, may be compromised if an Eavesdropper or the dishonest recipient somehow gains access to both the communications. Such an adverse situation can be dealt with encrypting the original message using fundamentals of quantum information and computation. For example, the quantum mechanical version of this protocol, i.e. QSS, can be implemented using the maximally entangled three-qubit GHZ state. In order to initiate the protocol, Alice, Bob, and Charlie share a three-qubit maximally entangled GHZ state (1.14). Alice, being the sender, splits the original message between Bob and Charlie in a way that the complete message cannot be retrieved unless they get together and cooperate efficiently with each other to recover the original message. For sharing a common key all the participants in the protocol measure their qubits either in X or Y direction at random where the eigen states in X and Y

basis are defined as

$$|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle) \tag{1.26}$$

Alice can use the joint key shared with Bob and Charlie later to communicate secure messages

Table 1.1 : The effects of Bob's and Charlie's measurements on Alice's state in a QSS protocol

Charlie Bob	$\|+x\rangle$	$\|-x\rangle$	$\|+y\rangle$	$\|-y\rangle$
$\|+x\rangle$	$\|+x\rangle$	$\|-x\rangle$	$\|-y\rangle$	$\|+y\rangle$
$\|-x\rangle$	$\|-x\rangle$	$\|+x\rangle$	$\|+y\rangle$	$\|-y\rangle$
$\|+y\rangle$	$\|-y\rangle$	$\|+y\rangle$	$\|-x\rangle$	$\|+x\rangle$
$\|-y\rangle$	$\|+y\rangle$	$\|-y\rangle$	$\|+x\rangle$	$\|-x\rangle$

to them. The effects of Bob's and Charlie's measurement outcomes on the state of Alice's qubit are shown in Table 1.1. After performing their measurements at random, Bob and Charlie announce their respective choices of measurement bases to Alice. The measurement outcomes however are still not disclosed and kept safely with the two receivers. The protocol proceeds further by Alice also announcing her choices of measurement basis to Bob and Charlie, without disclosing her measurement outcomes. Only the bases XXX, XYY, YXY, and YYX (for Alice, Bob, and Charlie, respectively) are accepted, for sharing the secret key. The results from the remaining random choices of bases are discarded for not containing any useful information. Clearly, neither Charlie nor Bob can identify the measurement outcomes of Alice without receiving the communication regarding the measurement choices of each other. Therefore, Bob and Charlie must get together to share their measurement outcomes so as to cumulatively find out the measurement outcomes of Alice. For instance, if both Bob and Charlie measure in X basis and their measurement outcomes are $+1(-1)$ and $+1(-1)$ respectively, then the corresponding outcome of Alice will be $+1$ when measured in X basis. On the other hand, if the measurement outcomes of Bob and Charlie are $+1$ and -1 respectively or *vice-versa*, then the corresponding outcome of Alice will be -1 when measured in X basis. Therefore, the QSS protocol provides an efficient way to split the information between recipients to keep the original message secure. Several practical versions of QSS that are based on entangled photon pairs [Karlsson *et al.*, 1999; Tittel *et al.*, 2001; Chen and Lo, 2007; Grice *et al.*, 2018; Williams *et al.*, 2019], or single photons [Schmid *et al.*, 2005; Bogdanski *et al.*, 2008; Han *et al.*, 2008; Hai-Qiang *et al.*, 2013] have been proposed for experimental implementation.

1.3.5 Quantum Noise

In ideal situations, the qubits or entangled systems must be isolated from the surroundings so that the system does not interact with the environment and the necessary quantum coherence between qubits remains intact. In reality however, environmental interactions with quantum systems are inevitable, leading to the study of open quantum systems and noise in case of practical quantum computations. Such interactions result in destruction of coherence between entangled qubits evolving the initially prepared pure state into a statistical mixture. Clearly, noise in general is an undesirable phenomenon, which in turn adversely affects the efficiency of prepared entangled resource in quantum information and computation [Situ and Huang, 2016; Huang *et al.*, 2017b; Gawron, 2010; Gawron *et al.*, 2008; Dajka *et al.*, 2015]. For example, if an entangled state is shared through noisy channel(s), it decreases the degree of entanglement or degrades nonlocal correlations present in the initial prepared state, thereby hindering the efficiency of such systems. Therefore, it is imperative to analyse the effects of noisy channels on entangled systems and device a mechanism to protect nonlocal correlations against the decoherence [Nielsen and Chuang, 2011].

The evolution of a quantum state ρ under noise is given by the operator-sum representation $\varepsilon(\rho)$ such that

$$\varepsilon(\rho) = \sum_i N_i \rho N_i^\dagger \tag{1.27}$$

where N_is are operational elements of the noise under consideration. In the following, we briefly describe few standard noisy channels to understand the operational elements associated with them.

(i) **Bit flip channel**: The bit-flip channel locally acts on a qubit to flip the state of a qubit with a probability of $(1-p)$, and leaves the state of the qubit unchanged with the probability p. Therefore, the operational elements of a bit flip channel are, $N_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $N_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

(ii) **Phase flip channel**: The phase flip channel flips the phase of a qubit ($|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $-|1\rangle$) with probability $1-p$, and leaves the state of the qubit unchanged with the probability p. Therefore, the operational elements of a phase flip channel are, $N_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $N_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

(iii) **Bit phase flip channel**: The bit phase flip channel flips both the bit as well as the phase of a qubit ($|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $-|0\rangle$) with probability $1-p$, and leaves the state of the qubit unchanged with the probability p. Therefore, the operational elements of a bit phase flip channel are, $N_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $N_1 = \sqrt{1-p}Y = \sqrt{1-p}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$.

(iv) **Depolarizing channel**: In comparison to above noisy channels, the depolarizing channel is much more destructive as when a qubit passes through a depolarizing channel, it gets depolarized to a completely mixed state $I/2$ with probability p. Thus, the state of quantum system ρ after passing through the depolarizing channel can be represented as $\varepsilon(\rho) = p\frac{I}{2} + (1-p)\rho$. The operational elements for this channel, therefore, are, $N_0 = \sqrt{\frac{1-3p}{4}}I$, $N_1 = \frac{\sqrt{p}}{2}X$, $N_2 = \frac{\sqrt{p}}{2}Y$, and $N_3 = \frac{\sqrt{p}}{2}Z$.

(v) **Amplitude damping**: The operational elements of an amplitude damping channel are $N_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$ and $N_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$. The amplitude damping noise signifies loss of energy due to environmental interaction or a decay process. The process can be summarized by assuming the decay of the excited state to the ground state for a two-level system with a probability p with emission of a photon which further results in the environment going from the ground state to the excited state.

(vi) **Phase damping**: The phase damping channel is the quantum mechanical channel that demonstrates loss in quantum information without loss in energy of the system. Rather the relative phase between qubits in a quantum system is lost. The operational elements of this channel are, $N_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}$ and $N_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}$. N_0 reduces the amplitude of quantum state $|1\rangle$, while maintaining the amplitude of $|0\rangle$ state; whereas N_1 reduces the amplitude of quantum state $|1\rangle$ and destroys $|0\rangle$ state. The effect of phase damping noise is equivalent to that of phase flip channel.

In order to protect nonlocal correlations from adverse effects of noise, various mechanisms such as entanglement distillation [Bennett *et al.*, 1996b,a; Pan *et al.*, 2003], quantum error correcting codes [Shor, 1995; Calderbank and Shor, 1996; Knill and Laflamme, 1997; Steane, 1996b; Lidar and Brun, 2013; Terhal, 2015], decoherence free subspace [Kwiat *et al.*, 2000; Lidar *et al.*, 1998], quantum zeno effect [Facchi *et al.*, 2004; Maniscalco *et al.*, 2008], dynamic decoupling [Viola and Lloyd, 1998; Viola *et al.*, 1999; Viola and Knill, 2003; Khodjasteh and Lidar, 2005; West *et al.*, 2010], application of weak measurement and its reversal operations [Korotkov and Keane, 2010; Korotkov and Jordan, 2006; Kim *et al.*, 2009; Xiao and Li, 2013; Cheong and Lee, 2012; Sun *et al.*, 2009; Suter and Álvarez, 2016] have been analysed and studied in detail.

1.4 BASIC TERMINOLOGIES AND CONCEPTS IN GAME THEORY

A game is a competitive activity among more than one rational players which consists of a set of rules, conditions of win and loss, and payoffs. The rules define the constraints of moves a player can opt for in a game. Payoffs are quantified rewards each player gets on performing a certain move or on achieving a fixed goal. While playing a game, each player attempts at performing the best move to attain maximum reward or payoff. The final payoff or reward of each player depends on the actions of all players or stakeholders involved in the game.

Therefore, game theory is a mathematical model of strategic decision making in a game. The theory was developed by John von Neumann, a mathematician and Oskar Morgenstern, an economist with the aim of solving problems related to economics [Neumann and Morgenstern, 1944]. The discovery of game theory initiated with a realization that the dynamics in economics has a correspondence with game-playing. In general, any situation where the moves of players affect each other's outcomes, thus involving strategic decision making can be modeled mathematically using game theory. For instance, the study of demand and supply of a product in market as a game can assist in evaluating its optimum cost in a competitive market [Shubik, 1981]. Likewise, the phenomenon of public choice for voting can be visualized as a game [Downs, 1957]. Another example of the theory lies in evolutionary biology where survival of the fittest being is modeled as survival games [Smith, 1974].

1.4.1 Different types of games

In this sub-section, we summarize basic terminologies used for different types of games in game theory.

(i) **Cooperative and Non-Cooperative Games :** Cooperative games are the ones where players negotiate and agree with each other on adopting strategies while playing [Myerson, 1991]. The players are in a coalition, and thus these games are studied separately under cooperative game theory. The traditional games however, are non-cooperative in nature. In non-cooperative games, players do not play as a team; they rather individually opt for the strategy that gives them the maximum reward [Myerson, 1991]. Prisoners' dilemma [Poundstone, 1992] is the best example of a non-cooperative game.

(ii) **Symmetric and Asymmetric Games :** If all strategies adopted by one player in a game is same as the strategies adopted by all other players; and the payoff achieved by players also remains the same even when the same strategy set is performed by interchanging players, then such a game is termed as a symmetric game [Nash, 1951]. Mostly, two-player games such as prisoners' dilemma [Poundstone, 1992] and chicken's game [Sugden, 2005] are symmetric. On the other hand, asymmetric games are those where the players have a different strategy space to opt from, and/or the payoff that a player attains on performing a particular strategy may not be the same as the payoff attained by the other player on performing the same strategy. An instance of asymmetric game is the ultimatum game [Güth *et al.*, 1982].

(iii) **Zero-sum and Non-zero-sum Games :** Zero-sum games are specific cases of constant sum games, where the sum of total payoffs of players should be exactly zero [Owen, 2013]. In such cases, the wining condition for a player becomes the losing situation for the other player-chess, tic-tac-toe, and many such games are examples of zero-sum games. Contrary to this, non-zero sum games are the ones where the sum of total payoff of all players is non-zero [Owen, 2013]. In general, cooperative games are examples of non-zero sum games because the coalition (of players) either wins or looses the game collectively.

(iv) **Normal and Extensive form Games :** In normal form games, the game is structurally represented in a tabular format, where the strategies and the corresponding payoffs of the players are written in a table. Whereas in an extensive form game, the description of a game is decorated on a decision-tree [Fudenberg and Tirole, 1991; Leyton-Brown and Shoham, 2008]. Nodes at different levels in a tree represent different players, edges represent the moves adopted by different players, and leaves of the tree define the payoffs of players on adopting respective strategies.

(v) **Simultaneous and Sequential move Games :** In simultaneous games, the players do not know about strategies adopted by other players, since all players take simultaneous moves. On the other hand in sequential games, a player adopts a strategy followed by another player. This way the players have knowledge about previous strategies adopted by other players. In general, simultaneous games are represented by normal form games, and sequential games are represented by extensive form games [Brocas *et al.*, 2018].

(vi) **Perfect, Imperfect, Complete, and Incomplete Information Games :** If every player has knowledge regarding strategies adopted by all other players, then the game is a perfect information game. For instance, tic-tac-toe and chess are perfect information games [Mycielski, 1992]. On the other hand, imperfect information games like poker, are the ones in which players do not completely know about the prior moves of other players in the game [Osborne and Rubinstei, 1994]. Simultaneous move games in general, are imperfect information games. Perfect information games are different from complete information games. The players in a complete information game also know about the strategies, payoffs and types of players in the game but they do not necessarily know about all the prior moves of the players. As opposed to the complete information game, players do not have all the information in case of incomplete information games. Bayesian games [Harsanyi, 1967a,b,c] are examples of incomplete information games, where atleast one player is unaware of the type of other players in the game. *Nature* is introduced as an additional player which assigns a type to each player depending on the "probability distribution or prior assumption" of available types [Leyton-Brown and Shoham, 2008]. This method further enables conversion of incomplete information games to imperfect information games.

(vii) **Common and Conflicting Interest Games :** Conflicting interest games [Osborne, 2003; Smith and Price, 1973; Smith, 1974] are those in which both the players have different preferences, like in the case of Battle of Sexes game. On the other hand, common interest games are the ones where players do not prefer one strategy over the other, but have similar interests in terms of opting for a particular strategy [Osborne and Rubinstei, 1994].

1.4.2 The Nash equilibrium

For a static game with finite set of strategies for players, John F. Nash [Nash, 1950, 1951] described a stable point known as the Nash Equilibrium (NE). It comprises of those strategy sets that optimize the payoffs of both players in the game, and in which no player gets an incentive by unilaterally changing her/his strategy. Further, a strategy set of a game is known as Pareto efficient (or Pareto-optimal) if there is no other strategy set that enables at least one player better off without making any other player worse off. The concept behind NE lies in the fact that multiple players contest in a game, and each player's payoff depends on the other players' choice of strategy or decision. Thus, NE is very useful in analysing decision making in situations of war or dilemma.

Table 1.2 : A payoff matrix for the Prisoners' dilemma game

Prisoner 2 Prisoner 1	Cooperate	Defect
Cooperate	$-1,-1$	$-3,0$
Defect	$0,-3$	$-2,-2$

Table 1.2 shows the payoff matrix table for a *Prisoners' dilemma* game [Poundstone, 1992]. The game represents a scenario where two prisoners are suspected of committing a crime and are being interrogated in two separate cells. They can either cooperate by accepting their crime or defect by denying their crime. When both accept their crime they get an equal payoff of -1 each. When both deny their crime, they get an equal payoff of -2 each. Further, if one prisoner accepts his crime and the other denies, then the one who denies gets 0 payoff and the one who accepts gets a lower payoff of -3. In the payoff matrix, the rows represent the strategies of Prisoner 1, and the columns represent the strategies of Prisoner 2. The numbers in each rectangle represent payoffs of prisoners depending on the strategies opted. For example, $(-3,0)$ shows that Prisoner 1 receives a payoff of -3 and Prisoner 2 receives a payoff of 0 for opting for strategy set cooperate and defect, respectively. Analysing the payoff matrix, it can be observed that each player is at a better position by denying his crime, independent of what the other player or prisoner chooses to do. Therefore, both prisoners denying their crime collectively forms the NE of the dilemma game. However, the common welfare/ pareto-optimal move for the prisoners would be cooperation from both players so that they get higher payoff each (-1) as compared to the defection move from both players (-2). Cooperation from both players is pareto-optimal whereas the obtained NE (defection from both players) is not. This contrasting situation is the dilemma in the game, henceforth justifying the role of finding NE in game theory.

Table 1.3 : A payoff matrix for the Battle of sexes game

Woman Man	Football	Movie
Football	$3,2$	$1,1$
Movie	$0,0$	$2,3$

There can be two types of NE- a pure strategy Nash equilibrium or a mixed strategy Nash equilibrium. [Neumann and Morgenstern, 1944]. An example of pure strategy NE is the one discussed above in case of prisoners' dilemma game [Poundstone, 1992]. In mixed strategies, players choose a probability distribution over the set of actions or strategies [Harsanyi, 1973; Neumann and Morgenstern, 1944]. In order to exemplify, payoffs in *battle of the sexes* game [Osborne and Rubinstei, 1994] are depicted in Table 1.3. The game represents a situation where a couple prefers to spend an evening together, but there choices to the type of evening are very different. For example, the male partner may prefer to go for a football match, whereas the female partner prefers to opt for a movie together. The payoff matrix in Table 1.3 suggests that there are two pure strategy NEs in the game- (Football, Football) and (Movie, Movie). For mixed strategies, let us assume that the woman prefers a football match with probability "p" and a movie with probability "$1-p$". Similarly, let us further assume that the man prefers a football match with probability "q" and a movie with probability "$1-q$". Therefore, the payoff when the man watches a football match or a movie can be evaluated as $3p+1(1-p)$ or $0p+2(1-p)$, respectively. Likewise, the woman's payoff on watching a football match or a movie is summarized as $2q+0(1-q)$ or $1q+3(1-q)$, respectively. Evidently, the man is invariant in choosing between the two activities if $3p+1(1-p)=0p+2(1-p)$ i.e., $p=\frac{1}{4}$. Similarly, the woman will have no preferences and will be equally rewarded by opting for either of the two activities if $2q+0(1-q)=1q+3(1-q)$ i.e., $q=\frac{3}{4}$. Therefore to sum up, the mixed strategy NE will correspond to the man going for a football match with $\frac{3}{4}$ probability (and movie with $\frac{1}{4}$ probability); and woman going for a football match with $\frac{1}{4}$ probability (and movie with $\frac{3}{4}$ probability)

Table 1.4 : A payoff matrix for the Stag hunt game

Player 2 / Player 1	Stag	Rabbit
Stag	$3,3$	$0,2$
Rabbit	$2,0$	$1,1$

In addition, there can be games with multiple pure strategy NEs [Osborne and Rubinstei, 1994]. If the equilibria comprise of same or corresponding strategies opted by players, then the game belongs to the category of coordination games. For instance, *stag hunt* game (common interest coordination game) represented in Table 1.4 and *battle of the sexes* game (conflicting interest coordination game) [Osborne and Rubinstei, 1994] represented in Table 1.3 are examples of coordination games. On the other hand, when the equilibria comprise of different or anti-corresponding strategies, the game is an anti-coordination game. An example of anti-coordination game is the hawk-dove game or chicken game [Sugden, 2005] as described in Table 6.2.

1.4.3 Applications of game theory

Game theory is an interesting and burgeoning field of study, which encompasses the analysis and resolution of various situations of conflict and dilemma [Neumann and Morgenstern, 1944]. The theory initiaited with the need of analysing marketing games in the economic realm [Shubik, 1981; Kreps, 1990; Friedman, 1991; Erica, 2003; Fudenberg, 2006; Tesfatsion, 2006], but its applicability spread across diverse academic spaces such as, political science [Hardin, 1995; Moulin, 1994; Brams, 1994; Fearon, 1995; Levy and Razin, 2004], biology [Smith, 1974, 1982; Hammerstein, 2003; Harper and Maynard Smith, 2003], computer science [Nisan and Ronen, 1999; Shoham, 2008; Greenwald and Littman, 2007; Bellucci *et al.*, 2004; Gubko, 2004; Knauss *et al.*, 2008; Tambe and An, 2012], and physics [Hauert and Szabó, 2005].

1.5 INTRODUCTION TO QUANTUM GAME THEORY

With the advent of quantum information and computation, curiosity to analyse classical game theory in quantum mechanical regime resulted in quantum game theory. The analysis in this realm began with the discovery of concept of quantum money in 1983 [Wiesner, 1983]. Later, the year 1999 witnessed various games where quantum strategies were employed in a classical game setting to help quantum players win a game with increased probability in comparison to players opting for classical strategies or in resolving situations of conflict. For example, Meyer demonstrated that a quantum player can always win a classical penny flip game against his classical opponent; and further depicted a relation between penny flip game setting and efficient quantum algorithms [Meyer, 1999]. Later, a slightly different scenario of the penny flip game was analysed, where a classical player opting for a mixed strategy wins against the quantum player performing unitary transformations [Anand and Benjamin, 2015]. The analysis presented by Anand and Benjamin was very significant in a sense that for certain settings and strategy sets, even a classical player can win against a quantum player. In addition, Eisert *et al.* demonstrated the role of quantum strategies in avoiding the dilemma present in classical prisoners' dilemma game [Eisert *et al.*, 1999]. Moreover, a three player game where the team always wins the game if they share a three qubit maximally entangled state was illustrated [Vaidman, 1999]. Furthermore, quantum game theory was also utilized to introduce fairness in remote gambling [Goldenberg *et al.*, 1999]. Later another gambling protocol was introduced for fairness without a third party, which can also be adapted in casino, and lottery system [Zhang *et al.*, 2014].

Parrondo's paradox consists of games which when played individually have higher probability of losing than winning, but if played alternately or in a specific random order, become winning games. The study of this paradox using quantum walks plays a significant role in building better algorithms and in understanding important physical process like Brownian ratchets. Flitney and Abbott examined the quantum version of parrondo's game, which led to the identification of innovative quantum algorithms [Flitney and Abbott, 2003]. Moreover, eavesdropping [Ekert, 1991; Gisin and Huttner, 1997] and optimal cloning [Werner, 1998] was also studied in the framework of games between players. Considering that lesser bits are used to implement quantum game theory than other applications of quantum mechanics, it becomes much easier to verify quantum games on an experimental front [Patel, 2007]. The idea of representing quantum communication protocols and algorithms in terms of games between quantum and classical players was further analysed by Iqbal [Iqbal, 2005]. On the similar lines, the BB84 protocol proposed by Bennett and Brassard [Bennett and Brassard, 1984], used for secure quantum key distribution was envisaged as a game and the mixed strategy NE of the game could hence, be evaluated [Houshmand *et al.*, 2010]. Similarly, various numerical schemes were formulated to find NE in terms of best response functions, when the strategy space was characterized by continuous variables [Avishai, 2012]. Furthermore, a Quantum Key distribution protocol was proposed using the concept of three-player quantum game, and using the maximally entangled GHZ triplet state [Kafatos, 1989; Bouwmeester *et al.*, 1999; Toyota, 2010]. Besides this, Toyota also highlighted the crucial role of entanglement of the initial state used in the protocol [Toyota, 2010].

Not surprisingly, since then many games have been formulated to study quantum information processing in detail. For example, quantum correlation games were designed using a two-qubit entangled singlet state as input, where the payoffs were defined as functions of correlations in an EPR-type experimental setting [Iqbal and Weigert, 2004]. Further, classically defined games were studied where a quantum team is shown to have an advantage over any classical team [Aharon and Vaidman, 2008]. Moreover, quantum games were also constructed from a system of Bell-type inequalities, and the example of prisoners' dilemma and Matching Pennies was considered to study the approach [Iqbal and Abbott, 2010]. Similarly, a new class of non-local games- generalized form of CHSH games- was studied to demonstrate that entanglement plays an important role for information processing tasks [Lawson *et al.*, 2010]. A review on quantum game theory was also done to analyse and discuss games such as prisoners' dilemma and parrondo's game [Lui *et al.*, 2010]. Besides, a new two-player quantum game based on the CHSH game was illustrated in 2013 [Bojic, 2013]. Furthermore, Werner-like states [Werner, 1989] were analysed for prisoner's dilemma and chicken game, to obtain values of quantum discord of the initial state; at which the dilemma in both the games could be resolved [Nawaz and

Toor, 2010]. Interestingly, game theory was also used, as a part of Quantum Decision Theory to formulate a scheme of how brains make decisions [Yukalov and Sornette, 2014]. Furthermore, quantum computer games such as the Schrödinger's cat and hounds game [Gordon and Gordon, 2012] have also been designed to demonstrate the fundamental concepts of quantum mechanics like superposition, constructive and destructive interference, measurements and entanglement, in a fun way. Substantial contributions made in the field of quantum game theory have been discussed in the following subsections, for comprehensive study. Apart from this, recently several game-theoretic models have been proposed in quantum realm, which display the latest trend of research in quantum game theory [Giannakis *et al.*, 2015; Balthazar *et al.*, 2015; Deng *et al.*, 2016; Auletta *et al.*, 2016; Melo-Luna *et al.*, 2017; Bao and Yunger Halpern, 2017; Rai and Pal, 2017; Frąckiewicz, 2018; Solmeyer *et al.*, 2018a,b; Samadi *et al.*, 2018; Khan *et al.*, 2018; Khan and Humble, 2019; Sarkar and Benjamin, 2019; Vijayakrishnan and Balakrishnan, 2019; Kolokoltsov, 2019].

1.5.1 The quantum advantage of superposition in penny flip game

With the aim of studying quantum algorithms, Meyer came-up with one of the early contributions in the area of quantum game theory [Meyer, 1999]. He efficiently demonstrated advantages of quantum strategies over classical ones in a penny flip game. The game comprises of two players- player P and player Q. The game starts with a penny being placed in *"heads-up"* position in a black box. The settings of the game allows player P and player Q to make moves once and twice, respectively where each player can use the strategy set to either flip the coin or leave it unchanged. To start the game, player Q either flips or not flips the penny without looking at its state. This is followed by player P's turn, as discussed has the same set of strategies to either flip or not flip the coin. Finally, the game ends with player Q's turn. At the end of the game, if the penny is still *"heads-up"*, player Q wins the game else player P wins the game. Classically, the game can be won by either players with equal probability. However, if player Q is a quantum player, he/she performs a quantum strategy (in particular, the Hadamard gate as discussed in subsection 1.2.2) during his/her turn and wins the game deterministically. Meyer, further demonstrated that the game holds structural similarities to Simon's problem [Simon, 1994] and Grover's algorithm [Grover, 1996].

1.5.2 Resolution of dilemma using entanglement

Soon after Meyer proposed the notion of quantum games, *Eisert et al.* discussed the prisoners' dilemma game in quantum realm [Eisert *et al.*, 1999] where the objective was to quantize and describe non-zero sum games. Eisert *et al.* demonstrated that the dilemma in the game can be avoided when both players initiate quantum strategies. A simple prisoners' dilemma game is demonstrated in Table 1.2, where the NE {Defect, Defect} strategy is not the pareto-optimal strategy giving rise to the said dilemma in the game. In the quantum regime, classical strategies, cooperate (C) and defect (D) are defined in the Hilbert space as $|C\rangle$ and $|D\rangle$, respectively. The players or prisoners (here, Alice and Bob) share the initial state $|\psi_0\rangle = \hat{J}|CC\rangle$, where $\hat{J}$ is an entangling unitary operator known to both players, say Alice and Bob. Once the entanglement is shared, players perform their respective strategies $\hat{U}_A$ and $\hat{U}_B$, respectively on their qubits, followed by the operation of a reversible disentangling gate $\hat{J}^\dagger$ on the evolved quantum state. After these operations, the final state $|\psi_f\rangle$ is measured using a pair of Stern-Gerlach type detectors, where

$$|\psi_f\rangle = \hat{J}^\dagger \left(\hat{U}_A \otimes \hat{U}_B\right) \hat{J}|CC\rangle \tag{1.28}$$

The payoffs of players in this game depend on the detector's outcome. Considering the statistical nature of quantum theory, payoffs are expressed as the expectation values according to the matrix entries in Table 1.2 such that

$$\begin{aligned} \$_A &= -P_{CC} - 2P_{DD} - 3P_{CD} \\ \$_B &= -P_{CC} - 2P_{DD} - 3P_{DC} \end{aligned} \tag{1.29}$$

where $P_{mn} = |\langle mn|\psi_f\rangle|^2$ is the probability associated with the measurement outcome $|mn\rangle$. The cooperation strategy is assumed to be $\hat{C} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and the defect strategy is considered to be a spin-phase flip operation denoted mathematically as $\hat{D} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. In order to ensure the game theoretic model to be fair, the entangling unitary operator is considered as,

$$\hat{J} = \exp\left(i\gamma\frac{\hat{D}\otimes\hat{D}}{2}\right) \tag{1.30}$$

The separable game ($\gamma = 0$) is the same as classical prisoners' dilemma game represented in section 1.4.2. However, the maximally entangled game ($\gamma = \frac{\pi}{2}$) resolves the dilemma as the new quantum strategy $\hat{Q} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ performed by both players comprises the pareto-optimal NE for the game. The quantum version of prisoners' dilemma game was also realized using NMR [Du *et al.*, 2002].

1.5.3 The Clauser-Horne-Shimony-Holt game

Clauser, Horne, Shimony, and Holt described the CHSH inequality [Clauser *et al.*, 1969] under the assumption of local realism. This inequality can be used to ascertain the presence or absence of quantum correlations in an underlying quantum system [Bell, 1964]. Alternately, to analyse nonlocal correlations in a simpler way, the inequality is formulated in terms of a game, termed as the CHSH game. The CHSH game is usually played between two cooperating players; Alice and Bob. In the settings of a game, a referee always generates two independent random bits: '*x*' and '*y*', and sends them to Alice and Bob, respectively. These random bits act as inputs to the players. On receiving the input bits, Alice and Bob output their answer bits as '*a*' and '*b*', respectively. Both players win the game if the addition modulo 2 (or XOR) of their outputs is equal to the logical AND of their inputs, i.e., $a \oplus b = x \cdot y$. Alice and Bob both aim at increasing their chances of win, and hence can discuss a priory the strategy to be used during the game. However, they cannot communicate after the commencement of the game, and do not have prior information about each other's input or output. The only information they have is about their individual inputs ('*x*' is known to Alice and '*y*' is known to Bob), based on which they produce their outputs '*a*' and '*b*', respectively. Here, for simplicity, it is assumed that the probability of an input to take value 0 or 1 is equiprobable. Classically, the game can be won with utmost 75% probability.

On the other hand, in quantum realm Alice and Bob share a two-qubit entangled state, i.e.,

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right] \tag{1.31}$$

Once the entanglement is distributed, Alice and Bob perform spin-projection measurements on their respective qubits based on the inputs received, and preserve the corresponding measurement outcomes as outputs. For example, let us assume that Alice and Bob perform measurements in a general basis $v_i(\theta)$ expressed as

$$\begin{aligned} |v_0(\theta)\rangle &= cos\theta|0\rangle + sin\theta|1\rangle \\ |v_1(\theta)\rangle &= -sin\theta|0\rangle + cos\theta|1\rangle \end{aligned} \tag{1.32}$$

where Alice uses θ_{A0} (θ_{A1}) when input '*x*' is 0 (1), and Bob use θ_{B0} (θ_{B1}) when input '*y*' is 0 (1). As per the rules of the game defined above, when product of inputs is 0, then the game will lead to success if and only if the outputs also have the same value. Considering the rules and strategy set opted by Alice and Bob, the winning probability of the game at different values of '*x*' and '*y*' is summarized in Table 1.5. Clearly, the total winning probability of the game is $\frac{1}{4}\Big[cos^2(\theta_{A0} - \theta_{B0}) + cos^2(\theta_{A0} - \theta_{B1}) + cos^2(\theta_{A1} - \theta_{B0}) + sin^2(\theta_{A1} - \theta_{B1})\Big]$. For optimizing the success probability, if Alice and Bob choose $\theta_{A0} = 0$, $\theta_{A1} = \frac{\pi}{4}$, $\theta_{B0} = \frac{\pi}{8}$, and $\theta_{B1} = -\frac{\pi}{8}$, then the winning probability of the game is $cos^2(\frac{\pi}{8}) \approx 0.8535$. Therefore, in the CHSH game, quantum strategy gives better winning probability (above 85%) than the classical winning probability (75%).

Table 1.5 : The dependence of winning prospects on inputs received by players in a CHSH game

x	y	Winning probability of CHSH game
0	0	$cos^2(\theta_{A0} - \theta_{B0})$
0	1	$cos^2(\theta_{A0} - \theta_{B1})$
1	0	$cos^2(\theta_{A1} - \theta_{B0})$
1	1	$sin^2(\theta_{A1} - \theta_{B1})$

1.5.4 A three player quantum game using the GHZ state

Similar to the CHSH game, there are various multi-party quantum games that exploit the nonlocal features of an entangled state for the benefit of players [Clauser *et al.*, 1969; Vaidman, 1999; Aravind, 2002]. One such game was proposed by Vaidman in 1999 [Vaidman, 1999]. The game consists of a team three players, say Alice, Bob and Charlie. The players in the game are well aware of the settings and rules of the game; they are also allowed to discuss their strategies before the start of the game. However, after the commencement of game, they are not allowed to communicate with each other. In the game, each player is asked one of the two possible questions, i.e., either the question is 'What is X?' or the question is 'What is Y'? Once a question is asked to a player, the player must respond with his/her answer- and the possible choices are either $+1$ or -1. The settings of the game are such that either each player is asked the X question or one of them is asked the X question and rest of them are asked the Y question. The team of three players wins the game if the product of their answers is +1 when all players are asked the X question; and -1 when one of the players is asked the X question and rest of them are asked the Y question. Clearly, if the players adopt classical strategies then at best they can win the game 75% of times. On the other hand, if the team of three players share a three-qubit maximally entangled GHZ state, then they always win the game by using a simple quantum strategy, i.e., whenever a player is asked the $X(Y)$ question, she/he measures her/his qubit in the $X(Y)$ basis and announces the corresponding measurement outcome as her/his answer. Hence, quantum strategies clearly win over classical strategies under the settings of three-party Vaidman game.

1.5.5 Visualisation of the BB84 protocol as a classical game

A static game model was used to study the well-known QKD protocol- the BB84 protocol- in the framework of a game [Houshmand *et al.*, 2010]. The sender (Alice), the receiver(Bob), and an eavesdropper (Eve) were considered as players in the game. For encoding, Alice's strategy set comprises of selecting encoding operations at random between z or x eigen bases; where z represents computational basis set and x represents Hadamard ($|+\rangle$, $|-\rangle$) basis set. Similarly for decoding and eavesdropping, Bob and Eve's strategy set also comprises of selection between z and x eigen bases for their respective measurements. Considering the intervention of Eve, the aim of Alice and Bob is to detect Eve's presence with maximum probability. On the other hand, the objective of Eve is to gain maximum information during intervention, while simultaneously minimizing her chances of detection. The NE analysis of the game demonstrated the existence of a mixed strategy NE with each player selecting z and x eigen bases with equal probability.

1.5.6 Correspondence of the Bell inequality with Bayesian games

In order to efficiently analyse the benefits of nonlocality in computational tasks, a special class of games known as Bayesian games [Harsanyi, 1967a,b,c] serves as the best tool to represent quantum correlations as they contain the required element of incompleteness in terms of partial information about other players. In fact, the type of atleast one player in the game is a random variable. The first link between Bayesian games and nonlocality was proposed to demonstrate the relation between the game's payoffs and Cereceda inequalities [Cheon and Iqbal, 2008; Cereceda, 2001]. Later, Brunner and Linden showed a direct correspondence between the Bell inequality and payoffs of a general two player Bayesian game [Brunner and Linden, 2013]. In the analysis, the structure of the CHSH game is utilized in settings of a Bayesian game, where players are considered to be of different types ('x_A' and 'x_B') depending on inputs ('x' and 'y') they receive from the referee. For instance, input $x = 0$ corresponds to type 0 of Alice, i.e., $x_A = 0$; input $x = 1$ corresponds to type 1 of Alice, i.e., $x_A = 1$; input $y = 0$ corresponds to type 0 of Bob, i.e., $x_B = 0$; and input $y = 1$ corresponds to type 1 of Bob, i.e., $x_B = 1$. Moreover, outputs ('a' and 'b') define the strategies ('y_A' and 'y_B') that the players opt for. Thus, in order to maintain the structure of a Bayesian game similar to the winning conditions of a CHSH game, when $x_A = x_B = 0$, or $x_A \neq x_B$, Alice and Bob get a non-zero payoff on choosing strategies (y_A and y_B) such that $y_A \oplus_2 y_B = 0$. Similarly, to obey the CHSH settings, when $x_A = x_B = 1$, the players get a non-zero payoff on choosing strategies $y_A(y_B) = 0(1)$ or $y_A(y_B) = 1(0)$. Hence, the overall condition of win in a CHSH game ($x_A \cdot x_B = y_A \oplus_2 y_B$) enables quantum players to exploit nonlocal correlations existing in the shared quantum system to increase the winning probability in comparison to classical strategies. Table 1.6 shows payoffs attained by different types of Alice and Bob in a game with the above defined settings. In each cell, the first number represents the payoff of Player 1, i.e., Alice, and the second number represents the payoff of Player 2, i.e., Bob.

Table 1.6 : Payoffs of Alice and Bob in a general game setting where dependence of payoffs on type of players commensurate with the input-output relation in a CHSH game (Here, u_1^A, u_1^B, u_2^A, u_2^B, u_3^A, u_3^B, u_4^A, and u_4^B are non-zero)

Bob Alice	$y_B = 0$	$y_B = 1$
$y_A = 0$	u_1^A, u_1^B	$0, 0$
$y_A = 1$	$0, 0$	u_2^A, u_2^B

(a) $x_A \cdot x_B = 0$

Bob Alice	$y_B = 0$	$y_B = 1$
$y_A = 0$	$0, 0$	u_3^A, u_3^B
$y_A = 1$	u_4^A, u_4^B	$0, 0$

(b) $x_A \cdot x_B = 1$

1.6 SCOPE OF THE THESIS

The advantages of quantum entanglement and nonlocality have shifted the focus of computation to quantum paradigm instead of the conventional classical computation. In the last three decades, the scientific community has not only taken a giant step towards understanding the fundamentals of quantum information and computation, but also has worked towards practical realization of a quantum computer. However, considering the technological difficulties in scaling up quantum resources, a fault tolerant quantum computer seems to be a rather distant dream, therefore the discussions regarding Noisy Intermediate Scale Quantum technology, where quantum computers comprising 50-100 qubits may be available, are gathering momentum. Nevertheless, there are still many interesting questions in foundations of quantum information and computation that requires a much better physical interpretation. For example, role of entanglement and nonlocal correlations exhibited by partially entangled pure states or mixed states is an area worth exploring for new avenues in quantum information and computation. The intricacy of problem increases even further if one considers the effects of decoherence on these correlations. Interestingly, the diverse academic domains of game theory and quantum computation were merged together as soon as the advantages of foundations of quantum mechanics were realized for computation. This marked the advent of quantum game theory, and since then various studies have been performed in the area. The analysis of foundations of quantum information and computation, and communication protocols using game theory generated significant interest among researchers after the seminal contributions from Eisert *et al.* and Meyer.

In the present Thesis, we represent quantum cryptographic protocols as games (chapter-2 and 3), and vice-versa (chapter-5). Moreover, the effect of noise is portrayed as a game for efficiently analysing the role of nonlocal correlations in real conditions (chapter-4). In addition, Bayesian game representation of Bell-CHSH inequality is studied for different maximally and non-maximally entangled pure states and mixed states (chapter-6). This Thesis is organized in 7 chapters and the content of each chapter is described briefly as follows.

In **chapter-1**, basic concepts and terminologies used in quantum information processing and game theory are described. Precisely, the chapter presents a brief review of literature addressing problems in quantum game theory, which lays foundation for the research described in further chapters of the Thesis.

In **chapter-2**, Ping-Pong protocol is analysed from the point of view of a game. The analysis results in understanding the different strategies of a sender and an eavesdropper to gain the maximum payoff in the game. The study presented in this chapter characterizes strategies that lead to different NE. Further, the conditions for Pareto-optimality depending on the parameters used in the game are also discussed. Moreover, the chapter contains brief analysis of LM05 protocol and its comparison with Ping-Pong protocol from the perspective of a generic two-way quantum key distribution game, with or without entanglement. The results provide an efficient understanding of general two-way quantum key distribution protocols in terms of the security and payoffs of different stakeholders in the protocol.

Further, the Ping-Pong protocol is analysed using different sets of non-maximally entangled three-qubit states in **chapter-3**. Interestingly, our results show that the non-maximally entangled non-orthogonal three-qubit states are more useful as resources in comparison to three-qubit maximally entangled GHZ states. The properties of orthogonal set of non-maximally entangled states as resources for the protocol, however, are similar to that of maximally entangled GHZ states – both the states are not preferable due to the vulnerability towards eavesdropping. On the other hand, non-maximally entangled non-orthogonal basis set holds importance for transferring two-bit information, one each from a sender, to a single receiver. The protocol is further analysed for various eavesdropping attacks, and the results are compared with the use of two shared Bell pairs for two-bit information transfer. Surprisingly, the use of non-maximally entangled non-orthogonal set of states is found to offer better qubit efficiency and increased security, as against the use of two separate maximally entangled Bell states with orthogonal basis. In addition, a mixed-state sharing protocol is also proposed so as to further enhance the security of the protocol. Finally, we extend the analysis presented in the chapter in the framework of a quantum game.

Nonlocal correlations in a quantum mechanical system hold an indispensable place in understanding the foundational aspects of theory; and for exploring efficient theoretical and experimental proposals in the regime of quantum computation and information which are otherwise not possible using classical resources. One of the possible ways to understand the nuances of nonlocal correlations is to put it in the framework of game theory. For this purpose, **chapter-4** addresses the issue of decoherence and protection of nonlocal correlations from local noise from the perspective of a game, considering the two players as noise and weak measurement reversal operations, respectively. In order to effectively understand the moves of players, maximum payoff and NE strategies are studied for different noisy channels. The results compare two different situations where payoffs of players are defined using the Bell inequality and discord, respectively. The analysis shows a contrasting description of payoffs and strategies in two different cases. The results obtained here shed light on the intricacies involved in the process of entanglement distribution through noisy channels, evaluating optimal parameters to obtain maximum payoff in the designed game, and NE strategies of players to win the desired game.

In **chapter-5**, the role of degree of entanglement is analysed for Vaidman's game in a setting where the players share a set of non-maximally entangled three-qubit states. The results show that the entangled states combined with quantum strategies may not be always helpful in winning a game as opposed to the classical strategies. Moreover, it is shown that a special class of W states can always be used to win the game using quantum strategies irrespective of the degree of entanglement between the three qubits. This analysis also helps in comparing the Vaidman's game with the secret sharing protocol. Furthermore, a new Vaidman-type game is proposed where the rule maker itself is entangled with the other two players and acts as a facilitator to share a secret key with the two players. For practical purposes, the analysis is extended to study the proposed game under noisy conditions. In addition, the results obtained here are also generalized for designing multi-qubit games.

Chapter-6 demonstrates the analysis of different Bayesian games where payoffs of players depend on the types of players involved in a two-player game. The dependence is assumed to commensurate with the CHSH game setting. For this, two different types of each player (Alice and Bob) are considered in the game, thus resulting in four different games clubbed together as one Bayesian game. Considering different combinations of common interest, and conflicting interest coordination and anti-coordination games, it is found that quantum strategies are always preferred over classical strategies if the shared resource is a pure non-maximally entangled state. However, when the shared resource is a class of mixed state, then quantum strategies are useful only for a given range of the state parameter. Surprisingly, when all conflicting interest games (Battle of the Sexes game and Chicken game) are merged into the Bayesian game picture, then the best strategy for Alice and Bob is to share a set of non-maximally entangled pure states. It is shown that this set not only gives higher payoff than any classical strategy, but also outperforms a maximally entangled pure Bell state, mixed Werner states, and Horodecki states. In the second half of the chapter, a general framework of a special class of Bell inequality- tilted Bell inequality, is proposed. The game is then studied as a common as well as conflicting interest Bayesian game. Thereafter, the effect of sharing an arbitrary two-qubit pure state and a class of mixed state as quantum resource is studied in those games; thus verifying that non-maximally entangled states with high randomness help attain maximum quantum benefit.

Chapter-7 provides a summary of contributions made through the dissertation, along with possible future directions. This is followed by the bibliography information.

…