7
Conclusions and Future scope

The advent of quantum mechanics and its role in quantum information processing and computing initiated a plethora of discussions spanning various applications such as teleportation, dense coding, entanglement swapping, secret sharing, cryptography, design of algorithms, and many others. Quantum game theory is an emerging field of study which captures the game-theoretic perspective of advantages in the quantum world. There are several efficient proposals of games which clearly depict the dominance of quantum players, using superposition of bits, i.e. qubits, and/or performing quantum operations on the shared state as strategies in the game, over classical players. Moreover, these games also hold correspondence to quantum information processing protocols or algorithms. In all such cases, the basic essence behind achieving quantum benefit is the (shared) initial resource, i.e., a quantum state. The quantum state used in the games can be pure or mixed, and may possess different degree of entanglement. Till now, very few studies analyse the advantages offered by non-maximally entangled states and mixed states as quantum resources in classical or quantum games. The Thesis summarizes our contributions in analysing different aspects of quantum game theory while studying the role of entanglement and mixedness of quantum states. The following paragraphs summarize the discussions and results obtained in previous chapters.

In the first part of the Thesis, the Ping-Pong protocol has been analysed from the perspective of a game. For this, different encoding and eavesdropping strategies are considered as strategies of the sender and the eavesdropper, respectively. The approach follows detailed analysis of pure strategy NE in the game. A relation is established between the NE and payoffs of the sender and the eavesdropper, emphasizing the dependency on the values of weights assigned to mutual information between different players, probability of detection of the eavesdropper, and number of operations applied by an eavesdropper to intervene the secret message. The study also unveils the strategies preferred by the sender to minimize the payoff of an eavesdropper. Moreover, the conditions at which the NE will be pareto-optimal are also described in detail. In order to study general two-way key distribution protocols with and without entanglement, a comparative analysis was performed between the PPP and LM05 protocol. Similar to the PP protocol, the payoffs of players- sender and eavesdropper- depend on weights attached to different terms used in the design of the game, such as mutual information between different players, probability of detection of the eavesdropper, and quantum bit error rate. For our analysis, we considered different types of eavesdropping attacks such as IR attack, DCNOT attack, and Wójcik's attack. This study, described in chapter-2, laid in-depth outlook on the strategies chosen by a sender and an eavesdropper in a protocol to get a better reward in the designed game set-up.

We further discussed the transfer of two-bit information using Ping-Pong protocol. The analysis suggested some interesting results for a multiparty PP protocol. Our results established that three-qubit non-orthogonal non-maximally entangled states are a better resource than two two-qubit maximally entangled Bell states for transfer of two bit information using PPP. Although the use of non-orthogonal states in the protocol involved probabilistic distinguishing of quantum states by POVM, these states still contribute in attaining better qubit efficiency and security as compared to maximally entangled Bell states. The overall comparison of security against various

eavesdropping operations for sharing a three-qubit non-orthogonal non-maximally entangled state, a maximally entangled GHZ state, and two maximally entangled Bell states, is clearly tabulated in chapter-3. The analysis concluded that the information shared between the sender and the receiver using a GHZ state is lesser as compared to other two resources. Moreover, an eavesdropper escapes the detection in at least 25% noisy channel, when a GHZ state is used in the PPP. Furthermore, by slightly compromising on the protocol's qubit efficiency, the study also directed an efficient proposal of mixed sharing of three-qubit non-orthogonal non-maximally entangled states and maximally entangled GHZ states in order to enhance security against various eavesdropping attacks. In addition, the protocol can also be used for a quantum dialogue using non-maximally entangled state with the aim of escalating the efficiency of information transfer.

With the discussion about PPP as a game, and its three-qubit counterpart where our study indicated the usefulness of a non-maximally entangled state over the maximally entangled state, in chapter-4, we extended our analysis in form of another representation as a game. For this, we considered the inevitable presence of noise in quantum channels. For example, when a quantum state is distributed to different parties, there is no guarantee of it being sent through an ideal noise-free path. However, in real situations, environmental noise affects the quantum correlations and degree of entanglement present initially in the original quantum state. Fortunately, there are several methods of prevention of loss of important quantum correlations in a quantum system. One such method is the application of weak measurement and its reversal operations on qubits. The study presented in chapter-4 personifies noise as a player, and the preventive strategy acting against noise as another player. It is assumed that the noise player wishes to reduce the nonlocal correlations as much as possible. On the other hand, the preventive player applying weak measurement wishes to reverse the actions of the noise player. This approach gives a novel outlook to the problem of noise. For a better understanding of the effects of noise and weak measurement operations on nonlocal correlations, nonlocal correlations are quantified using the Bell operator and geometric discord in two separate game settings. Thereafter, pure strategy NE for these games is evaluated. The analysis is carried out for an amplitude damping, a phase damping, and a depolarizing noise. An elaborate analysis for maximum payoffs of players and NE in the game is demonstrated in this chapter. Overall, the analysis brings out a detailed insight in a two-player (noise and weak measurement) game, while specifically indicating the best weak measurement parameters corresponding to different noisy channels for a given state parameter of an arbitrary two-qubit state.

Furthermore, the Thesis also addressed the role of degree of entanglement for Vaidman's game in chapter-5. The dependency of success probability of winning the game using three-qubit entanglement in the shared quantum state is presented in detail. The results interestingly demonstrated that entanglement and quantum strategies may not be always useful in winning the game. A set of GHZ class and W class states were found, for which classical strategies are proved to be better than the quantum strategies. However, quantum strategies were found to be always better than the classical strategies in winning the game in case of a special class of W-type states, i.e., W_n states. We further demonstrated a similarity between the Vaidman's game using general three-qubit pure states and the protocol of quantum secret sharing. This enabled the proposal of an efficient game, where rule-maker of the game is itself entangled with other two players. Similar to the correspondence of QSS with the Vaidman's game, the proposed game was shown to have correspondence and practical application as a facilitated secret sharing protocol. In the protocol, a facilitator verifies if the players in the game are honest or not, as well as allows sharing of information between them simultaneously. Clearly, the rule-maker or facilitator in the game aborts the process of information transfer as soon as the players are proven to be cheats. These games have also been studied under real situations, i.e., their winning probabilities under noisy conditions are obtained. For this, amplitude damping, depolarizing, and phase flip channels are taken into consideration. Interestingly, when two qubits of a three-qubit GHZ state are subjected

to amplitude damping channel, they still help attain more winning probability than that achieved classically. Moreover, analysis of similar games has been further extended for more than three players, involving four, five, and six players. GHZ states proved to be useful for all extensions, because of the benefit of 100% winning prospects. We found that the multi-player extensions of the Vaidman's game also hold similar correspondence to multi-party quantum secret sharing. Therefore, the study effectively highlights transition from a game model to quantum cryptography, and its subsequent extension in multiple dimensions.

Recent years witnessed a strange connection between two completely unrelated and diversified fields, quantum nonlocality and Bayesian games due to the common element of incompleteness in both of them. Most Bayesian games holding relation with Bell and Bell-type inequalities demonstrated reliability on maximally entangled states for getting better payoff than classical players. In this work, the utility of all pure two-qubit entangled Bell states, set of Werner, and Horodecki class states as resources is compared with the classical strategies for Bayesian games. The obtained results reflect that players sharing a two-qubit maximally or non-maximally entangled pure states have an edge over the players sharing a Werner or a Horodecki class states. Furthermore, a fully conflicting interest Bayesian game was designed as opposed to the previous Bayesian games where interests of players did not conflict for all types of player combinations. Similar observations are found in fully conflicting interest Bayesian games confirming that all pure states contribute to higher payoff than the classical limit. However, surprisingly in case of pure states, a specific range of non-maximally entangled states showed more payoff as compared to a maximally entangled Bell state. Interestingly, sets of mixed states violating the Bell-CHSH inequality were not found useful in the designed game, as they led to lesser payoff than classical strategies. Apart from this, a general Bayesian game representation of the tilted Bell-CHSH inequality is formulated, and the use of all pure two-qubit entangled Bell states, set of Werner, and Horodecki class states is witnessed for the game at varying tilt parameter.

Following the analysis presented in the Thesis, security of several other quantum cryptographic protocols can be studied using the game-theoretic model similar to the one proposed for PPP, and a general two-way QKD protocol including LM05 protocol. Clearly, it will be interesting to analyse, characterize, compare, and generalize the usefulness of non-maximally entangled states as against maximally entangled states in quantum cryptography protocols. Another dimension would be to extend and generalize the PPP with efficient modifications in order to witness the improvements on using three-qubit non-maximally non-orthogonal entangled states. One of the problems of interest can be evaluation and comparison of mixed strategy Nash equilibriums to pure strategy Nash equilibriums in these games.

Considering the effects of noise on coherence, it is imperative to analyse the nuances of noise and associated protective measurements from noise. We believe that the demonstration presented in the Thesis to study the adverse effects of decoherence as a game between two players can further be efficiently extended to describe and compare the usefulness of different protective measures including weak measurement techniques that preserve non-local correlations in presence of noise. The game-theoretic study presented in this Thesis will, therefore, be beneficial to researchers working in theory as well as experiments.

Moreover, it would be interesting to study such games in repeated setting where every player will learn from his/her past strategies in taking different moves and act accordingly. Thus, extension of our work can be visualized in terms of repeated games with the aid of quantum automata theory. Furthermore, one can propose and analyse new games and establish their relations with quantum cryptographic protocols. As discussed in the Thesis, for an efficient analysis and physical interpretation, one can further characterize the role of multiqubit entanglement and nonlocality for pure and mixed states in such games and protocols. We further

believe that an extension of the strategy space, and generalized parameters in a game setting will provide an extensive insight into the usefulness of different pure and mixed states in fully conflicting as well as Dilemma-involving Bayesian games.

…