5
Partially entangled states in Vaidman'-type games and its application in Quantum Secret Sharing

5.1 INTRODUCTION

Most of the past work in quantum game theory demonstrates that quantum strategies give better results in comparison to classical strategies. For instance, quantum strategies can be efficiently utilized by a player to defeat his classical opponent in a classical penny flip game which has direct relation to certain quantum algorithms [Meyer, 1999]. Similarly, quantum mechanics also helps in providing a solution to avoid the Prisoners' dilemma [Eisert *et al.*, 1999]. The quantum version of Prisoners' dilemma game was further implemented experimentally using an NMR quantum computer [Du *et al.*, 2002]. Contrary to the dominance of quantum strategies in characterizing a quantum game, Anand demonstrated an interesting result for a particular penny flip game such that a player opting for a mixed strategy can still win against a player opting for a quantum strategy where two players share an entangled state [Anand and Benjamin, 2015]. Therefore, it becomes important to understand and analyse the role of entanglement and nonlocality in game theory. Furthermore, there is also a need to study and analyse the importance of using different entangled quantum systems under different game settings to characterize the benefits of such entnangled systems in various situations.

In this chapter, we analyse a game proposed by Vaidman [Vaidman, 1999] and described in detail in subsection 1.5.4 of Chapter 1. As discussed, a team of three players always wins the game when they share a three-qubit maximally entangled GHZ state. On the other hand, when players opt for pure classical strategies, the team wins the game in utmost $3/4$ cases. In this chapter, we revisit Vaidman's game considering two different classes of three-qubit entangled states, namely, GHZ class [Greenberger *et al.*, 1990] and W class of states [Dür *et al.*, 2000]. Our aim is to analyse the role of entanglement in Vaidman's game by establishing a relation between the winning probability of Vaidman's game [Vaidman, 1999] and the degree of entanglement of various three-qubit entangled states used as a resource in the game. Our analysis demonstrates that for the GHZ class, there are set of states for which classical strategies give better winning probability than quantum strategies. Instead of sharing GHZ class states, if players share a special class of W states, quantum strategies always give an upper edge over classical strategies irrespective of degree of entanglement. We further establish a direct correspondence between Vaidman's game and QSS [Hillery *et al.*, 1999].

Moreover, we also propose a similar game, where one of the players sharing the three-qubit entanglement is the facilitator and defines the rules of a game played by the other two players. A close examination of the proposed game shows that the rule-maker benefits whenever the other two players share a non-maximally entangled state. By sharing a non-maximally entangled state, the rule-maker is able to modify rules such that the other two players loose the game. To analyse further, we extend our discussion to study the proposed game in a noisy environment. For our purpose, we again consider the examples of an amplitude damping, a depolarizing channel and a phase flip channel [Nielsen and Chuang, 2011]. Our results show that in case of W states, the quantum winning probability exceeds the classical winning probability even if qubits pass through a phase flip channel. For GHZ states, the quantum success probability is almost always more than the classical success probability when qubits pass through a phase flip or an amplitude damping channel. In all other cases, quantum strategies are found to be better than classical strategies for a fixed range of noise parameters only. Moreover, in Section 5.3, we suggest an application of the proposed game for facilitated secret sharing between three parties, where one of the players is a facilitator and also controls the secret sharing protocol. In later sections of this chapter, we also demonstrate a generalization of Vaidman's game and the proposed game for multiple players. The fact that the quantum resources used in this work can be experimentally prepared [Bouwmeester *et al.*, 1999; Eibl *et al.*, 2004; Dong *et al.*, 2016], suggests that the results obtained here may have strong applicability in QSS or other similar protocols.

5.2 CORRESPONDENCE OF VAIDMAN'S GAME WITH QUANTUM SECRET SHARING

There is a direct correspondence between the QSS protocol [Hillery *et al.*, 1999] described in Chapter 1.3.4 to the Vaidman's game [Vaidman, 1999] discussed in Section 1.5.4. The set of random basis (XXX, XYY, YXY, and YYX) that are accepted for formulation of a shared secret message in the QSS protocol are the questions the three players, namely Alice, Bob, and Charlie, are asked in Vaidman's game. Further, the winning conditions in this game are also the same as the measurement outcomes of the three users in QSS protocol sharing a standard GHZ state, and measuring their qubits in an appropriate basis. As per the description of the game in Section 1.5.4, three players can win the game if the product of their answers is 1 when all of them are asked the X question or -1 if one of them is asked the X question and rest of them are asked the Y question. Clearly, three players sharing a maximally entangled three-qubit GHZ state always win the game because of the strong correlations between the three qubits of the GHZ state. For example, the three qubits in the GHZ state are correlated as

$$\begin{aligned} &\{M_A^X\}\{M_B^X\}\{M_C^X\} = 1 \\ &\{M_A^X\}\{M_B^Y\}\{M_C^Y\} = -1 \\ &\{M_A^Y\}\{M_B^X\}\{M_C^Y\} = -1 \\ &\{M_A^Y\}\{M_B^Y\}\{M_C^X\} = -1 \end{aligned} \tag{5.1}$$

where $\{M_i^X\}$ is the measurement outcome of the i^{th} player measuring her/his qubit in the X basis, and $\{M_i^Y\}$ is the measurement outcome of the i^{th} player measuring her/his qubit in the Y basis. Hence, the above discussion establishes a clear correspondence between the Vaidman's game and the QSS protocol. In the following sections, this correspondence is used to establish a secure key between users in a QSS protocol.

5.2.1 Use of GHZ class states

The Vaidman's game is analysed in a more general set-up where the three players share a general GHZ state represented in Eq. (1.12), instead of sharing a maximally entangled GHZ state as discussed in the original game. As shown in Figure 5.1, when the players share a general GHZ state, the success probability of winning the above defined game varies from 0.5 to 1. For simplicity, it is assumed that the probability of players being asked the set of 4 questions (XXX, XYY, YXY, YYX) is equally likely. In Figure 5.1, the winning probability of the game, i.e, $\frac{1}{2}(1 + sin2\theta)$ is plotted against the entanglement measure. It can be clearly seen that the players win the game with 100% certainty only for the maximally entangled state, i.e., when degree of entanglement τ attains its maximum unit value (at $\theta = \pi/4$). For all other values of three-tangle where $0 < \tau < 1$, the winning probability is always less than one (which the players achieve by sharing a maximally entangled GHZ state). Interestingly, only the set of states with $\tau > 0.25$ achieve better success probability than the classical success rate (75%) of the game. At $\tau = 0.25$, quantum strategies have equal prospects of enabling win to the quantum players, as the best classical strategy. Additionally, for the set of states with $\tau < 0.25$, classical strategies are more beneficial in comparison to quantum strategies.

Hence, for Vaidman's game, entanglement or quantum strategies do not guarantee a sure-shot win as against classical strategies.

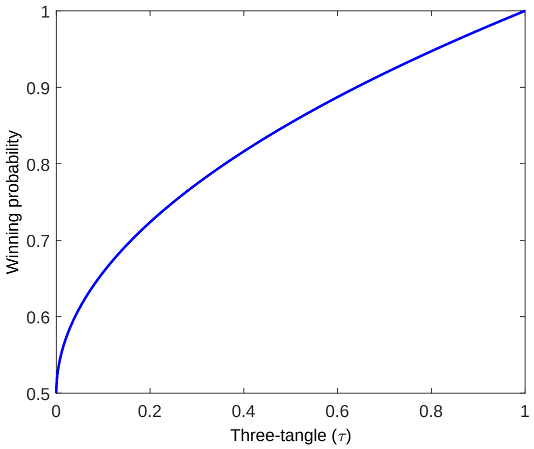

Figure 5.1 : Success probability of winning Vaidman's game using GHZ-type states

5.2.2 Use of W class states

Although W-type states belong to another inequivalent class of three-qubit states, they can also be used as resources in winning Vaidman's game with a slightly varying set of questions. For example if W states are used as resources instead of GHZ states, the players may be asked either "What is Z?" or "What is Y?". Similar to the GHZ case, the answers to these questions can be either +1 or -1. Moreover, the rules are set-up in a way that either all players are asked the Z question; or one of the players is asked the Z question and the remaining two are asked the Y question. The players win the game if the product of their answers is -1, if all are asked the Z question; and +1, in all other cases. If the players share the standard W state, given in Eq. (1.15), before beginning to play the game, then they can win this game with a probability of 0.875. On similar grounds as discussed in Section 5.2 that QSS directly commensurate with the Vaidman's game, the standard W state can be effectively used for probabilistic QSS [Hillery *et al.*, 1999]. Similar to the case of GHZ class, here, the winning probability of the Vaidman's game is studied if the three players share a general W-type state as shown in Eq. (1.13). Considering the rules of the game, it is found that the

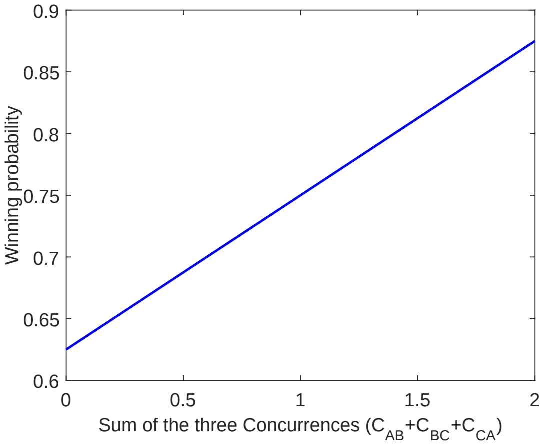

Figure 5.2 : Success probability of winning Vaidman's game using W-type states

winning probability of the team is $\frac{1}{4}\left(\frac{5}{2}+bc+ab+ac\right)$, if the players share a general W state. This value is attained assuming that the team will be asked the set of 4 questions (ZZZ, ZYY, YZY, YYZ) with equal probability. The plot of winning probability of Vaidman's game versus the sum of three residual concurrences [Hill and Wootters, 1997; Wootters, 1998, 2001] is demonstrated in Figure 5.2. The figure demonstrates that the winning probability of Vaidman's game linearly increase with the sum of residual concurrences for W-type states. Furthermore, the plot also indicates that the winning probability of Vaidman's game is always greater than the classical winning probability for W-type states having sum of two-qubit concurrences greater than 1. Moreover, the highest winning probability of 0.875 can be achieved for $a=b=c=\frac{1}{\sqrt{3}}$, which is for the standard W state, given in Eq. (1.15).

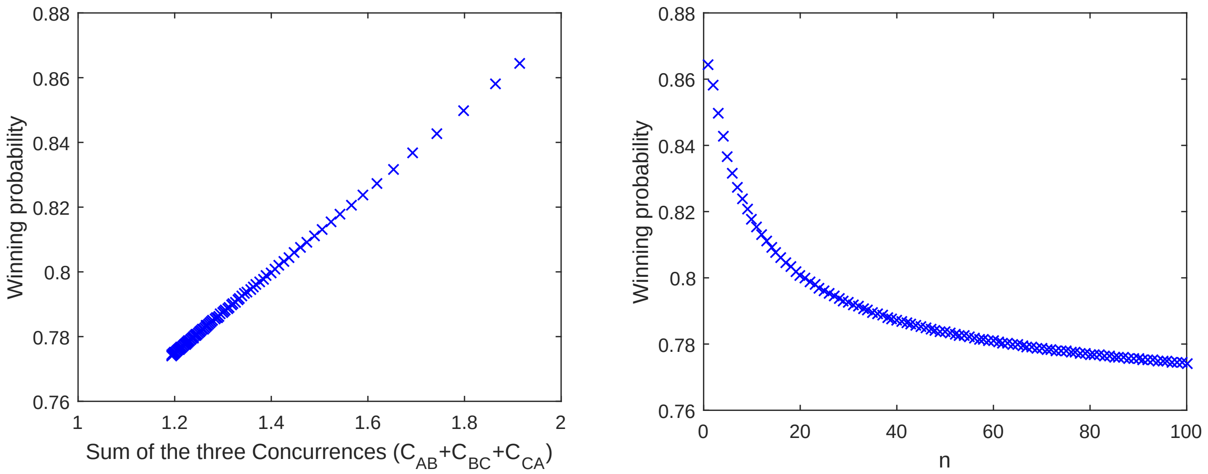

Figure 5.3 : Success probability of winning Vaidman's game using W_n states

Although the use of non-maximally entangled states as resources, in general, leads to probabilistic information transfer [Karlsson and Bourennane, 1998; Shi and Tomita, 2002], Pati and Agrawal [Agrawal and Pati, 2006] have shown that there exists a special class of W-type states which can be used for perfect teleportation and dense coding. Such states can be represented as

$$|W_n\rangle = \frac{1}{\sqrt{2(1+n)}}(|100\rangle + \sqrt{n}e^{i\gamma}|010\rangle + \sqrt{n+1}e^{i\delta}|001\rangle) \tag{5.2}$$

where n is a positive integer and δ and γ are relative phases. The efficient applications of these states [Agrawal and Pati, 2006] in quantum information and computation led to address the role of non-maximally entangled states in quantum information processing [White *et al.*, 1999; Mozes *et al.*, 2005; Wang *et al.*, 2009; Liang *et al.*, 2013]. Considering their usefulness as non-maximally entangled three-qubit states in quantum information, here, the role of W_n states is further investigated for their utility in Vaidman's game as well. It is observed that the winning probability of the game while the player share W_n states as resource is given by $\frac{1}{8(n+1)}(5+5n+\sqrt{n+1}+\sqrt{n}(\sqrt{n+1}+1))$. Unlike the case of general GHZ or W states where the success probability exceeds the classical limit only after a certain threshold as measured by an entanglement measure, Figure 5.3 clearly depicts that if the three players share W_n states, then the success probability is always greater than the classical success probability, independent of the value of sum of residual concurrences. Interestingly, the figure further shows the dependence of winning probability of the game on state parameter n. The plots highlight that the highest winning probability is 0.86425, which is attained for $n=1$ when the sum of three residual concurrences is 1.914. Nevertheless, the winning probability is always greater than the one obtained using classical strategies. The analysis presented here from the perspective of Vaidman's game adds another dimension to the importance of W_n states as resources in comparison to other non-maximally entangled W or GHZ states.

5.2.3 A comparison of the use of GHZ and W states

The above analysis suggests that although a standard GHZ state achieves 100% success probability in winning the Vaidman's game which is more than the 87.5% winning probability achieved by the standard W or 86.4% winning probability achieved by the W_1 state; only the set of GHZ-type states with a value of $\tau > 0.25$ are useful for obtaining the success probability greater than the one obtained using classical strategies. However, GHZ states with $\tau > 0.5625$ and $\tau > 0.5307$ give better results as compared to standard W state, and W_1 state, respectively. In addition, only limited class of W-type states with the sum of three residual concurrences greater than one, can be beneficial for winning the game. However, a special class of W-type states, i.e. W_n states always result in better prospects of winning the Vaidman's game, in comparison to any classical resource or strategy, for all values of n and sum of three residual concurrences.

5.3 A TWO-PLAYER GAME WHERE THE FACILITATOR IS ENTANGLED WITH BOTH THE PLAYERS

The basic premise of Vaidman's game can be efficiently utilized in another interesting game set-up, where the rule-maker itself is entangled with the players playing a two-player Vaidman-type game. In our proposed game, Alice, Bob, and Charlie share a three-qubit entangled state. Charlie prepares the state and distributes one particle each to Alice (A) and Bob (B), keeping one (C) particle with himself. Charlie strikes a deal with Alice and Bob, and agrees to help them if they win the game as per the rules defined by him. For this, Charlie measures his qubit in a general basis given by

$$|b_0\rangle = sin\lambda|0\rangle - cos\lambda|1\rangle; \qquad |b_1\rangle = cos\lambda|0\rangle + sin\lambda|1\rangle \tag{5.3}$$

Charlie, after completing his measurement, asks one of the questions "What is X?" or "What is Z?" to the team. In the proposed game, Alice and Bob are not allowed to discuss their answers to the questions asked, and have to announce their individual answers. Since the answers correspond to measurement outcomes, their answers can be either $+1$ or -1. If the team is asked the X (Z) question, both Alice and Bob measure their qubits in X (Z) basis and announce their measurement outcomes as answers to the asked questions. Charlie decides the rules of the game based on his measurement outcomes, i.e.,

$$|b_0\rangle_C : \quad \{M_A^X\}\{M_B^X\} = 1 \qquad \{M_A^Z\}\{M_B^Z\} = -1 \tag{5.4}$$

$$|b_1\rangle_C : \quad \{M_A^X\}\{M_B^X\} = -1 \qquad \{M_A^Z\}\{M_B^Z\} = 1 \tag{5.5}$$

If Charlie's measurement outcome is $|b_0\rangle$, he declares the winning condition to be the one listed in Eq. (5.4), and if his measurement outcome is $|b_1\rangle$, he declares the winning condition to be the one listed in Eq. (5.5). Here, $\{M_i^X\}$ represents the measurement outcome when the i^{th} player measures her/his qubit in the X basis, and $\{M_i^Z\}$ represents the measurement outcome when the i^{th} player measures her/his qubit in the Z basis.

In order to study the use of different quantum resources in this game, firstly it is considered that Charlie prepares a three-qubit W state as shown in Eq. (1.15). Clearly, the success probability of the team to win this game depends on the parameter λ- governing the basis in which Charlie performs a measurement. The winning probability is evaluated to be $0.916667 - 0.833334cos^2\lambda$. Figure 5.4 shows a plot of winning probability with respect to the parameter λ. The maximum winning probability that a team of two players can achieve is 0.9167 for $\lambda = \frac{\pi}{2}$, i.e., when Charlie

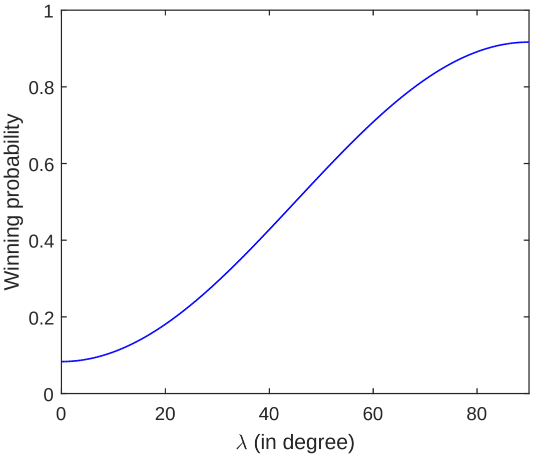

Figure 5.4 : Success probability of winning the proposed game where the rule-maker is entangled with the players using a standard W state

measures his qubit in computational basis ($|b_0\rangle = |0\rangle$ and $|b_1\rangle = |1\rangle$). On the other hand, if Charlie measures his qubit in the basis represented as $|b_0\rangle = |1\rangle$ and $|b_1\rangle = |0\rangle$, i.e. when $\lambda = 0^\circ$, then the winning probability is only 0.0833, i.e. it is highly probable that the team looses the game as opposed to classical winning probability of 0.5. Thus, if Charlie wants to make an easy deal for the team, and eventually help them, he prefers to prepare a standard W state and performs measurement in the computational basis ($|b_0\rangle = |0\rangle$ and $|b_1\rangle = |1\rangle$) so that the team can win the game with a success rate of 91.667%. In this situation, the use of quantum strategy suggested by Charlie is always preferred over classical strategies for the team of Alice and Bob.

For further analysis, it is considered that Charlie prepares a three-qubit GHZ state as shown in Eq. (1.14) and shares the respective qubits with Alice and Bob. In this case, the team has only 50% winning probability irrespective of the measurement basis used by Charlie, which is in fact equivalent to the players opting for any classical strategy, i.e. where the team does not measure its qubits, but randomly announce answers as $+1$ or -1. However, Charlie can change the set of questions as X and Y, instead of X and Z and may ask Alice and Bob to perform measurements in X and Y basis, respectively. Therefore, in such a game set-up, the measurement outcome dependent rules of the game would also be altered to

$$|b_0\rangle_C : \qquad \{M_A^X\}\{M_B^X\} = -1 \qquad \{M_A^Y\}\{M_B^Y\} = +1 \tag{5.6}$$

$$|b_1\rangle_C : \qquad \{M_A^X\}\{M_B^X\} = +1 \qquad \{M_A^Y\}\{M_B^Y\} = -1 \tag{5.7}$$

Hence, if Charlie obtains $|b_0\rangle$ as his measurement outcome, then Alice's and Bob's outcomes must satisfy Eq. (5.6). On the contrary, if Charlie obtain $|b_1\rangle$ as his measurement outcome, then the outcomes of the team should satisfy Eq. (5.7). The success probability of a team winning this game is $0.5(1+sin2\lambda)$, and the maximum winning probability of 1 is attained for $\lambda = \frac{\pi}{4}$, i.e., when Charlie performs a measurement in diagonal basis ($|-\rangle$, $|+\rangle$). In general, Figure 5.5 describes the winning probability of the team for different values of the measurement parameter λ, when the team shares a standard GHZ state as a resource. Interestingly, for this game set-up, the standard GHZ state leads to a winning probability which is always better that the best classical strategy irrespective of the measurement basis used by Charlie. However, the same is not true if one uses the W state as a

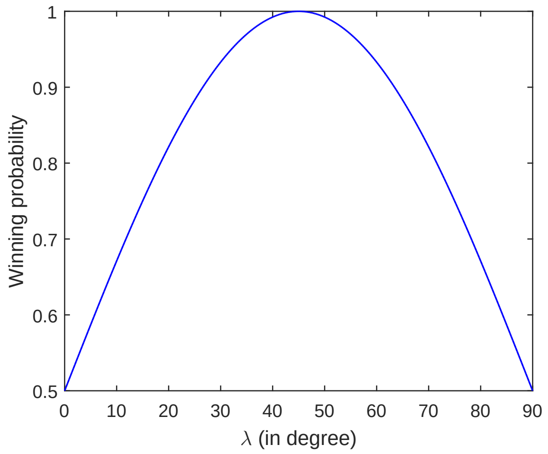

Figure 5.5 : Success probability of winning the proposed game where the rule-maker is entangled with the players using a standard *GHZ* state

resource in this set-up as the winning probability shows better results only for a certain range of the measurement parameter λ.

Table 5.1 : Winning probability of the three-qubit proposed game in a noisy environment

Quantum State	Noise	Winning probability of the game
W state	Amplitude damping	$0.75-0.1667D_1-0.1667D_2$ $+0.1667\sqrt{(1-D_1)(1-D_2)}$
	Depolarizing channel	$0.91667-0.45833D_1-0.45833D_2$ $+0.229167D_1D_2$
	Phase flip channel	$0.91667-0.333D_1-0.333D_2$ $+0.667D_1D_2$
GHZ state	Amplitude damping	$0.5+0.5\sqrt{(1-D_1)(1-D_2)}$
	Depolarizing channel	$1-0.75D_1-0.75D_2+0.75D_1D_2$
	Phase flip channel	$1-D_1-D_2+2D_1D_2$

5.3.1 Analysis of the proposed game in presence of noise

In this subsection, the proposed game discussed above is analysed in a noisy environment to study the nature and robustness of these states under real conditions. This analysis also enables one to study the effect of decoherence on the success rate of the proposed game. It is considered that Charlie prepares a three-qubit state and sends two qubits to Alice and Bob for the game to proceed. These qubits pass through a noisy channel, degrading the correlation between qubits of the state, and thus the success probability of the team (Alice and Bob) may also get affected. The quantum state ρ after passing through a noisy channel changes to $\varepsilon(\rho)$ such that $\varepsilon(\rho)=\sum_i E_i\rho E_i^\dagger$ where $E_i s$ are the operation elements of noise. For our purpose, phase flip, depolarizing, and amplitude damping noisy channels (Section 1.3.5) are considered to study the effect of decoherence on the success probability. In order to compare the effect of three noisy channels on the game using standard W state as a resource, firstly the winning probability of the players is evaluated under

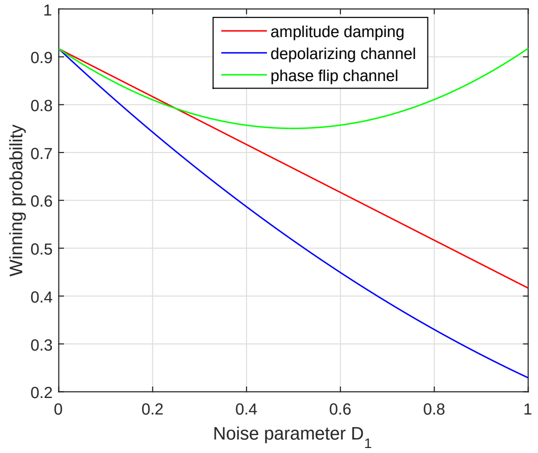

Figure 5.6 : Success probability of winning the game with respect to noise parameter ($D_1 = D_2$) using the standard W state

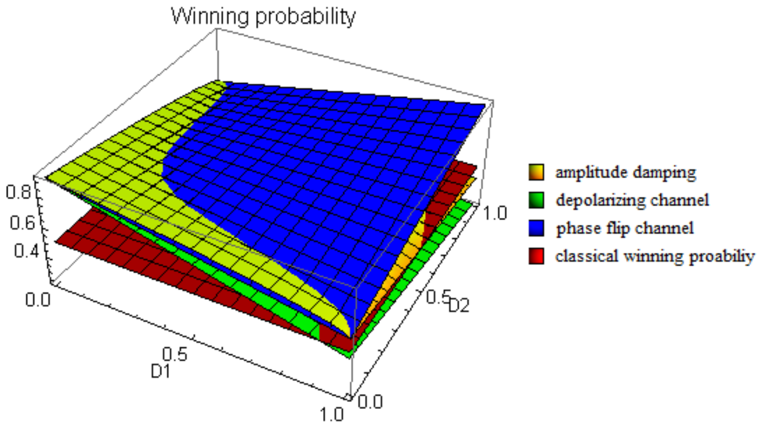

Figure 5.7 : Success probability of winning the game with respect to both the noise parameters ($D_1 \neq D_2$) using the standard W state

noisy conditions in the game. The success probability in such cases is/are listed in Table 5.1. Figure 5.6 demonstrates the success probability of the game with respect to noise parameter D_1 (associated with the noisy channel through which qubit is sent to Alice), assuming that the noise parameters on Alice's (D_1) and Bob's (D_2) qubits are equal. Further, a 3-D plot is shown in Figure 5.7 displaying variance between the winning probability of the game with the two noise parameters D_1 and D_2. Figure 5.6 and 5.7 clearly demonstrate that the winning probability of the game under phase flip noise is more than the winning probability of the game under amplitude damping noise for a large range of noise parameters, and more than the winning probability of the game under depolarizing noise for all noise parameters. Further, the success rate of the game under the phase flip noise is always more than the classical winning probability (0.5). Moreover, our results show that when the players share a W state, the winning probability is more robust towards an amplitude damping channel in comparison to a depolarizing channel. In both the cases however, the success probability falls below the classical winning probability, for higher values of noise parameters. In addition, the winning probability of the game is discussed when a GHZ state is shared in a noisy

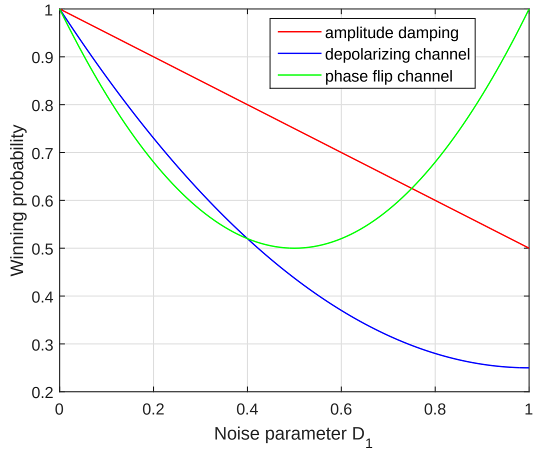

Figure 5.8 : Success probability of winning the game with respect to noise parameter ($D_1 = D_2$) using a maximally entangled GHZ state

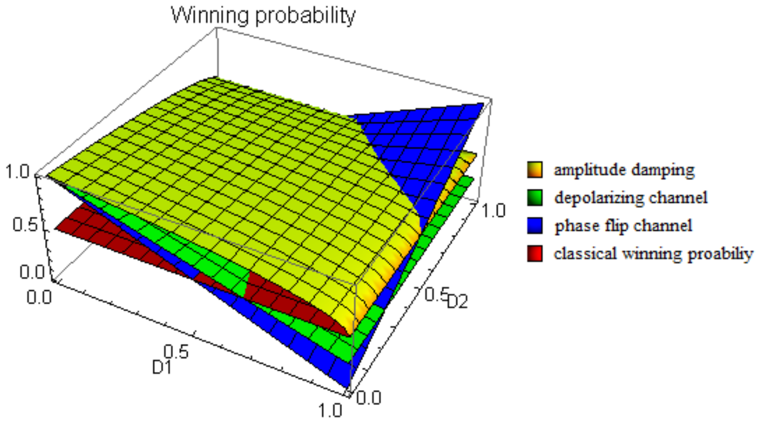

Figure 5.9 : Success probability of winning the game with respect to both the noise parameters ($D_1 \neq D_2$) using a maximally entangled GHZ state

environment. The results are depicted in Figures 5.8 and 5.9. Figure 5.8 shows the relation between winning probability of the game and the noise parameter D_1 assuming that $D_1 = D_2$. Further, Figure 5.9 describes the effect of both the parameters on the success probability of the game. These plots indicate that when both the noise parameters are equal, the game is resistant to phase flip as well as amplitude damping channel, because the then winning probability of the game is almost always greater than the classical winning probability (0.5). However, in case of depolarizing channel, for high value of the noise parameter, winning probability falls below the classical case. Moreover, for $D_1 \neq D_2$, only the success probability in case of an amplitude damping noise exceeds the classical winning probability. In other noisy environments, the winning probability may fall below the classical success probability depending on the ranges of D_1 and D_2.

5.3.2 Applications in quantum cryptography

Since the winning conditions of Vaidman's game are nothing but the premise of QSS protocol, a relation is proposed with applications in secret sharing. The set-up is such that two players, Alice and Bob are kept in two different cells, and are partially disallowed to communicate. Here, partial communication means a type of controlled communication where the players can communicate only under the presence of a facilitator or a controller (Charlie in our case). The facilitator listens the message and has the authority to permit or not permit any communication between the two. In order to accomplish this task, it is preferred to exploit the properties of a standard W state over the use of a W_1 state. The reason for such a preference lies in the success rate of winning Vaidman's game which is 87.5% when a standard W state is shared, as opposed to 86.425% when a W_1 state is shared among the team members. Moreover, it is considered that Charlie performs his measurement in the basis as shown in Eq. (5.3) at $\lambda = \frac{\pi}{2}$.

Table 5.2 : The control mode of facilitated information sharing

Charlie's measurement outcome	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
Alice's basis	Z	Z	X	X	X	X
Bob's basis	Z	X	Z	X	X	X
Is the choice of basis accepted?	yes	no	no	yes	yes	yes
Alice's measurement outcome	$+1$	-	-	$+1$	-1	$+1$
Bob's measurement outcome	$+1$	-	-	$+1$	$+1$	-1
Correlation as expected?	✓	-	-	×	✓	✓
Alice and Bob are asked to announce their outcome and it is checked if their results comply with (12) in more than or equal to 75% cases						

Table 5.3 : The message mode of facilitated information sharing

Charlie's measurement outcome	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
Alice's basis choice	X	X	X	Z	Z	Z
Bob's basis choice	X	X	Z	X	Z	Z
Basis choice accepted?	yes	yes	no	no	yes	yes
Alice's measurement outcome	$\|+\rangle$	$\|-\rangle$	-	-	$\|0\rangle$	$\|1\rangle$
Bob's measurement outcome	$\|+\rangle$	$\|-\rangle$	-	-	$\|1\rangle$	$\|0\rangle$
$\|0\rangle$ and $\|+\rangle$ correspond to secret bit: 0 $\|1\rangle$ and $\|-\rangle$ correspond to secret bit: 1						
Let Charlie announce that Bob should flip his outcome whenever he chooses Z basis for measurement						
Shared secret bit	0	1	-	-	0	1

To share a secret key, Charlie begins by randomly opting for either of the two different modes, namely control mode or message mode. The control mode corresponds to Charlie's measurement outcome $|1\rangle$, and is used to check the authenticity of Alice and Bob, as shown in Table 5.2. Similarly, the message mode corresponds to Charlie's measurement outcome $|0\rangle$, and is used to share a secret key with Alice and Bob, as depicted in Table 5.3. Thus, Charlie prepares "m" standard W states as shown in Eq. (1.15) and distributes the first and second qubit of each state to Alice and Bob, respectively keeping the third qubit with himself. Charlie, then performs a single qubit measurement on his qubit in the computational ($|0\rangle, |1\rangle$) basis. Further, Alice and Bob randomly choose their bases of measurement (either X or Z) and announce their respective choices to Charlie. If they choose two different bases, then their choices are discarded. An alternative to this method is that Charlie randomly chooses a basis of measurement (either X or Z) and announces his choice to Alice and Bob. This will ensure that both Alice and Bob perform measurements in the same basis that Charlie announced. This step is repeated for "m" qubits, wherein Alice and Bob note down the measurement outcomes at each repetition.

If Charlie gets $|0\rangle$ as his measurement outcome, then the measurement results of Alice and Bob will be related as in Eq. (5.4) with certainty. As discussed above, this will be the message mode of the proposed secret sharing scheme, wherein Alice's and Bob's measurement outcomes will either be same or different. The relation between their measurement outcomes is only known to Charlie, which he announces at the end of the protocol. On the other hand, if Charlie gets $|1\rangle$ as his measurement outcome, then the measurement results of Alice and Bob will be related as in Eq. (5.5) in 75% cases. Since this is a control mode, Charlie secretly asks both Alice and Bob to tell their individual measurement outcomes to him, which he verifies to check if anyone (Alice or Bob) is cheating. If the results announced by Alice and Bob comply with the results in Eq. (5.5) less than 75% times, then cheating is suspected. Moreover, as Alice and Bob are not allowed to discuss, they cannot distinguish between the message mode and the control mode unless Charlie announces. If both, Alice and Bob are asked to announce their measurement outcomes, then the control mode of secret sharing is taking place. While, if none of them is asked to announce her/his results, then the message mode of secret sharing occurs. If Charlie suspects cheating in the control mode, he aborts the communication and does not announce the relation between outcomes of Alice and Bob for message runs. However, if Charlie does not find anything suspicious, he announces in the end, which results correspond to message and control mode, and also the relation between the Alice's and Bob's measurement outcomes in the message mode. This protocol, therefore, enables the controller to check a pair of agents for their honesty, and simultaneously allows the sharing of a secret key between them, if both are proved honest.

Instead of sharing a W state, if players in the game share a GHZ state, then Charlie performs his measurement in the diagonal basis as shown in Eq. (5.3) at $\lambda = \frac{\pi}{4}$. Here, the control mode corresponds to the measurement outcome $|-\rangle$ and the message mode corresponds to the measurement outcome $|+\rangle$. The protocol remains the same, i.e., the control mode verifies if Alice and Bob are honest or not, and the message mode leads to sharing of a common secret key between Alice and Bob. In message mode, Alice and Bob randomly choose their bases of measurement (either X or Y) and announce their choice of bases to Charlie. As earlier, if they choose two different bases, then their choices are discarded. If Charlie gets $|+\rangle$ as his measurement outcome, then he knows that the measurement results of Alice and Bob are related as in Eq. (5.7) with certainty. This will be the message mode and the relation between outcomes of Alice and Bob is only known to Charlie, which he announces at the end of the protocol. On the other hand, if Charlie gets $|-\rangle$ as the measurement outcome, then the measurement results of Alice and Bob are related as in Eq. (5.6) in all cases. Similar to the previous protocol, Charlie secretly asks both Alice and Bob to announce their measurement outcomes. If the outcomes announced by Alice and Bob do not always comply with the results in Eq. (5.6), then dishonesty is suspected and the protocol is aborted. Otherwise the players proceeds further so that the three players share a secret key, as in the case described above for the W state.

5.4 AN EXTENSION OF VAIDMAN'S GAME FOR MULTIQUBIT SYSTEMS

For a three qubit system, Vaidman's game has four set of questions, XXX, XYY, YXY, and YYX, with answers $+1$, -1, -1, and -1 respectively. On similar grounds, while sharing four, five, and six qubit systems, 7, 15, and 30 different types of questions, can be asked to the players in the game. For instance, if a four qubit quantum state is shared between four players, then they can be asked the following eight questions: $XXXX$, $XXYY$, $XYXY$, $XYYX$, $YXXY$, $YXYX$, $YYXX$, $YYYY$, i.e. all X questions, all Y questions, or two X and two Y questions. Depending on the different set of questions that can be asked in a game, various different games can be formulated. For example, in case of four players, one can formulate a single game. On the other hand, for a five and six players scheme, one can design two and three distinct games respectively.

In addition, for more than three-player games, it was found that sharing a W state between the players was not beneficial as it leads to lesser winning chances as compared to the one achieved classically. Therefore, with the increase in system's complexity and the number of players, W states are not of much use for this type of game. The GHZ states however are still useful and can be used as shared resources among the players, with a success probability of 100%. Table 5.4 describes the rules of different four, five, and six player games and their winning conditions when the following defined four, five, and six qubit GHZ states are shared between players, respectively.

$$|GHZ_4\rangle = \frac{1}{\sqrt{2}}(|0000\rangle - |1111\rangle) \tag{5.8}$$

$$|GHZ_5\rangle = \frac{1}{\sqrt{2}}(|00000\rangle - |11111\rangle) \tag{5.9}$$

$$|GHZ_6\rangle = \frac{1}{\sqrt{2}}(|000000\rangle - |111111\rangle) \tag{5.10}$$

For example, in a four-player game, either all players are asked the X question or two are asked X and two are asked Y question. The game is won if the product of player's answers is -1 when all are asked X question, and if the product of the player's answers is $+1$ when two are asked the X question and remaining two are asked the Y question. Classically the success probability of the game can not exceed 0.8517. However, a four qubit GHZ state with $\tau_4 \geq 0.51$ always gives better winning probability than the classically achieved probability. Moreover, the players always win the game, when a maximally entangled GHZ state is shared.

Similarly in a five-player game, there are two possibilities of questionnaires. In the first one, either all players are asked X question, or two players are asked Y question, and the remaining three are asked X question. In order to win the game, the team's answers must product to -1 in case of all X questions, and $+1$ in case of two Y and three X questions. The maximum winning probability of the game by all classical means is 0.909. However, by sharing a five qubit GHZ class state with $\tau_5 \geq 0.67$, the players achieve higher winning probability for the game, than by classical methods. In another five-player game set-up, either two players are asked Y question and remaining three players are asked X question, or all except one player (who is asked X question) are asked Y question. Whenever two players are asked Y question, then product of their answers should be $+1$, and whenever four players are asked Y question, then product of their answers should be -1. Although, classically this game can be won with a success probability 0.6667, sharing a five-qubit GHZ state with $\tau_5 \geq 0.11$, always leads to better winning prospects than the classical success rate. Moreover, sharing a maximally entangled five-qubit GHZ state results in a 100% win for the team. Table 5.4 further lists the outcomes of different six player games with the GHZ states as resources.

5.5 A THREE-PLAYER GAME WHERE THE FACILITATOR IS ENTANGLED WITH THE THREE PLAYERS

The following game is an extension of the game proposed in Section 5.3. In this game, Alice, Bob, Charlie, and Dave share a four-qubit GHZ state defined in Eq. (5.8). Dave prepares a four-qubit state and gives one qubit each to Alice (A), Bob (B), and Charlie (C), keeping one (D) qubit with himself. Here, Dave is the rule-maker and thus, he decides the winning conditions for the team (Alice, Bob, and Charlie). For this, Dave measures his qubit in a general basis as shown in Eq. (5.3), and then asks questions "What is X?" or "What is Y?" to the team. Alice, Bob, and Charlie can individually give answer as $+1$ or -1 and are not allowed to discuss before answering. A player who is asked the X (Y) question, measures her/his qubits in X (Y) basis and gives her/his measurement result as the answer.

$$\begin{aligned} &\{M_A^X\}\{M_B^X\}\{M_B^X\} = +1 \qquad &\{M_A^X\}\{M_B^Y\}\{M_C^Y\} \quad &= -1 \\ &\{M_A^Y\}\{M_B^X\}\{M_C^Y\} = -1 \qquad &\{M_A^Y\}\{M_B^Y\}\{M_C^X\} \quad &= -1 \end{aligned} \tag{5.11}$$

Table 5.4 : Generalization of Vaidman's Game for Multi-qubit Systems

Number of players	Winning conditions for the game	Classical winning probability	Range of n-tangle τ_n of GHZ states for which quantum strategies outperform classical strategy
4 Game 1	$XXXX = -1$ $XXYY = XYXY = XYYX = YXXY$ $= YXYX = YYXX = +1$	0.8517	$0.51 \leq \tau_4 \leq 1$
5 Game 1	$XXXXX = -1$ $YYXXX = YXYXX = YXXYX = YXXXY$ $= XYYXX = XYXYX = XYXXY = XXYYX$ $= XXYXY = XXXYY = +1$	0.909	$0.67 \leq \tau_5 \leq 1$
5 Game 2	$YYXXX = YXYXX = YXXYX = YXXXY$ $= XYYXX = XYXYX = XYXXY$ $= XXYYX = XXYXY = XXXYY = +1$ $XYYYY = YXYYY = YYXYY$ $= YYYXY = YYYYX = -1$	0.6667	$0.11 \leq \tau_5 \leq 1$
6 Game 1	$XXXXXX = -1$ $YYXXXX = YXYXXX = YXXYXX = YXXXYX$ $= YXXXXY = XYYXXX = XYXYXX = XYXXYX$ $= XYXXXY = XXYYXX = XXYXYX = XXYXXY$ $= XXXYYX = XXXYXY = XXXXYY = +1$	0.9375	$0.765 \leq \tau_6 \leq 1$
6 Game 2	$YYXXXX = YXYXXX = YXXYXX = YXXXYX$ $= YXXXXY = XYYXXX = XYXYXX = XYXXYX$ $= XYXXXY = XXYYXX = XXYXYX = XXYXXY$ $= XXXYYX = XXXYXY = XXXXYY = +1$ $XXYYYY = XYXYYY = XYYXYY = XYYYXY$ $= XYYYYX = YXXYYY = YXYXYY = YXYYXY$ $= YXYYYX = YYXXYY = YYXYXY = YYXYYX$ $= YYYXXY = YYYXYX = YYYYXX = -1$	0.5	$0 \leq \tau_6 \leq 1$
6 Game 3	$XXYYYY = XYXYYY = XYYXYY = XYYYXY$ $= XYYYYX = YXXYYY = YXYXYY = YXYYXY$ $= YXYYYX = YYXXYY = YYXYXY = YYXYYX$ $= YYYXXY = YYYXYX = YYYYXX = -1$ $YYYYYY = +1$	0.9375	$0.765 \leq \tau_6 \leq 1$

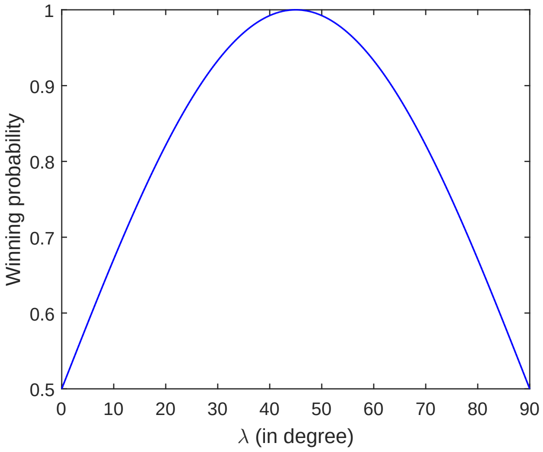

Figure 5.10 : Success probability of winning the proposed game where the rule-maker is entangled with the players using a four-qubit maximally entangled GHZ state

$$\begin{aligned} \{M_A^X\}\{M_B^X\}\{M_B^X\} &= -1 \qquad \{M_A^X\}\{M_B^Y\}\{M_C^Y\} &= +1 \\ \{M_A^Y\}\{M_B^X\}\{M_C^Y\} &= +1 \qquad \{M_A^Y\}\{M_B^Y\}\{M_C^X\} &= +1 \end{aligned} \tag{5.12}$$

If Dave's measurement outcome is $|b_0\rangle$, the winning condition for the game is as shown in Eq. (5.11), and if his measurement outcome is $|b_1\rangle$, the winning condition for the game is as shown in Eq. (5.12). Here, $\{M_i^X\}$ is the measurement outcome when the i^{th} player measures her/his qubit in X basis, and $\{M_i^Y\}$ is the measurement outcome when the i^{th} player measures her/his qubit in Y basis. Whenever Dave prepares a maximally entangled four-qubit state as shown in Eq. (5.8), the success probability of the game depends on the parameter of basis in which the measurement is performed. Figure 5.10 shows the relation between the winning probability of the team for different values of parameter λ. Clearly λ is a controlling parameter that controls the winning probability of the game for the other three players. From Figure 5.10, it can be observed that the maximum winning probability (1) is achieved for $\lambda = \frac{\pi}{4}$, i.e., if Dave measures his qubit in diagonal basis $|-\rangle$, $|+\rangle$, the above game is always won by the players. Classically such a game can only be won half the times, when the team gives random answers to the asked questions. Similarly, one can also generalize different n-player games in higher dimensions, where the facilitator is entangled with the players in the team. Such multi-player games can also be extended so as to share a secret key among the players in a similar manner as described in the subsection 5.3.2.

5.6 CONCLUSIONS

In this work, the role of degree of entanglement was addressed for Vaidman's game. The relation between the success probability of winning the Vaidman's game by sharing an entangled quantum state with the degree of entanglement of the shared state has been established. The results obtained here indicate that entanglement and quantum strategies may not always be beneficial in winning a quantum game. For instance, we found that there are set of GHZ class and W class states, for which classical strategies give better results (in terms of game winning prospects) than quantum strategies. On the other hand, for the special class of W-type states, i.e., W_n states, quantum strategies are always better than the classical strategies in winning the Vaidman's game. Moreover, we established a similarity between the Vaidman's game using general three-qubit pure states and the QSS protocol. Further, we also proposed an efficient game, where the player deciding the rules of the game (also termed as the controller) is itself entangled with other two players. The proposed game may find an application in facilitated secret sharing, where a facilitator examines players for their honesty and simultaneously controls the process of sharing information between them.

These games are also studied under real situations, i.e., by taking into account the success probability of the game under noisy conditions using an amplitude damping channel, a depolarizing channel, and a phase flip channel. Interestingly, we found that both W and GHZ states, when used as a shared quantum state in the game, are more robust to phase flip noise. Moreover, GHZ states give better winning probability than that achieved classically, even when two of its qubits pass through an amplitude damping channel. Further, our analysis has been extended for similar games among four, five, and six players. Our analysis found that for games having more than three players, GHZ states are a useful resource for the proposed protocol, as they help attain 100% winning probability. Precisely, the range of n-tangle is analysed for different GHZ-type states to demonstrate the feasibility of opting quantum resources in comparison to classical strategies. Furthermore, our analysis also confirmed that similar to the proposed there-qubit game, the multi-qubit counterpart will also hold similar applications in the secret sharing protocol.

...