Analysing the efficiency of partially entangled states in Vaidman's-type games and its applications in Quantum Secret Sharing

Hargeet Kaur[a] and Atul Kumar[a]

[a]Indian Institute of Technology Jodhpur, Rajasthan

ARTICLE HISTORY
Compiled October 1, 2018

ABSTRACT
We analyse the role of degree of entanglement for Vaidman's game in a setting where the players share a set of partially entangled three-qubit states. Our 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. We further find the conditions under which quantum strategies are always helpful in achieving higher winning probability in the game in comparison to classical strategies. Moreover, we show 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. Our analysis also helps us in comparing the Vaidman's game with the secret sharing protocol. Furthermore, we propose a new Vaidman-type game 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 multi-qubit games.

KEYWORDS
Vaidman's game; quantum secret sharing; entanglement; noise; GHZ and W

1. Introduction

Game theory is an eminently interesting and flourishing field of study, wherein many situations of conflicts can be efficiently examined and resolved (Neumann & Morgenstern, 1944). With the advent of quantum information and computation, game theory has generated a lot of interest in analysing quantum communication protocols from the perspective of a game (Bennett & Brassard, 1984; Houshmand et al., 2010). The analysis not only allows one to study the fundamental of quantum mechanics but also provides a much better insight to the communication protocol in terms of security, payoffs of different players, and complex nature of multi-qubit entanglement. The aim is to study and compare the payoffs of different users and security of a protocol using classical and quantum strategies. In general, quantum strategies are found to be preferable in comparison to the classical strategies. For example, Meyer demonstrated how quantum strategies can be utilized by a player to defeat his classical opponent in a classical penny flip game (Meyer, 1999). He further

CONTACT Hargeet Kaur. Email: kaur.1@iitj.ac.in

explained the relation of penny flip game setting to efficient quantum algorithms. Similarly, Eisert (Eisert et al., 1999) suggested a solution based on quantum theory for avoiding the Prisoners' Dilemma. The quantum version of Prisoners' Dilemma game was also experimentally realized using a NMR quantum computer (Du et al., 2002). On the other hand, Anand and Benjamin (Anand & Benjamin, 2015) found that for a scenario in penny flip game where two players share an entangled state, a player opting for a mixed strategy can still win against a player opting for a quantum strategy. Therefore, it becomes important to analyse the role of quantum entanglement in game theory. Furthermore, one must also understand and study the importance of using different entangled systems under different game scenarios to take the advantage of usefulness of such entangled systems in different situations.

In this article, we analyse a game proposed by Vaidman (Vaidman, 1999) in which a team of three players always wins the game, when they share a three qubit maximally entangled state. The team, however, does not win the game when players opt for pure classical strategies, in fact the maximum winning probability that can be achieved using classical strategies is 3/4. Our analysis of Vaidman game includes two different classes of three-qubit entangled states, namely, GHZ class (Greenberger et al., 1990) and W class of states (Dur et al., 2000). We attempt to establish a relation between the winning probability of Vaidman's game (Vaidman, 1999) with the degree of entanglement of various three-qubit entangled states used as a resources in the game. Interestingly, our results show that for GHZ class, there are set of states for which classical strategies give better winning probability than the quantum strategies. In comparison to the GHZ class, for a special class of W states, quantum strategies prove to be always better than the classical strategies. We further establish a direct correspondence between Vaidman's game and Quantum Secret Sharing (QSS) (Hillery et al., 1999).

In addition, we also propose a Vaidman-type game where one of the players sharing the three-qubit entanglement defines the rules of a game to be played between him/her and the other two players. A detailed examination of the proposed game shows that the rule-maker finds himself in an advantageous situation whenever they share a partially entangled state, because this enables the rule-maker to modify rules in such a way that the team of other two players loose the game. We have further analysed the proposed game in a noisy environment, where we have considered that the qubits of the shared state may pass through an amplitude damping or a depolarizing channel or a phase flip channel. Our results show that in case of W states, the winning probability using quantum strategy, still exceeds the classical winning probability for a phase flip channel. For GHZ state, the success probability using quantum strategy almost always exceeds the winning probability using classical strategies using both phase flip and amplitude damping channel. In all other cases, quantum strategies are found to be better than classical strategy for a certain range of decoherence parameters. Moreover, we further suggest an application of such a game in facilitated secret sharing between three parties, where one of the players is a facilitator and also controls the secret sharing protocol. In the later sections of the article, we have demonstrated the extension of Vaidman's game and the proposed game for multi-qubit scenario. Since the states used as resources in this article can be experimentally prepared (Bouwmeester et al., 1999; Dong et al., 2016; Eibl et al., 2004), the results obtained here may find applications in Quantum Secret Sharing or other similar protocols.

The organization of the article is as follows. In Section II and III, we briefly describe three-party entanglement and QSS, respectively. In section IV, we establish a correspondence of Vaidman's game with QSS, and in corresponding subsections we

further demonstrate the outcomes of using GHZ and W class of states for Vaidman's game. A new Vaidman-type game is proposed in the Section V followed by its study in noisy conditions, and its application for QSS in the subsections. In section VI, a generalization of Vaidman's game for more than three players is discussed. To further extend the analysis, in section VII, the multi-player version of the game proposed in Section V is described. Finally, we conclude the article in Section VIII.

2. Three-qubit Entanglement

Dur et al. (Dur et al., 2000) classified pure states of a three-qubit entangled systems in two inequivalent classes, namely GHZ class and W class represented as

$$|\psi_{GHZ}\rangle = sin\theta|000\rangle + cos\theta|111\rangle \tag{1}$$

and

$$|\psi_W\rangle = a|100\rangle + b|010\rangle + c|001\rangle, \tag{2}$$

respectively where $\theta \in (0, \pi/4)$ and $|a|^2 + |b|^2 + |c|^2 = 1$. The above two classes are termed as inequivalent classes as a state belonging to one of the class cannot be converted to a state belonging to another class by performing any number of Local Operations and Classical Communication (LOCC). The degree of entanglement for a pure three-qubit system can be defined using a measure called three-tangle (τ) (Coffman et al., 2000), given by

$$\tau = C^2_{P(QR)} - C^2_{PQ} - C^2_{PR} \tag{3}$$

where $C_{P(QR)}$ represents the concurrence of the qubit P, with qubits Q and R taken together as one entity (Hill & Wootters, 1997; Wootters, 1998, 2001). The terms C_{PQ} and C_{PR} can be defined in a similar fashion such that,

$$C(|\psi\rangle) = |\langle\psi|\sigma_y \otimes \sigma_y|\psi^*\rangle| \tag{4}$$

Here, ψ^* denotes the complex conjugate of the wave function representing the two-qubit entangled state. The value of three-tangle varies between 0 for product states to 1 for states having maximum entanglement. For example, the three-tangle for a state represented as $(a|0\rangle + b|1\rangle) \otimes (c|00\rangle + d|11\rangle)$ is 0 and for GHZ states represented as

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{5}$$

is 1. Similarly, the standard state in W class is represented by

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |001\rangle) \tag{6}$$

Although the standard W state possesses genuine three-qubit entanglement, the same cannot be identified using the three-tangle as an entanglement measure as the three-tangle of the standard W state is 0. Nevertheless, one can be assured that the

W class of states exhibit genuine tripartite entanglement using other entanglement measures such as average residual entanglement (Dur et al., 2000) or sigma ($'\sigma'$) (Emary & Beenakker , 2004).

3. Quantum Secret Sharing

Secret sharing is the process of splitting a secret message into parts, such that no part of it is sufficient to retrieve the original message (Hillery et al., 1999). The original idea was to split the information between the two recipients, one of which may be a cheat (unknown to the sender). Only when the two recipients cooperate with each other, they retrieve the original message. The protocol, therefore, assumes that the honest recipient will not allow the dishonest recipient to cheat, hence, splitting the information between the two.

The original protocol can be implemented using the maximally entangled three-qubit GHZ state, as given in (5), shared between three users Alice, Bob, and Charlie. Alice splits the original information between Bob and Charlie in a way that the complete message cannot be recovered unless they cooperate with each other. For sharing a joint key with Bob and Charlie, Alice suggests all of them to measure their qubits either in X or Y direction at random where the eigen states in X and Y basis are defined as

$$|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle), \quad |\pm y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle) \tag{7}$$

The effects of Bob's and Charlie's measurements on the state of Alice's qubit is shown

Table 1. Effect of Bob's and Charlie's measurement on Alice's state in a GHZ state

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

in Table 1. After performing their measurements at random, Bob and Charlie announce their choice of measurement bases (but not the measurement outcomes) to Alice. This is followed by Alice telling her choice of measurement basis to Bob and Charlie. Only the bases XXX, XYY, YXY, and YYX (for Alice, Bob, and Charlie, respectively) are accepted, for sharing the secret key. The results from all other random choices of bases are discarded.

Bob and Charlie must meet and tell each other their measurement outcomes so as to collectively know the measurement outcome 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.

4. Vaidman's Game representing Quantum Secret Sharing

In this section, we show a correspondence between the QSS protocol (Hillery et al., 1999) to the Vaidman's game (Vaidman, 1999). We, therefore, first briefly describe the Vaidman's game. In this game, three players, namely Alice, Bob, and Charlie, are taken to arbitrary remote locations: A, B, and C, respectively. Now each player is asked one of the two possible questions: Either "What is X?" or "What is Y?". The players can give only two possible answers, either -1 or +1. The rules of the game suggest that either each player is asked the X question or two of the players are asked the Y question and the remaining one is asked the X question. The team of three players wins the game if the product of their answers is +1 (when all are asked the X question) and -1 (when one is asked the X question and two are asked the Y question). Clearly, if the players adopt the classical strategy then at best they can achieve a winning probability of 3/4. On the other hand, if the three players share a three-qubit maximally entangled GHZ state, as shown in (5), 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 uses the measurement outcome obtained in the measurement process as her/his answer.

4.1. Use of GHZ class states in Vaidman's game

That the three players always win the game using the above strategy is because of the strong correlations between the three qubits of the GHZ state. For example, the three qubits in the GHZ state are related as

$$\begin{aligned} \{M_A^X\}\{M_B^X\}\{M_C^X\} &= 1 \\ \{M_A^X\}\{M_B^Y\}\{M_C^Y\} &= -1 \\ \{M_A^Y\}\{M_B^X\}\{M_C^Y\} &= -1 \\ \{M_A^Y\}\{M_B^Y\}\{M_C^X\} &= -1 \end{aligned} \tag{8}$$

where $\{M_i^X\}$ is the measurement outcome of the player $'i'$ measuring her/his qubit in X basis, and $\{M_i^Y\}$ is the measurement outcome of the player $'i'$ measuring her/his qubit in Y basis. A clear correspondence between the Vaidman's game and the QSS protocol is shown in (8).

We now proceed to analyse the Vaidman's game in a more general setting where the three players share a general GHZ state represented in (1), instead of sharing a maximally entangled GHZ state as described in the original game. Clearly, for a general GHZ state, the success probability of winning the above defined game varies from 0.5 to 1 as shown in Figure 1. Here, we have assumed that the probability of players being asked the set of 4 questions (XXX, XYY, YXY, YYX) is equally likely. In Figure 1, the winning probability of the game, i.e, $\frac{1}{2}(1 + sin2\theta)$ is plotted against the degree of entanglement, three tangle (τ). It is evident that only for maximally entangled state, i.e., when τ attains its maximum value (at $\theta = \pi/4$), the players have 100% chances of winning the game. For all other values of τ the success probability is always less than the one obtained with a maximally entangled state. Interestingly, only the set of states with $\tau > 0.25$ achieve better success probability in comparison to a situation where all the three players opt for classical strategies. Therefore, for the set of states with $\tau < 0.25$, classical strategies will prove to be better in comparison to quantum strategies. Hence, for Vaidman's game, entanglement may not be always useful in winning

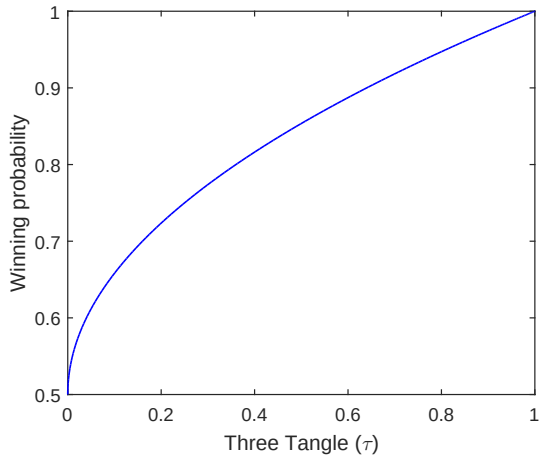

Figure 1. Success probability of winning Vaidman's game using GHZ-type states

the games using quantum strategies in comparison to classical strategies.

4.2. Use of W class states in Vaidman's game

Although W-type states belong to a different class of states, they can also be used as resources in winning Vaidman's game with a different set of questions. In this case, the players may be asked either "What is Z?" or "What is Y?". As earlier, the answers to these questions can again be either +1 or -1. For this, either all players are asked the Z question; or one of the players is asked the Z question and the remaining 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 (6), before the start of play then they can win this game with a success probability of 0.875. On similar grounds, we can use the standard W state for probabilistic QSS, as QSS holds direct correspondence with the Vaidman's game.

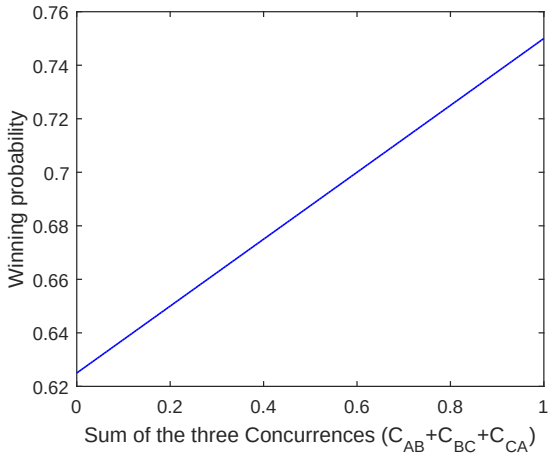

Figure 2. Success probability of winning Vaidman's game using W-type states

Similar to the case of GHZ class, here, we analyse the success probability of the Vaidman's game if the three players share a general W-type state as shown in (2). In such a scenario, the team wins the game with a success probability of $\frac{1}{4}(\frac{5}{2}+bc+ab+ac)$. This value holds true for an assumption 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 is demonstrated in Figure 2. The figure shows 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 for W-type states, the winning probability of Vaidman's game is always greater than the classical winning probability if the sum of two qubit concurrences exceeds 1. Moreover, the highest success probability of 0.875 can be achieved for $a = b = c = \frac{1}{\sqrt{3}}$.

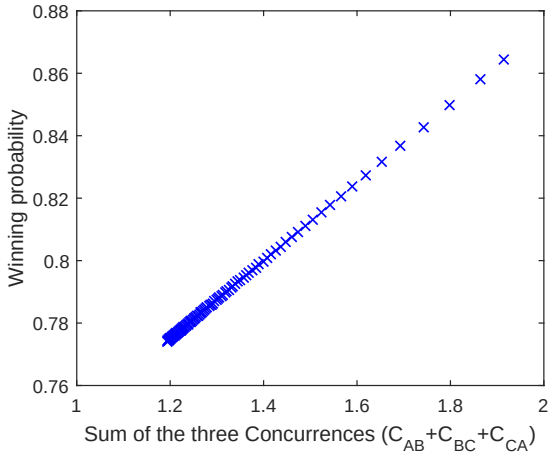

Figure 3. Success probability of winning Vaidman's game using W_n states

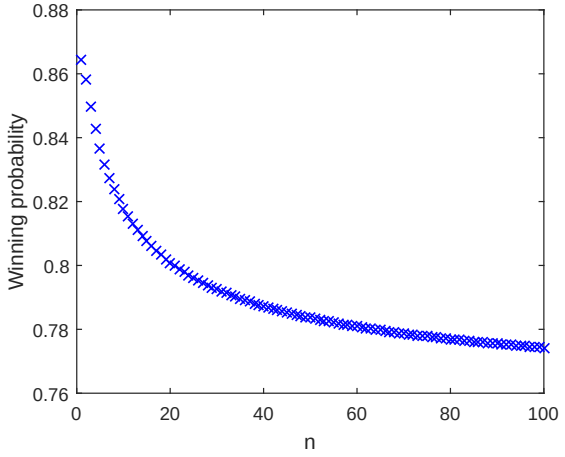

Figure 4. Success probability of winning Vaidman's game using W_n states

Although the use of partially entangled systems, in general, leads to probabilistic information transfer (Karlsson & Bourennane, 1998; Shi & Tomita, 2002), Pati and

Agrawal (Agrawal & 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

$$|W_n\rangle = \frac{1}{\sqrt{2(1+n)}}(|100\rangle + \sqrt{n}e^{i\gamma}|010\rangle + \sqrt{n+1}e^{i\delta}|001\rangle) \tag{9}$$

where n is a positive integer and δ and γ are relative phases. This motivates us to analyse the usefulness of these states for Vaidman's game. We found that the success probability of the game by sharing W_n states as resources can be given by $\frac{1}{8(n+1)}(5 + 5n + \sqrt{n+1} + \sqrt{n}(\sqrt{n+1}+1))$. Figure 3 clearly depicts that if the three players share W_n states, then the success probability using quantum strategies is always greater than the success probability using the classical strategies, independent of the value of sum of residual concurrences. Furthermore, Figure 4 depicts the dependence of winning probability of Vaidman's game on parameter n. The highest success probability of 0.86425 is achieved 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.

4.3. 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 winning probability achieved by the standard W 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. Moreover, W-type states with the sum of three concurrences greater than one, can be useful in winning the game. In addition, a special class of W-type states, i.e. W_n states give better prospects of winning the Vaidman's game, in comparison to any classical resource or strategy, for all values of n.

5. A two-player game where the rule-maker is entangled with the players

The essence of Vaidman's game can be efficiently employed in an interesting scenario, where the rule-maker itself is entangled with the players playing the Vaidman-type game. In our proposed game, Alice, Bob and Charlie share a three-qubit entangled state. We assume that Charlie prepares a three-qubit state and gives one qubit each to Alice (A) and Bob (B), keeping one (C) qubit with himself. Charlie agrees to help Alice and Bob, if they win the game as per the rules defined by Charlie. For this, Charlie measures his qubit in a general basis as shown in (10). Charlie, then asks questions "What is X?" or "What is Z?" to the team. Alice and Bob are not allowed to discuss and have to give individual answers each. Their answer can be +1 or -1. If the team is asked the X (Z) question, both Alice and Bob measure their qubits in X (Z) basis and give their measurement results as answers to the asked questions.

$$|b_0\rangle = sin\lambda|0\rangle - cos\lambda|1\rangle; \qquad |b_1\rangle = cos\lambda|0\rangle + sin\lambda|1\rangle \tag{10}$$

$$|b_0\rangle_C : \quad \{M_A^X\}\{M_B^X\} = 1 \qquad \{M_A^Z\}\{M_B^Z\} = -1 \tag{11}$$

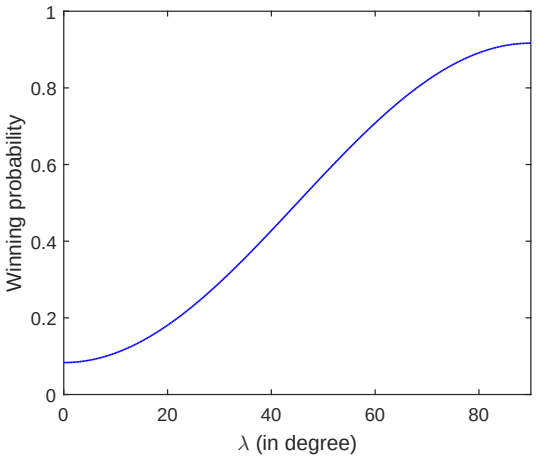

Figure 5. Success probability of winning the proposed game where the rule-maker is entangled with the players using a standard W state

$$|b_1\rangle_C : \quad \{M_A^X\}\{M_B^X\} = -1 \quad \{M_A^Z\}\{M_B^Z\} = 1 \tag{12}$$

If Charlie's measurement outcome is $|b_0\rangle$, he declares the winning condition to be the one listed in (11), and if his measurement outcome is $|b_1\rangle$, he declares the winning condition to be the one as listed in (12). Here, $\{M_i^X\}$ is the measurement outcome when the player $'i'$ measures her/his qubit in X basis, and $\{M_i^Z\}$ is the measurement outcome when the player $'i'$ measures her/his qubit in Z basis.

We first consider that Charlie prepares a three-qubit W state as shown in (6). Clearly, the success probability of the team winning the game will depend on the parameter λ- governing the basis in which Charlie performs a measurement. It can be easily calculated that the value of the success probability achieved is $0.916667 - 0.833334cos^2\lambda$. A plot of the success probability achieved with respect to the parameter λ is shown in Figure 5. The maximum winning probability that the team can achieve is 0.9167 for $\lambda = \frac{\pi}{2}$, i.e., when Charlie measures in computational basis ($|b_0\rangle = |0\rangle$ and $|b_1\rangle = |1\rangle$). On the other hand, if Charlie measures in computational basis $|b_0\rangle = |1\rangle$ and $|b_1\rangle = |0\rangle$, i.e. when $\lambda = 0°$, then the team mostly looses the game as the winning probability is only 0.0833. Thus, if Charlie wants to help Alice and Bob, 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 is always preferable for the team of Alice and Bob.

If Charlie prepares a three-qubit GHZ state as shown in (5) and shares it with Alice and Bob, then the team has only 50% success probability irrespective of the measurement basis used by Charlie, which is equivalent to a classical case where the team may choose not to measure its qubits and randomly answer as +1 or -1. However, if Charlie modifies the questions as X and Y and asks Alice and Bob to make a measurement in the X and Y basis, respectively, then in such a scenario the measurement outcome-dependent rules of the game would also be modified as:

$$|b_0\rangle_C : \quad \{M_A^X\}\{M_B^X\} = -1 \quad \{M_A^Y\}\{M_B^Y\} = +1 \tag{13}$$

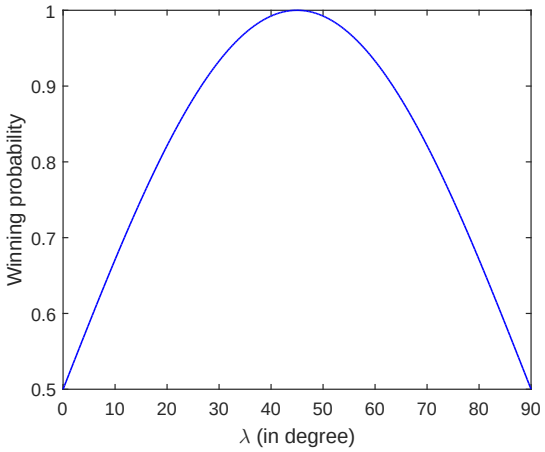

Figure 6. Success probability of winning the proposed game where the rule-maker is entangled with the players using a standard GHZ state

$$|b_1\rangle_C : \quad \{M_A^X\}\{M_B^X\} = +1 \quad \{M_A^Y\}\{M_B^Y\} = -1 \tag{14}$$

Therefore, if Charlie obtains $|b_0\rangle$ as his measurement outcome, then the outcomes of Alice and Bob satisfy (13). On the contrary, if Charlie obtain $|b_1\rangle$ as his measurement outcome, then the outcomes of Alice and Bob satisfy (14). The success chances of the 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 6 describes the success probability of the team as against the measurement parameter λ when standard GHZ state is used as a resource.

5.1. Analysis of the proposed game in noisy environment

In this subsection, we analyse the game discussed above in a noisy environment to study the nature and robustness of these states under real conditions and to study the effect of decoherence on the success probability of the proposed game. For this, we consider that Charlie prepares a three-qubit state and sends two qubits to Alice and Bob for the game to proceed. These two qubits may pass through a noisy channel, degrading the entanglement and correlation between qubits, 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. The various types of noisy channels (Nielsen & Chuang, 2000) we consider for our purpose are as follows:

- **Phase flip channel**: The phase flip channel flips the phase of the qubit ($|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $-|1\rangle$) with probability $1 - p$. The operation elements of this channel are: $E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $E_1 = \sqrt{1-p}Z = \sqrt{1-p}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- **Depolarizing channel**: When a qubit passes through a depolarizing channel, it gets depolarized to a completely mixed state $I/2$ with probability p. With probability $1 - p$ the qubit is left untouched. The state of the quantum state ρ after passing this channel is $\varepsilon(\rho) = p\frac{I}{2} + (1 - p)\rho$

- **Amplitude damping**: The operation elements of amplitude damping are $E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$ and $E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$

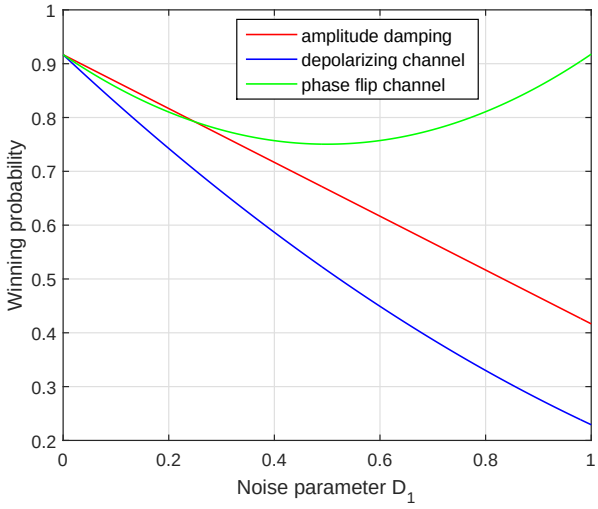

Figure 7. Success probability of winning the game with respect to noise parameter ($D_1 = D_2$) using the standard W state

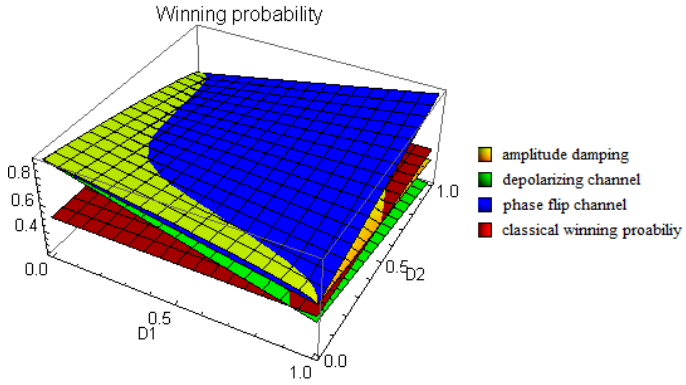

Figure 8. Success probability of winning the game with respect to both the noise parameters ($D_1 \neq D_2$) using the standard W state

In order to compare the effect of above noisy channels on the game using standard W state as a resource, we evaluate the success probability of the game under noisy conditions. The success probability in such cases are listed in Appendix B. Figure 7 shows a plot of success probability of the game with respect to noise parameter D_1 (on qubit sent to Alice), assuming that the noise parameters on Alice's (D_1) and Bob's (D_2) qubit are equal. We further demonstrated a 3-D plot in Figure 8 showing variance between the winning probability of the game and the two noise parameters D_1 and D_2. Figure 7 and 8 clearly demonstrate that the game is most resistant to phase flip noise as the success rate of the game is always above the classical winning probability of 0.5. Moreover, our results show that the winning probability using the W state is more robust towards the amplitude damping channel in comparison to the

depolarizing channel. In both the cases however, the success probability falls below the classical winning probability, for higher values of noise parameters.

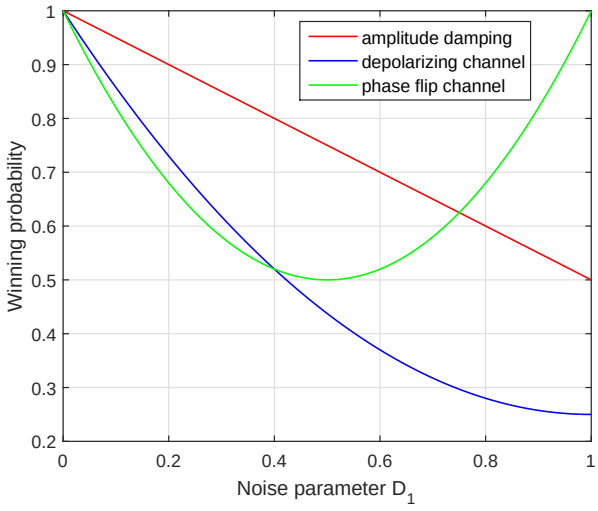

Figure 9. Success probability of winning the game with respect to noise parameter ($D_1 = D_2$) using a maximally entangled GHZ state

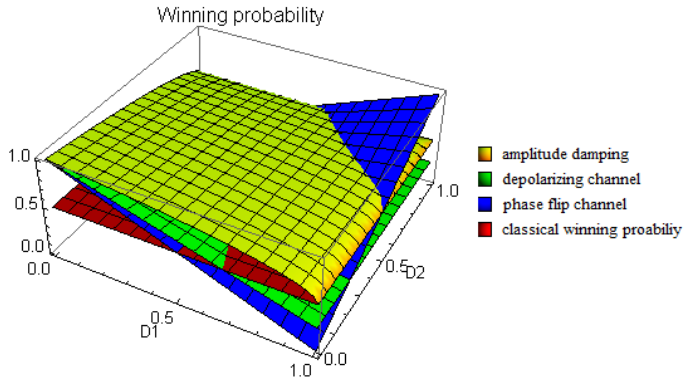

Figure 10. Success probability of winning the game with respect to both the noise parameters ($D_1 \neq D_2$) using a maximally entangled GHZ state

We have also evaluated the success probability of game when a GHZ state is shared in a noisy environment. The results are depicted in Figure 9 and 10. Figure 9 shows the relation between the winning probability of game and the noise parameter D_1 assuming that $D_1 = D_2$. Further, Figure 10 describes the effect of both the parameters on success probability. These plots suggest that when both the noise parameters are equal, the game is resistant to phase flip as well as amplitude damping channel, as the success rate of the game is almost always greater than the classical winning probability of 0.5. However, in case of depolarizing channel, for high value of noise parameter, the winning probability falls below the classical case. Moreover, for $D_1 \neq D_2$, only the success probability in case of amplitude damping noise exceeds the classical winning probability. In other noisy environments, the winning probability may fall below the classical winning probability of 0.5.

5.2. An application of the above game in secret sharing

For establishing a relation between the proposed game and secret sharing, we consider that Alice and Bob are kept in two different cells and are partially disallowed to communicate. By partially, we mean that they can communicate only under the presence of a facilitator or a controller (Charlie in our case), who listens and allows secure communication between the two. To accomplish this task, we prefer to exploit the properties of a standard W state over the use of a W_1 state, because the success rate of winning Vaidman's game is 87.5% when a standard W state is shared, as opposed to 86.425% when a W_1 state is shared within the team members. Also, we further consider that Charlie performs his measurement in the basis as shown in (10) at $\lambda = \frac{\pi}{2}$.

Table 2. 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 3. 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

In order to share a key, Charlie chooses to operate in two different modes, namely control mode and message mode. The control mode corresponds to Charlie's measurement outcome $|1\rangle$, and is used to check whether Alice and Bob are honest or not, as shown in Table 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 (Table 3). For this, Charlie prepares $'m'$ standard W states as shown in (6) and distributes qubits 1 and 2 of each state to Alice and Bob, respectively keeping the third qubit with himself. Charlie, then performs a measurement on his qubit in the computational ($|0\rangle$, $|1\rangle$) basis. Meanwhile, Alice and Bob randomly choose their bases of measurement (either X or Z) and announce their choice of bases to Charlie. If they choose two different bases, then their choices are discarded. Alternately, Charlie randomly chooses a basis of measurement and announces his choice to Alice and Bob. This will ensure that both Alice and Bob perform measurements in the same basis. This step is repeated for $'m'$ qubits, and Alice and Bob note down their measurement results each time.

If Charlie gets $|0\rangle$ as his measurement outcome, then he knows that the measurement results of Alice and Bob are related as in (11) with certainty. As explained above, this will be the message mode of the proposed secret sharing scheme, wherein Alice's and Bob's outcomes will either be same or different. The relation between their 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 the measurement outcome, then the measurement results of Alice and Bob are related as in (12) in 75% cases. Since this is a control mode, Charlie secretly asks both Alice and Bob to announce their measurement outcomes, 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 (12) less than 75% times, then cheating is suspected. Moreover, as Alice and Bob are not allowed to discuss, they cannot distinguish between the message and the control mode. 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 disallows communication and does not announce the relation between the 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 outcomes of 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 simultaneous sharing of a secret key with them, if they are proved honest.

Instead of sharing a W state, if the players in the game share a GHZ state, then Charlie performs his measurement in the diagonal basis as shown in (10) 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 is used to check the honesty of Alice and Bob and the message mode is used for sharing a mutual secret key between Alice and Bob. In this case, Alice and Bob randomly choose their bases of measurement (either X or Y) and announce their choice of bases to Charlie. 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 (14) with certainty. This will be the message mode and the relation between the 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 (13) in all cases. Similar to the previous protocol, Charlie secretly asks both Alice and Bob to announce their measurement outcomes. If the results announced by Alice and Bob do not always comply with the results in (13), then cheating is suspected and the protocol is aborted, else it proceeds further so that the three players finally share a secret key, as in the case described above for the W state.

6. Extension of Vaidman's game in higher dimensions

For a three qubit system, Vaidman's game has 4 set of questions, XXX, XYY, YXY, and YYX, with answers +1, -1, -1, and -1 respectively. Similarly, for four, five, and six qubit systems, 8, 16, and 32 different types of questions, can be asked to the players in the game. For instance, if a four qubit state is shared between four players, then they can be asked the following 8 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 set of questions that can be asked in a game, one can

formulate games. For example, for a four-qubit case one can formulate a single game, but for a five or six qubits, one can formulate 2 or 3 distinct games respectively.

For more than three-player games, we realized that sharing a W state between the players lead to the chances of win being less than the one that can be 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% cases. Appendix A describes the rules of different four, five, and six player games and their winning condition when a GHZ state is shared between the players. For example, in a 4-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 the player's answers is -1 when all are asked question X, and if the product of the player's answers is +1 when two are asked question X and two are asked question Y. 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 a better winning probability than that achieved classically. Moreover, the players always win the game, when a maximally entangled GHZ state is shared.

Similarly in a 5-player game, there are two possible scenarios. In the first one, either all players are asked question X, or two are asked question Y and three are asked question X. 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. Classically the maximum winning probability of the game is 0.909. However, sharing any five qubit GHZ class state with $\tau_5 \geq 0.67$ yields higher winning probability of the game, than by classical means. In another five-player scenario, either two players are asked Y question and remaining three 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 the teams answers should be +1, and whenever four players are asked Y question, then product of the teams answers should be -1. Although, classically this game can be won with a success probability not more than 0.6667, sharing a five-qubit GHZ state with $\tau_5 \geq 0.11$, always leads to a winning probability greater than the classical one. Clearly, sharing the maximally entangled five-qubit GHZ state results in a 100% win for the team. Appendix A further lists the outcomes of different 6 player games with GHZ states as resources.

7. A three-player game where the rule maker is entangled with three players

The following game is an extension of the one proposed in Section 5. In this game, Alice, Bob, Charlie, and Dave share a four-qubit entangled state. Dave prepares the four-qubit state and gives one qubit each to Alice (A), Bob (B), and Charlie (C), keeping one (D) qubit with himself. Dave is the rule-maker and thus decides the winning conditions for the team (Alice, Bob and Charlie). For this, Dave measures his qubit in a general basis as shown in (10), 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

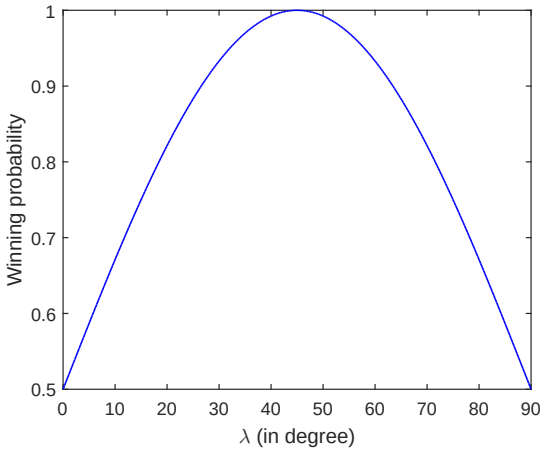

Figure 11. Success probability of winning the proposed game where the rule-maker is entangled with the players using a 4 qubit maximally entangled GHZ state

result as the answer.

$$\begin{aligned} \{M_A^X\}\{M_B^X\}\{M_B^X\} = +1 \quad & \{M_A^X\}\{M_B^Y\}\{M_C^Y\} = -1 \\ \{M_A^Y\}\{M_B^X\}\{M_C^Y\} = -1 \quad & \{M_A^Y\}\{M_B^Y\}\{M_C^X\} = -1 \end{aligned} \tag{15}$$

$$\begin{aligned} \{M_A^X\}\{M_B^X\}\{M_B^X\} = -1 \quad & \{M_A^X\}\{M_B^Y\}\{M_C^Y\} = +1 \\ \{M_A^Y\}\{M_B^X\}\{M_C^Y\} = +1 \quad & \{M_A^Y\}\{M_B^Y\}\{M_C^X\} = +1 \end{aligned} \tag{16}$$

If Dave's measurement outcome is $|b_0\rangle$, he declares the winning condition to be as shown in (15), and if his measurement outcome is $|b_1\rangle$, he declares the winning condition to be as shown in (16). Here, $\{M_i^X\}$ is the measurement outcome when the player $'i'$ measures her/his qubit in X basis, and $\{M_i^Y\}$ is the measurement outcome when the player $'i'$ measures her/his qubit in Y basis.

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|0000\rangle - |1111\rangle) \tag{17}$$

If Dave prepares a maximally entangled four-qubit state as shown in (17), then the team wins the game with different winning probability for different values of parameter λ (Figure 11). Clearly λ is a controlling parameter that controls the winning probability of the game for the other three players. From Figure 11, we can observe that the maximum winning probability of 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 in half the cases. Similar to the above proposed game, one can generalize different games in higher dimensions as well. This can also be extended for sharing a secret key among players in a similar manner as described in the subsection 5.2.

8. Conclusion

In this article, we addressed the role of degree of entanglement for Vaidman's game. We analysed the relation between the success probability of the Vaidman's game with the three-qubit entanglement measures considering both quantum and classical strategies. The results obtained here indicate that entanglement and quantum strategies may not be always useful in winning the game. For example, we found that there are set of GHZ class and W class states, for which classical strategies are proved to be better than the 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. We further explored a correspondence between the Vaidman's game using general three-qubit pure states and the QSS protocol. In addition, we have proposed an efficient game, where the player deciding the rules of the game itself is entangled with other two players. The proposed game may find an application in facilitated secret sharing, where a facilitator checks the players involved for their honesty and simultaneously controls the process of sharing information between them.

We have also analysed these games under real situations, i.e., considering the success probability of the game under noisy conditions, for example using amplitude damping, depolarizing channel and phase flip channel. Interestingly, it has been 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, we have also extended our analysis for similar games between four, five and six players. In the game having more than three players, it has been found that GHZ states are a useful resource for the proposed protocol, as they help attain 100% winning probability. Furthermore, just like the three qubit proposed game holds application in secret sharing, the multi-qubit counterpart of the game, as discussed, will also hold similar utilization.

References

Agrawal, P., & Pati, A. K. (2006). Perfect teleportation and superdense coding with W states. *Phys. Rev. A*, *74*(062320).

Anand, N., & Benjamin, C. (2015). Do quantum strategies always win? *Quantum Information Processing*, *14*, 4027–4038.

Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceeding of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 175–179.

Bouwmeester, D., Pan, J. W., Daniell, M., Weinfurter H. and Zeilinger, A., (1999). Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement. *Phys. Rev. Lett.*, *82*(1345).

Coffman, V., Kundu, J., & Wootters, W. K. (2000). Distributed entanglement. *Phys. Rev. A*, *61*(052306).

Dong, L, Wang, J. X., Li, Q. Y., Shen, H. Z., Dong, H. K., Xiu, X. M., Gao, Y. J. & Oh, C. H. (2016). Nearly deterministic preparation of the perfect W state with weak cross-Kerr nonlinearities. *Phys. Rev. A*, *93*(012308).

Du, J., Li, H., Xu, X., Shi, M., Wu, J., Zhou, X., & Han, R. (2002). Experimental Realization of Quantum Games on a Quantum Computer. *Phys. Rev. Lett.*, *88*(137902).

Dur, W., Vidal, G., & Cirac, J. I. (2000). Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, *62*(062314).

Eibl, M., Kiesel, N., Bourennane, M., Kurtsiefer, C., & Weinfurter, H. (2004). Experimental

Realization of a Three-Qubit Entangled W State. *Phys. Rev. Lett.*, *92*(077901).
Eisert, J., Wilkens, M., & Lewenstein, M. (1999). Quantum Games and Quantum Strategies. *Phys. Rev. Lett.*, *83*(15), 3077–3080.
Emary, C., & Beenakker, C. W. J. (2004). Relation between entanglement measures and Bell inequalities for three qubits. *Phys. Rev. A*, *69*(032317).
Greenberger, D. M., Horne, M. A., Shimony, A., Zeilinger, A. (1990). Bells theorem without inequalities. *Am. J. Phys.*, *58*(12), 1131–1143.
Hill, S., & Wootters, W. K. (1997). Entanglement of a pair of quantum bits. *Phys. Rev. Lett.*, *78*(26), 5022–5025.
Hillery, M., Buzek, V., & Berthiaume, A. (1999). Quantum secret sharing. *Phys. Rev. A*, *59*(3), 1829–1834.
Houshmand, M., Houshmand, M., & Mashhadi, H. R. (2010). Game Theory based View to the Quantum Key Distribution BB84 Protocol. *Third International Symposium on Intelligent Information Technology and Security Informatics IEEE*, 332–336.
Karlsson, A., & Bourennane, M. (1998). Quantum teleportation using three-particle entanglement. *Phys. Rev. A*, *58*(6), 4394–4400.
Meyer, D. A. (1999). Quantum Strategies. *Phys. Rev. Lett.*, *82*(5), 1052–1055.
Neumann, J. V., & Morgenstern, O. (1944). Theory of Games and Economic Behavior. Princeton, N.J: Princeton Univ. Press.
Nielsen, M. A., & Chuang, I. L. (2000). Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, England.
Shi, B. S., & Tomita, A. (2002). Teleportation of an unknown state by W state. *Phys. Lett. A*, *296*, 161–164.
Vaidman, L. (1999). Variations on the Theme of the Greenberger-Horne-Zeilinger Proof. *Foundations of Physics*, *29*(4), 615–630.
Wootters, W. K. (1998). Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, *80*(10), 2245–2248.
Wootters, W. K. (2001). Entanglement of formation and concurrence. *Quantum Information and Computation*, *1*(1) 27–44.

Appendix A. 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 exceeds classical strategy
4 Game 1	$XXXX = -1$ $XXYY = +1$ $XYXY = +1$ $XYYX = +1$ $YXXY = +1$ $YXYX = +1$ $YYXX = +1$	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	$0.765 \leq \tau_6 \leq 1$

Number of players	Winning conditions for the game	Classical winning probability	Range of n-tangle τ_n of GHZ states for which quantum strategies exceeds classical strategy
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	$XXYYYY = XYXYYY$ $= XYYXYY = XYYYXY$ $= XYYYYX = YXXYYY$ $= YXYXYY = YXYYXY$ $= YXYYYX = YYXXYY$ $= YYXYXY = YYXYYX$ $= YYYXXY = YYYXYX$ $= YYYYXX = -1$ and $YYYYYY = +1$	0.9375	$0.765 \leq \tau_6 \leq 1$

Appendix B. 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	$1 - D_1 - D_2 + 2D_1D_2$