Key Distribution based on Three Player Quantum Games

Norihito Toyota, Hokkaido Information University, Ebetsu, Nisinopporo 59-2, Japan
email :toyota@do-johodai.ac.jp

Abstract

We study a new QKD that is different from the scheme proposed by [10], though it essentially takes our ground on three-player quantum games and Greenberg-Horne-Zeilinger triplet entangled state (GHZ state) [16] is used. In our scheme proposed in this article, Bob and Charlie (and Alice also) that they are players in a game get some common key or information (applied strategies and their payoffs in the game) by knowing some results of the measurement made by Alice. There is not any arbiter in our scheme, since existence of an arbiter increase the risk of wiretapping. For it is difficult to detect wiretapping, when an arbiter repeatedly sends classical information. Lastly we discuss robustness for eavesdrop. We show that though maximally entangled case and non-entangled case provided essentially equivalent way in QKD, the latter is not available in the case there are some eavesdroppers.

keywords: Three-Player Quantum Game, Quantum Key Distribution, Payoff, Entangled State, Eavesdrop

1 Introduction

Quantum version of information science has opened the doors of new and large possibility of computer science[1]. Quantum game[2] is an interesting subject and remains in the realm of the unknown in potential capacities. Two schemes for quantum games have been proposed so far. One has been proposed by Eisert et al. [3] where the strategy space of players is a two parameter set of 2×2 matrices and Prisoners Dilemma was discussed. It is shown that starting with maximally entangled initial state, the dilemma disappears for a suitable quantum strategy. Moreover they pointed out that a quantum strategy displays its superiority to all the classical strategies. The details of this scheme were also reviewed by Rosero [4]. Another one has been introduced by Marinatto and Weber [5] applying it to the game of Battle of Sexes. In their scheme, starting with maximally entangled initial state, the players are allowed to apply the probabilistic tactics of unitary operators. As result, they found the strategy for which both the players can get equal payoffs. Recently two schemes could be studied by a unified way[8]. Two schemes are one aspect of the generalized quantization scheme developed by Nazawa and Toor[8]. Furthermore, the scheme was extended to three-player quantum games by Ramzan and Khan[9].

Quantum game theory is not only a tool to resolve a dilemma in some games and find better payoffs than ones of classical strategies, but also it has more potential ability and will provide wide types of communication protocols. For further details, you can consult the article given by Iqbal[6]. In fact Ramzan and Khan studied an interesting aspects of communication based on three-player quantum Prisoner's Dilemma[9]. Moreover the authors investigated a cryptographic protocol based on a scheme of the generalized three-player quantum game[10].

In classical cryptography in 20-th century, key distribution that generates a private key in a secure way between two or several remote parties is an important subject. In public key crypto-systems such as Rivest-Shamir-Adelman(RSA)[11], the receiver generates a pair of keys; a public key and a private key. The security of the communication relies on the difficulty to factorize a large integer into some prime numbers. The public key is used to encrypt the message by a sender, while the private one is used for a receiver to decrypt it. But it has been proved that quantum algorithm can solve the factorization problem in polynomial time[12]. On the other hand, quantum information theory itself provides some ways of quantum key distribution (QKD). First protocol was proposed by Bennet and Brassard[13]. After that Eckert proposed a different approach to QKD[14]. Many protocols are developed as of today[15].

Inspired by a series of researches, we propose a new kind of communication scheme based on three-player quantum game in this article. We mainly study QKD that is different from the scheme proposed [10], though it essentially takes our ground on three-player quantum games and Greenberg-Horne-Zeilinger triplet entangled state (GHZ state) [16] is used. In the scheme of [10], Alice finds messages sent from Bob and Charlie by making a measurement of the qubits that are manipulated by their unitary operators. In our scheme proposed in this article, Bob and Charlie (and Alice also) get some common key or information by knowing the some results of the measurement made by Alice. In [9] where the quantum version of Prisoner's Dilemma game is adopted, Bob and Charlie can extract information about the strategy applied by Alice from their payoffs by mutual understanding that they will apply the same strategy. The information about payoffs is brought by an arbiter. On the contrary there are not any arbiters in our scheme. Existence of an arbiter increase the risk of wiretapping, because when an arbiter sends classical information, but not quantum state, to Bob and Charlie, it is difficult to detect wiretapping. As it is better that there are not any arbiters in a protocol in view of wiretapping, an arbiter is excluded in our scheme. Moreover Bob and Charlie (and Alice) can extract other people's information (applied strategies and their payoffs) theoretically by some information shown by Alice. Lastly we discuss robustness for eavesdrop. We show that though maximally entangled case and non-entangled case provide an essentially equivalent way as QKD, the latter is not available in the case there are any eavesdroppers.

2 Protocol for Key Distribution

The protocol proposed in this article is based on three-player quantum games. Three players are Alice , Bob and Charlie following custom in this field. As result of the game, three player find other people's strategies and payoffs after Alice revealed some information to Bob and Charlie about the result of the quantum game. First of all we describe the framework of quantum games.

2.1 Framework of Quantum Game

Basically we follow the generalized formalism of quantum games proposed by Nawaz and Toor [8] and its extension given by Ramzan and Khan [9]. In scheme of this article, Alice , Bob and Charlie join the game. Each player can choose one among two strategies C and D and we assume the game is symmetric for three players. We express the strategies C as 0 and D as 1, respectively and a set of strategies of three players as (0,0,1) for example. The set of strategies (0,0,1) denotes that Alice applies the strategy C, Bob does C and Charlie does D.

First Alice prepares an initial quantum state that consists of three qubits and passes second qubit and third one to Bob and Charlie, respectively. Bob and Charlie accept one qubit, respectively and Alice keeps remaining one qubit that is first qubit. We suppose the initial quantum state shared between three players is the form ;

$$|\psi_{in}>=\cos\frac{\gamma}{2}|000>+i\sin\frac{\gamma}{2}|111>, \tag{1}$$

where $0\geq\gamma\geq\pi/2$. There is no entanglement for $\gamma=0$ and the case of $\gamma=\pi/2$ denotes maximally entangled state.

Next the players locally manipulate their individual qubits. The classical strategies C and D are assigned to the two basis vector $|0>$ and $|1>$ in the Hilbert space, respectively. The strategies of the players are represented by a unitary operator U_k defined by [8]

$$U_k=\cos\frac{\theta_k}{2}R_k+\sin\frac{\theta_k}{2}Q_k, \tag{2}$$

where $k=$ A(Alice), B(Bob) and C(Charlie), and R_k and Q_k are unitary operators defined by

$$\begin{aligned} R_k|0>&=e^{i\alpha_k}|0>, \qquad R_k|1>=e^{-i\alpha_k}|1>,\\ Q_k|0>&=e^{i(\frac{\pi}{2}-\beta_k)}|1>, \quad Q_k|1>=e^{i(\frac{\pi}{2}+\beta_k)}|0>, \end{aligned} \tag{3}$$

where $0\leq\theta_k\leq\pi$, and $-\pi\leq\alpha_k,\beta_k\leq\pi$. After applying the local operators of three players, the density matrix of the initial state $\rho_{in}=|\psi_{in}><\psi_{in}|$ changes to

$$\rho_f=(U_A\bigotimes U_B\bigotimes U_C)\rho_{in}(U_A\bigotimes U_B\bigotimes U_C)^\dagger. \tag{4}$$

After that, Bob and Charlie return their qubits to Alice and so Alice gets ρ_f. To determine the payoffs for three players, we introduce a operator;

$$\$^{(k)}=\$^{(k)}_{000}P_{000}+\$^{(k)}_{001}P_{001}+\$^{(k)}_{010}P_{010}+\$^{(k)}_{100}P_{100}+\$^{(k)}_{011}P_{011}+\$^{(k)}_{110}P_{110}+\$^{(k)}_{101}P_{101}+\$^{(k)}_{111}P_{111}, \tag{5}$$

where

$$
\begin{aligned}
P_{000} &= |\psi_{000}><\psi_{000}|, \quad |\psi_{000}>=\cos\frac{\delta}{2}|000>+i\sin\frac{\delta}{2}|111>,\\
P_{111} &= |\psi_{111}><\psi_{111}|, \quad |\psi_{111}>=\cos\frac{\delta}{2}|111>+i\sin\frac{\delta}{2}|000>,\\
P_{001} &= |\psi_{001}><\psi_{001}|, \quad |\psi_{001}>=\cos\frac{\delta}{2}|001>+i\sin\frac{\delta}{2}|110>,\\
P_{110} &= |\psi_{110}><\psi_{110}|, \quad |\psi_{110}>=\cos\frac{\delta}{2}|110>+i\sin\frac{\delta}{2}|001>,\\
P_{010} &= |\psi_{010}><\psi_{010}|, \quad |\psi_{010}>=\cos\frac{\delta}{2}|010>-i\sin\frac{\delta}{2}|101>,\\
P_{101} &= |\psi_{101}><\psi_{101}|, \quad |\psi_{101}>=\cos\frac{\delta}{2}|101>-i\sin\frac{\delta}{2}|010>,\\
P_{011} &= |\psi_{011}><\psi_{011}|, \quad |\psi_{011}>=\cos\frac{\delta}{2}|011>-i\sin\frac{\delta}{2}|100>,\\
P_{100} &= |\psi_{100}><\psi_{100}|, \quad |\psi_{100}>=\cos\frac{\delta}{2}|100>-i\sin\frac{\delta}{2}|011>
\end{aligned} \tag{6}
$$

with $0 \leq \delta \leq \pi/2$ and $\$^{(k)}_{abc}$ are the elements of the payoff matrix given in table 1. δ denotes entanglement in the base for measurement (computational) base. In quantum version of usual game theories, a payoff is really given by an expectation value. In this scheme, Alice takes the final projective measurement in the computational basis given by Eq.(6). The payoffs for three players are obtained as the mean values of the payoff operators;

$$P^k(\theta_k,\alpha_k,\beta_k,\delta,\gamma) = Tr(\$^{(k)}_{abc}\rho_f), \tag{7}$$

where $a,b,c \in \{0,1\}$ that mean strategies of three players and Tr is taken for $|\psi_{abc}>$ basis. By using equations (1)∼(7), the payoffs for three players are given by

$$
\begin{aligned}
P^k(\theta_k,\alpha_k,\beta_k) &= C_AC_BC_C\Big(\eta_1\$^{(k)}_{000}+\eta_2\$^{(k)}_{111}+\xi(\$^{(k)}_{000}-\$^{(k)}_{111})\cos 2(\alpha_A+\alpha_B+\alpha_C)\Big)\\
&+ S_AS_BS_C\Big(\eta_2\$^{(k)}_{000}+\eta_1\$^{(k)}_{111}-\xi(\$^{(k)}_{000}-\$^{(k)}_{111})\cos 2(\beta_A+\beta_B+\beta_C)\Big)\\
&+ C_AC_BS_C\Big(\eta_1\$^{(k)}_{001}+\eta_2\$^{(k)}_{110}+\xi(\$^{(k)}_{001}-\$^{(k)}_{110})\cos 2(\alpha_A+\alpha_B-\beta_C)\Big)\\
&+ S_AS_BC_C\Big(\eta_2\$^{(k)}_{001}+\eta_1\$^{(k)}_{110}-\xi(\$^{(k)}_{001}-\$^{(k)}_{110})\cos 2(\beta_A+\beta_B-\alpha_C)\Big)\\
&+ S_AC_BC_C\Big(\eta_1\$^{(k)}_{100}+\eta_2\$^{(k)}_{011}-\xi(\$^{(k)}_{100}-\$^{(k)}_{011})\cos 2(-\beta_A+\alpha_B+\alpha_C)\Big)\\
&+ C_AS_BS_C\Big(\eta_2\$^{(k)}_{100}+\eta_1\$^{(k)}_{011}+\xi(\$^{(k)}_{100}-\$^{(k)}_{011})\cos 2(-\alpha_A+\beta_B-\beta_C)\Big)\\
&+ S_AC_BS_C\Big(\eta_1\$^{(k)}_{101}+\eta_2\$^{(k)}_{010}-\xi(\$^{(k)}_{101}-\$^{(k)}_{010})\cos 2(\beta_A-\alpha_B+\beta_C)\Big)\\
&+ C_AS_BC_C\Big(\eta_2\$^{(k)}_{101}+\eta_1\$^{(k)}_{010}+\xi(\$^{(k)}_{101}-\$^{(k)}_{010})\cos 2(\alpha_A-\beta_B+\alpha_C)\Big)\\
&+ \frac{1}{8}\sin[\theta_A,\theta_B,\theta_C]\\
&\Big\{ \cos\delta\sin\gamma\cos(\alpha_A+\alpha_B+\alpha_C-\beta_A-\beta_B-\beta_C)\sum_{a,b,c\in\{0,1\}}\$_{abc}(-1)^{(a+b+c)}\\
&- \cos\gamma\sin\delta\Big(+\big(\$^{(k)}_{000}-\$^{(k)}_{111}\big)\cos(\alpha_A+\alpha_B+\alpha_C+\beta_A+\beta_B+\beta_C)\\
&\quad +\big(\$^{(k)}_{110}-\$^{(k)}_{001}\big)\cos(\alpha_A+\alpha_B-\alpha_C+\beta_A+\beta_B-\beta_C)\\
&\quad +\big(\$^{(k)}_{010}-\$^{(k)}_{101}\big)\cos(\alpha_A-\alpha_B+\alpha_C+\beta_A-\beta_B+\beta_C)\\
&\quad +\big(\$^{(k)}_{100}-\$^{(k)}_{011}\big)\cos(\alpha_A-\alpha_B-\alpha_C+\beta_A-\beta_B-\beta_C)\Big)\Big\},
\end{aligned} \tag{8}
$$

where

$$
\begin{aligned}
C_k &= \cos^2(\theta_k/2), \quad S_k = \sin^2(\theta_k/2), \quad \textit{and so } C_k + S_k = 1 && (9)\\
\eta_1 &= \cos^2\frac{\gamma}{2}\cos^2\frac{\delta}{2} + \sin^2\frac{\gamma}{2}\sin^2\frac{\delta}{2}, && (10)\\
\eta_2 &= \sin^2\frac{\gamma}{2}\cos^2\frac{\delta}{2} + \cos^2\frac{\gamma}{2}\sin^2\frac{\delta}{2}, && (11)\\
\xi &= \frac{1}{2}\sin(\delta)\sin(\gamma), && (12)\\
\sin[\theta_A, \theta_B, \theta_C] &= \sin(\theta_A)\sin(\theta_B)\sin(\theta_C). && (13)
\end{aligned}
$$

This is a function of the entanglement parameters γ and δ, strategy parameters of three players, α_k, β_k and θ_k, and the elements $\$^{(k)}_{abc}$of a payoff matrix.

Table 1. The payoff matrix for a three-player game where the first number in the parenthesis denotes the payoff of Alice, the second number denotes the one of Bob and third number denotes one of Charlie.

		Charlie C	Charlie D
		Bob	Bob
		C D	C D
Alice	C	$(\$^{(A)}_{000},\$^{(B)}_{000},\$^{(C)}_{000})$, $(\$^{(A)}_{010}, \$^{(B)}_{010},\$^{(C)}_{010})$	$(\$^{(A)}_{001},\$^{(B)}_{001},\$^{(C)}_{001})$, $(\$^{(A)}_{011}, \$^{(B)}_{011},\$^{(C)}_{011})$
	D	$(\$^{(A)}_{100},\$^{(B)}_{100},\$^{(C)}_{100})$, $(\$^{(A)}_{110}, \$^{(B)}_{110},\$^{(C)}_{110})$	$(\$^{(A)}_{101},\$^{(B)}_{101},\$^{(C)}_{101})$, $(\$^{(A)}_{111}, \$^{(B)}_{111},\$^{(C)}_{111})$

@

3 Scenario of QKD

3.1 Basic Protocol of QKD

First of all, let assume the payoff matrix is opened to the public. Alice prepares the initial quantum state represented by Eq.(1), and sends the second qubit and the third qubit to Bob and Charlie, respectively, but keeps the first qubit for herself.

After Bob and Charlie accept their qubits, they and Alice locally manipulate their individual qubits by the unitary operator Eq.(2) and (3), respectively. Three players can choose a favorite parameter set of the unitary operators. After that, Bob and Charlie return their qubit manipulated by their unitary operator to Alice. Alice performs a measure of the total state Eq.(4) to determine the payoffs, and convey some information to Bob and Charlie. By the information, Bob and Charlie can find all information, including opponent's strategy and payoffs, of the game. Thus everyone has common information. If they come to an agreement about the correspondence between parameters applied in this protocol and some digital information each other in advance, they can have some common digital information. This is the essential scenario for the key sharing conveyed by the common information. The outline of this protocol is given in Fig.1.

We show that the scenario is actually available in the following subsections. What information should Alice open to the public in the scenario? How can Bob and Charlie find others' information about the game? We will show them by giving concrete expressions for them. We investigate things dividing into three cases; non-entangled cases, maximally entangled cases and partially entangled cases. Explicit expressions of various quantities are, however, too complicate to analysis them. So we impose some symmetries or conditions on each case in order to simplify things.

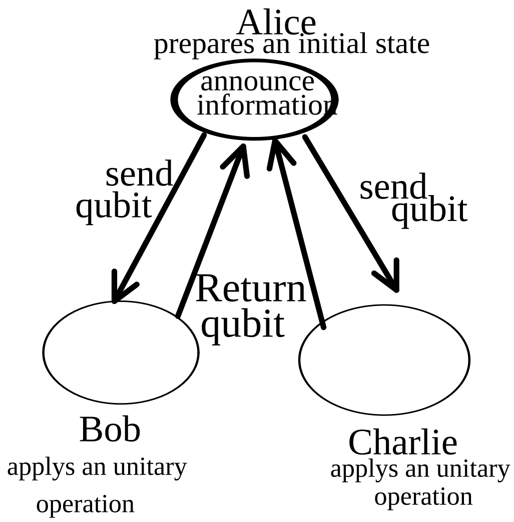

Fig.1 The outline of the protocol@

@

3.2 Non Entanglement Cases

In this subsection we consider the case without any entangled states, both the initial state and the computational base. We take $\gamma = \delta = 0$ which leads to $\eta_1 = 1$ and $\eta_2 = \xi = 0$, and assume that the phase parameters $\alpha_i = \beta_i = 0$.

Then we get the payoff;

$$\begin{aligned} P^k(\theta_k, \alpha_k, \beta_k) &= C_AC_BC_C\$^{(k)}_{000} + S_AS_BS_C\$^{(k)}_{111} + C_AC_BS_C\$^{(k)}_{001} + S_AS_BC_C\$^{(k)}_{110} \\ &\quad + S_AC_BC_C\$^{(k)}_{100} + C_AS_BS_C\$^{(k)}_{011} + S_AC_BS_C\$^{(k)}_{101} + C_AS_BC_C\$^{(k)}_{010} \qquad (14) \\ &= C_BC_CD^{(k)}_A + S_BC_CE^{(k)}_A + C_BS_CF^{(k)}_A + S_BS_CG^{(k)}_A \quad \text{for Alice} \qquad (15) \\ &= C_AC_CD^{(k)}_B + S_AC_CE^{(k)}_B + C_AS_CF^{(k)}_B + S_AS_CG^{(k)}_B \quad \text{for Bob} \qquad (16) \\ &= C_AC_BD^{(k)}_C + S_AC_BE^{(k)}_C + C_AS_BF^{(k)}_C + S_AS_BG^{(k)}_C \quad \text{for Charlie,} \qquad (17) \end{aligned}$$

where

$$\begin{aligned} D^{(k)}_A &= C_A\$^{(k)}_{000} + S_A\$^{(k)}_{100} & E^{(k)}_A &= C_A\$^{(k)}_{010} + S_A\$^{(k)}_{110} \\ F^{(k)}_A &= C_A\$^{(k)}_{001} + S_A\$^{(k)}_{101} & G^{(k)}_A &= C_A\$^{(k)}_{011} + S_A\$^{(k)}_{111} \qquad (18) \\ D^{(k)}_B &= C_B\$^{(k)}_{000} + S_B\$^{(k)}_{010} & E^{(k)}_B &= C_B\$^{(k)}_{100} + S_B\$^{(k)}_{110} \\ F^{(k)}_B &= C_B\$^{(k)}_{001} + S_B\$^{(k)}_{011} & G^{(k)}_B &= C_B\$^{(k)}_{101} + S_B\$^{(k)}_{111} \qquad (19) \\ D^{(k)}_C &= C_C\$^{(k)}_{000} + S_C\$^{(k)}_{001} & E^{(k)}_C &= C_C\$^{(k)}_{100} + S_C\$^{(k)}_{101} \\ F^{(k)}_C &= C_C\$^{(k)}_{010} + S_C\$^{(k)}_{011} & G^{(k)}_C &= C_C\$^{(k)}_{110} + S_C\$^{(k)}_{111}. \qquad (20) \end{aligned}$$

Eq.(14)-(17) are the same equations, but they are available expressions for each player, respectively. $X^{(k)}_{k\prime}$, where $X = D, E, F, G$ and $k' =$ A,B and C, have proper information of player k'.

What information should Alice convey for Bob and Charlie to get information about opponent's payoffs and strategies? For Bob, unknown data are P_A, P_B, P_C, C_A and C_C which are strategies of Alice and Charlie (notice that $\alpha_k = \beta_k = 0$ and of course Bob knows his strategy C_B). Taking account of $k = A, B, C$, Bob has three payoff equations given by Eq.(16). So Alice needs to open two data to the public. Thus Bob can evaluate other unknown data in principle. It, however, is so intricate to get explicit expressions. Imposing some conditions or symmetries will make the expressions simpler but non-trivial.

Due to the aim, Eq. (15)-(17) is rewritten as followings;

$$\begin{aligned}
P^k(\theta_k,\alpha_k,\beta_k) &= C_B C_C(D_A^{(k)}-E_A^{(k)}-F_A^{(k)}+G_A^{(k)})+C_B(F_A^{(k)}-G_A^{(k)}) \\
&\quad +C_C(E_A^{(k)}-G_A^{(k)})+G_A^{(k)} \quad \text{for Alice} && (21)\\
&= C_A C_C(D_B^{(k)}-E_B^{(k)}-F_B^{(k)}+G_B^{(k)})+C_C(F_B^{(k)}-G_B^{(k)}) \\
&\quad +C_C(E_B^{(k)}-G_B^{(k)})+G_B^{(k)} \quad \text{for Bob} && (22)\\
&= C_A C_B(D_C^{(k)}-E_C^{(k)}-F_C^{(k)}+G_C A^{(k)})+C_A(F_C^{(k)}-G_C^{(k)}) \\
&\quad +C_B(E_C^{(k)}-G_C^{(k)})+G_C^{(k)} \quad \text{for Charlie} && (23)
\end{aligned}$$

It is natural to classify into the following three cases to simplify the things from Eq.(21)-(23);

$$\begin{aligned}
\text{Case I:} \quad & (F_A^{(k)}-G_A^{(k)}=)F_B^{(k)}-G_B^{(k)}=F_C^{(k)}-G_C^{(k)}=0 \\
& \$_{001}^{(k)}=\$_{101}^{(k)}, \quad \$_{011}^{(k)}=\$_{111}^{(k)} \text{ and } \$_{010}^{(k)}=\$_{110}^{(k)}, \\
& (\$_{001}^{(k)}=\$_{101}^{(k)}=\$_{011}^{(k)}=\$_{111}^{(k)} \text{ and } \$_{010}^{(k)}=\$_{110}^{(k)}), && (24)\\
\text{Case II:} \quad & (E_A^{(k)}-G_A^{(k)}=)E_B^{(k)}-G_B^{(k)}=E_C^{(k)}-G_C^{(k)}=0 \\
& \$_{100}^{(k)}=\$_{101}^{(k)}=\$_{110}^{(k)}=\$_{111}^{(k)}, \\
& (\$_{100}^{(k)}=\$_{101}^{(k)}=\$_{110}^{(k)}=\$_{111}^{(k)} \text{ and } \$_{010}^{(k)}=\$_{011}^{(k)}), && (25)\\
\text{Case III:} \quad & \text{Case (I)} \bigwedge \text{Case (II)} \\
& \$_{001}^{(k)}=\$_{101}^{(k)}=\$_{010}^{(k)}=\$_{100}^{(k)}=\$_{110}^{(k)}=\$_{111}^{(k)}=\$_{011}^{(k)}, \\
& \text{(The same relations hold)} && (26)
\end{aligned}$$

where the equations within the parentheses denote the cases that the conditions are also imposed on Alice. Alice is a special person in the sense that she puts together everyone's states, observe the payoffs by making a measurement and so can see all P^k, and announces them. Thus Alice has fully information about this quantum game in the end.

In the case I without $F_A^{(k)}-G_A^{(k)}=0$, we obtain

$$\begin{aligned}
C_A &= \frac{(P^B-G_B^{(B)})(E_B^{(A)}-G_B^{(A)})-(P^A-G_B^{(A)})(E_B^{(B)}-G_B^{(B)})}{(P^A-G_B^{(A)})(D_B^{(B)}-E_B^{(B)})-(P^B-G_B^{(B)})(D_B^{(A)}-E_B^{(A)})}, \\
C_C &= \frac{P^A-G_B^{(A)}}{C_A(D_B^{(A)}-E_B^{(A)})+E_B^{(A)}-G_B^{(A)}}, \qquad \text{for Bob} && (27)\\
C_A &= \frac{(P^B-G_C^{(B)})(E_C^{(A)}-G_C^{(A)})-(P^A-G_C^{(A)})(E_C^{(B)}-G_C^{(B)})}{(P^A-G_C^{(A)})(D_C^{(B)}-E_C^{(B)})-(P^B-G_C^{(B)})(D_C^{(A)}-E_C^{(A)})}, \\
C_B &= \frac{P^A-G_C^{(A)}}{C_A(D_C^{(A)}-E_C^{(A)})+E_C^{(A)}-G_C^{(A)}}, \qquad \text{for Charlie.} && (28)
\end{aligned}$$

Notice that $E_A^{(k)}=\$_{111}^{(k)}$, $F_A^{(k)}=G_A^{(k)}=\$_{001}^{(k)}$ in this case. These quantities are trivial in the sense that they do not depend on Alice's strategy and only depend on the payoff matrix originally opended to the public. $X_{\bar{k\prime}}^k$ where $\bar{k}'=B,C$, however, is nontrivial and depends on both payoff matrix and their respective strategy. Thus this condition does not make above expressions trivial.

From Eq. (27) and (28), we see that when Alice opens P^A and P^B to the public, Bob and Charlie can find C_A. As result, they can get the information about opponent's strategy, C_C for Bob and C_B for Charlie. So Bob and Charlie can find the strategies of all players and evaluate P^k. Three players come to acquire full information of the quantum game, P^k and C_k, since Alice originally observes all states and payoffs.

When Alice informs Bob of P^A and his payoff P^B, and Charlie of P^A and his payoff P^C, they can also get full information according to the following equations derived from Eq.(23) and (24) for Charlie;

$$\begin{aligned} C_A &= \frac{(P^C - G_C^{(C)})(E_C^{(A)} - G_C^{(A)}) - (P^A - G_C^{(A)})(E_C^{(C)} - G_C^{(C)})}{(P^A - G_C^{(A)})(D_C^{(C)} - E_C^{(C)}) - (P^C - G_C^{(C)})(D_C^{(A)} - E_C^{(A)})}, \\ C_B &= \frac{P^A - G_C^{(A)}}{C_A(D_C^{(A)} - E_C^{(A)}) + E_C^{(A)} - G_C^{(A)}}, \qquad \text{for Charlie.} \end{aligned} \tag{29}$$

There is another case to be considered. Alice opens all of her information, P_A and C_A. Then Bob and Charlie can easily evaluate the strategies of their opponent from Eq.(27) and (28). So they can also know full information of this game by similar logic to the former case. Everything also does not change in the case I including $F_A^{(k)} - G_A^{(k)} = 0$.

The case II without $E_A^{(k)} - G_A^{(k)} = 0$, we obtain

$$\begin{aligned} C_C &= \frac{(P^B - G_B^{(B)})(F_B^{(A)} - G_B^{(A)}) - (P^A - G_B^{(A)})(F_B^{(B)} - G_B^{(B)})}{(P^A - G_B^{(A)})(D_B^{(B)} - F_B^{(B)}) - (P^B - G_B^{(B)})(D_B^{(A)} - F_B^{(A)})}, \\ C_A &= \frac{P^A - G_B^{(A)}}{C_C(D_B^{(A)} - F_B^{(A)}) + F_B^{(A)} - G_B^{(A)}}, \qquad \text{for Bob} \end{aligned} \tag{30}$$

$$\begin{aligned} C_B &= \frac{(P^B - G_C^{(B)})(F_C^{(A)} - G_C^{(A)}) - (P^A - G_C^{(A)})(F_C^{(B)} - G_C^{(B)})}{(P^A - G_C^{(A)})(D_C^{(B)} - F_C^{(B)}) - (P^B - G_C^{(B)})(D_C^{(A)} - F_C^{(A)})}, \\ C_A &= \frac{P^A - G_C^{(A)}}{C_B(D_C^{(A)} - F_C^{(A)}) + F_C^{(A)} - G_C^{(A)}}, \qquad \text{for Charlie.} \end{aligned} \tag{31}$$

Notice that $E_{\bar{k'}}^{(k)} = G_{\bar{k'}}^{(k)} = \$_{100}^{(k)}$ in this case. When including $E_A^{(k)} - G_A^{(k)} = 0$, one more equation $F_C^{(k)} = \$_{010}^{(k)}$ is added to the relations. These quantities are trivial in the sense that they do not depend on three players' strategies and only depend on the payoff matrix originally opened to the public. Only $F_B^{(k)}$ and $D_{k'}^{(k)}$, however, are nontrivial and depend on both payoff matrix and their respective strategy. Thus this does not make above expressions trivial.

Then we see that when Alice open P^A and P^B to the public, Bob and Charlie can find C_A. As result, they can get the information about the opponent's strategy, C_C for Bob and C_B for Charlie. So Bob and Charlie can find the strategies of all players and evaluate P_C. Three players come to acquire full information of the quantum game, P^k and C_k.

When Alice informs Bob of P^A and his payoff P^B, and Charlie of P^A and his payoff P^C, They can also get full information according to the following equations for Charlie;

$$\begin{aligned} C_A &= \frac{(P^C - G_C^{(C)})(F_C^{(A)} - G_C^{(A)}) - (P^A - G_C^{(A)})(F_C^{(C)} - G_C^{(C)})}{(P^A - G_C^{(A)})(D_C^{(C)} - F_C^{(C)}) - (P^C - G_C^{(C)})(D_C^{(A)} - F_C^{(A)})}, \\ C_B &= \frac{P^A - G_C^{(A)}}{C_A(D_C^{(A)} - F_C^{(A)}) + F_C^{(A)} - G_C^{(A)}}, \qquad \text{for Charlie.} \end{aligned} \tag{32}$$

There is another case to be considered. Alice opens all of her information, P_A and C_A. Then Bob and Charlie can easily evaluate the strategy of their opponent from the following Eq.(33) and (34).

$$C_C = \frac{P^A - G_B^{(A)} - C_A(F_C^{(A)} - G_C^{(A)})}{(C_A(D_B^{(A)} - F_B^{(A)})}, \qquad \text{for Bob} \tag{33}$$

$$C_B = \frac{P^A - G_C^{(A)} - C_A(F_C^{(A)} - G_C^{(A)})}{C_A(D_C^{(A)} - F_C^{(A)})}, \qquad \text{for Charlie.} \tag{34}$$

They can also know full information of this game by similar logic to the former case. Everything becomes simpler in the case III. From Eq. (21)-(23), we obtain

$$\begin{aligned} P^k &= C_A C_C (D_B^{(k)} - F_B^{(k)}) + G_B^{(k)}, \\ C_C &= \frac{P^A - G_B^{(A)}}{C_A (D_B^{(A)} - F_B^{(A)})}, \qquad \text{for Bob.} \end{aligned} \tag{35}$$

$$\begin{aligned} P^k &= C_B C_C (D_C^{(k)} - F_C^{(k)}) + G_C^{(k)}, \\ C_B &= \frac{P^A - G_C^{(A)}}{C_A (D_C^{(A)} - F_C^{(A)})}, \qquad \text{for Charlie.} \end{aligned} \tag{36}$$

$$\tag{37}$$

Then $E_{k\prime}^{(k)} = G_{k\prime}^{(k)} = F_{k\prime}^{(k)} = \$_{100}$. When Alice opens P^A and C^A to the public, all players know full information of this game for the same logic as before.

If the further condition $D_{\bar{k}\prime}^{(k)} = F_{\bar{k}\prime}^{(k)}$ and $E_{\bar{k}\prime}^{(k)} = G_{\bar{k}\prime}^{(k)}$ adding to Case III is imposed, we have only a trivial result. Then we notice that $\$_{000}^{(k)} = \$_{001}^{(k)}$ and $\$_{010}^{(k)} = \$_{110}^{(k)}$, $\$_{100}^{(k)} = \$_{101}^{(k)}$ and $\$_{111}^{(k)} = \$_{110}^{(k)}$ from $D_B^{(k)} = F_B^{(k)}$ and $E_B^{(k)} = G_B^{(k)}$. Moreover we notice that $\$_{000}^{(k)} = \$_{011}^{(k)}$ and $\$_{011}^{(k)} = \$_{001}^{(k)}$, $\$_{111}^{(k)} = \$_{101}^{(k)}$ and $\$_{100}^{(k)} = \$_{110}^{(k)}$ from $D_C^{(k)} = F_C^{(k)}$ and $E_C^{(k)} = G_C^{(k)}$. So $\$_{0ab}^{(k)}$ take all the same value and $\$_{1ab}^{(k)}$ take so. After all, $D_{\bar{k}\prime}^{(k)} = F_{\bar{k}\prime}^{(k)} = \$_{000}^{(k)}$, $E_C^{(k)} = G_C^{(k)} = \$_{100}^{(k)}$ and $E_B^{(k)} = G_B^{(k)} = \$_{110}^{(k)}$. Thus all $X_{k\prime}^{(k)}$s' are trivial and have no private information for Bob and Charlie.

3.3 Maximally Entanglement Cases

We consider the maximally entangled cases in the initial state and the computational base where $\gamma = \delta = \pi/2$. Then we see that $\xi = \eta_1 = \eta_2 = 1/2$ and the last term in Eq. (8) that the coefficient of the term is $\frac{1}{8}\sin[\theta_A, \theta_B, \theta_C]$ vanishes. When $\theta_B = \theta_C = 0$, we obtain the trivial payoff

$$P^k = C_A \$_{000}^{(k)} \pm S_A \$_{001}^{(k)}. \tag{38}$$

So all people including eavesdropper Eva can obtain full information of this game as soon as Alice opens something of (classical) information of this game to the public. If Alice privately conveys it to Bob and Charlie, Eva can obtain full information by eavesdrops. Since the information is a classical type (note the information such as P^k and C_k is classical), it is difficult to detect the eavesdrops.

We take $\beta_k = \alpha_k = 0$ for simplicity but $\theta_A\theta_B\theta_C \neq 0$. Then we obtain the following equations;

$$\begin{aligned} P^k(\theta_k, \alpha_k, \beta_k) &= C_A C_B C_C \$_{000}^{(k)} + S_A S_B S_C \$_{111}^{(k)} + C_A C_B S_C \$_{001}^{(k)} + S_A S_B C_C \$_{110}^{(k)} \\ &\quad + S_A C_B C_C \$_{011}^{(k)} + C_A S_B S_C \$_{100}^{(k)} + S_A C_B S_C \$_{010}^{(k)} + C_A S_B C_C \$_{101}^{(k)} && (39) \\ &= C_B C_C D_A'^{(k)} + S_B S_C E_A'^{(k)} + C_B S_C F_A'^{(k)} + S_B C_C G_A'^{(k)} \quad \text{for Alice} && (40) \\ &= C_A C_C D_B'^{(k)} + S_A S_C E_B'^{(k)} + C_A S_C F_B'^{(k)} + S_A C_C G_B'^{(k)} \quad \text{for Bob} && (41) \\ &= C_A C_B D_C'^{(k)} + S_A S_B E_C'^{(k)} + C_A S_B F_C'^{(k)} + S_A C_B G_C'^{(k)} \quad \text{for Charlie,} && (42) \end{aligned}$$

where

$$\begin{aligned} D_A^{(k)} &= C_A \$_{000}^{(k)} + S_A \$_{011}^{(k)} \qquad & E_A^{(k)} &= C_A \$_{101}^{(k)} + S_A \$_{110}^{(k)}, \\ F_A^{(k)} &= C_A \$_{001}^{(k)} + S_A \$_{110}^{(k)} \qquad & G_A^{(k)} &= C_A \$_{100}^{(k)} + S_A \$_{111}^{(k)}, && (43) \\ D_B^{(k)} &= C_B \$_{000}^{(k)} + S_B \$_{101}^{(k)} \qquad & E_B^{(k)} &= C_B \$_{011}^{(k)} + S_B \$_{111}^{(k)}, \\ F_B^{(k)} &= C_B \$_{001}^{(k)} + S_B \$_{011}^{(k)} \qquad & G_B^{(k)} &= C_B \$_{010}^{(k)} + S_B \$_{111}^{(k)}, && (44) \\ D_C^{(k)} &= C_C \$_{000}^{(k)} + S_C \$_{001}^{(k)} \qquad & E_C^{(k)} &= C_C \$_{011}^{(k)} + S_C \$_{010}^{(k)}, \\ F_C^{(k)} &= C_C \$_{101}^{(k)} + S_C \$_{100}^{(k)} \qquad & G_C^{(k)} &= C_C \$_{110}^{(k)} + S_C \$_{111}^{(k)}. && (45) \end{aligned}$$

By comparing these equations to (14)-(20) in the non-entangled case, we find that both expressions are transferred from one hand to the other by exchanging $100 \leftrightarrow 011$ and $010 \leftrightarrow 101$. So there is a sort of symmetry in the both cases;

$$100 \longleftrightarrow 011 \quad \text{and} \quad 010 \longleftrightarrow 101. \tag{46}$$

Thus there is no essential difference between maximally entangled case and non-entangled case.

We give a little comment on the cases of $\alpha_k \neq 0 \neq \beta_k$. In both non-entangled case and maximally entanglement case, the last term in Eq. (8) vanishes. Then both cases with $\alpha_k \neq 0 \neq \beta_k$ are linearly transformed each other in the elements of a payoff matrix such as;

$$\begin{aligned}
\begin{pmatrix} \$'_{000} \\ \$'_{111} \end{pmatrix} &= \begin{pmatrix} \eta_1 + \xi\cos(\alpha_A+\alpha_B+\alpha_C) & \eta_2 - \xi\cos(\alpha_A+\alpha_B+\alpha_C) \\ \eta_2 - \xi\cos(\beta_A+\beta_B+\beta_C) & \eta_1 + \xi\cos(\beta_A+\beta_B+\beta_C) \end{pmatrix} \begin{pmatrix} \$_{000} \\ \$_{111} \end{pmatrix}, \\
\begin{pmatrix} \$'_{001} \\ \$'_{110} \end{pmatrix} &= \begin{pmatrix} \eta_1 + \xi\cos(\alpha_A+\alpha_B-\beta_C) & \eta_2 - \xi\cos(\alpha_A+\alpha_B-\beta_C) \\ \eta_2 - \xi\cos(\beta_A+\beta_B-\alpha_C) & \eta_1 + \xi\cos(\beta_A+\beta_B-\alpha_C) \end{pmatrix} \begin{pmatrix} \$_{001} \\ \$_{110} \end{pmatrix}, \\
\begin{pmatrix} \$'_{100} \\ \$'_{011} \end{pmatrix} &= \begin{pmatrix} \eta_1 - \xi\cos(-\beta_A+\alpha_B+\alpha_C) & \eta_2 + \xi\cos(-\beta_A+\alpha_B+\alpha_C) \\ \eta_2 + \xi\cos(\alpha_A-\beta_B+\beta_C) & \eta_1 - \xi\cos(\alpha_A-\beta_B+\beta_C) \end{pmatrix} \begin{pmatrix} \$_{100} \\ \$_{011} \end{pmatrix}, \\
\begin{pmatrix} \$'_{101} \\ \$'_{101} \end{pmatrix} &= \begin{pmatrix} \eta_1 - \xi\cos(\beta_A-\alpha_B+\beta_C) & \eta_2 + \xi\cos(\beta_A-\alpha_B+\beta_C) \\ \eta_2 + \xi\cos(\alpha_A-\beta_B+\alpha_C) & \eta_1 - \xi\cos(\alpha_A-\beta_B+\alpha_C) \end{pmatrix} \begin{pmatrix} \$_{101} \\ \$_{101} \end{pmatrix}. \qquad (47)
\end{aligned}$$

So in both non-entangled case and maximally entangled case, $\alpha_k \neq 0 \neq \beta_k$ does not have any crucial influence on previous results in this article.

3.4 Partially Entangled Cases

We take $\alpha_k = 0 = \beta_C$, $\beta_A - \beta_B = \pi$ and $\beta_A + \beta_B = 2\pi$ for simplicity but $\theta_A\theta_B\theta_C \neq 0$. There are many equivalent choices of these parameters and the this choice is only one example among them. Then we obtain the following equations for the last term in Eq. (8);

$$P^k(\theta_k, 0, \beta_k)_{last} = \frac{1}{8}\sin[\theta_A, \theta_B, \theta_C]\Big\{\sin\big(\delta-\gamma\big)\sum_{a,b,c\in\{0,1\}} \$^{(k)}_{abc}(-1)^{(a+b+c)}\Big\}. \qquad (48)$$

So we consider the case of $\delta = 0$ and $\gamma = \pi/2$, or $\delta = \pi/2$ and $\gamma = 0$ as a partially entangled case. Under this choice, we obtain

$$\eta_1 = \eta_2 = \frac{1}{2}, \qquad \xi = 0 \qquad (49)$$

$$P^k(\theta_k, 0, \beta_k)_{last} = \pm\sqrt{C_A C_B C_C S_A S_B S_C}\sum_{a,b,c\in\{0,1\}} \$^{(k)}_{abc}(-1)^{(a+b+c)}, \qquad (50)$$

where $\pm$ corresponds to two choices of δ and γ. From Eq.(48), Eq. (8) is rewritten as follows;

$$\begin{aligned}
P^k(\theta_k, \alpha_k, \beta_k) &= \frac{1}{2}\Big\{\$^{(k)}_{000}\Big(c_A c_B c_C \pm s_A s_B s_C\Big)^2 + \$^{(k)}_{111}\Big(c_A c_B c_C \mp s_A s_B s_C\Big)^2 \\
&+ \$^{(k)}_{001}\Big(c_A c_B s_C \mp s_A s_B c_C\Big)^2 + \$^{(k)}_{110}\Big(c_A c_B s_C \pm s_A s_B s_C\Big)^2 \\
&+ \$^{(k)}_{100}\Big(s_A c_B c_C \mp c_A s_B s_C\Big)^2 + \$^{(k)}_{011}\Big(s_A c_B c_C \pm c_A s_B s_C\Big)^2 \\
&+ \$^{(k)}_{101}\Big(s_A c_B s_C \pm c_A s_B c_C\Big)^2 + \$^{(k)}_{010}\Big(s_A c_B s_C \mp c_A s_B c_C\Big)^2\Big\}, \qquad (51)
\end{aligned}$$

where

$$c_k = \cos(\frac{\theta_k}{2}), \qquad and \qquad s_k = \sin(\frac{\theta_k}{2}). \qquad (52)$$

Furthermore we impose a condition on the payoff matrix to make the analysis simpler.

$$\$_{111} = \$_{000}, \qquad \$_{001} = \$_{110}, \qquad \$_{100} = \$_{011}, \qquad \$_{101} = \$_{010}. \qquad (53)$$

This is a sort of duality, since this means $\$_{abc} = \$_{\bar{a}\bar{b}\bar{c}}$ where $\bar{0} = 1$ and $\bar{1} = 0$. We call this duality NOT-duality that also means $C \Longleftrightarrow D$ symmetry. Under this NOT-duality, we obtain

$$
\begin{aligned}
P^k(\theta_k, 0, \beta_k) &= \Big\{\$^{(k)}_{000}\Big(C_AC_BC_C + S_AS_BS_C\Big) + \$^{(k)}_{001}\Big(C_AC_BS_C + S_AS_BC_C\Big) && (54)\\
&\quad +\$^{(k)}_{100}\Big(S_AC_BC_C + C_AS_BS_C\Big) + \$^{(k)}_{101}\Big(S_AC_BS_C \pm C_AS_BC_C\Big)\Big\} && (55)\\
&= C_BC_C(\$^{(k)}_{000} + \$^{(k)}_{100} - \$^{(k)}_{001} - \$^{(k)}_{101}) + C_B(\bar{F}^{(k)}_A - \bar{G}^{(k)}_A)\\
&\quad +C_C(\bar{E}^{(k)}_A - \bar{G}^{(k)}_A) \ \text{ for Alice}, && (56)\\
&= C_AC_C(\$^{(k)}_{000} + \$^{(k)}_{101} - \$^{(k)}_{001} - \$^{(k)}_{100}) + C_C(\bar{E}^{(k)}_B - \bar{G}^{(k)}_B)\\
&\quad +C_C(\bar{F}^{(k)}_B - \bar{G}^{(k)}_B) \ \text{ for Bob}, && (57)\\
&= C_AC_B(\$^{(k)}_{000} + \$^{(k)}_{001} - \$^{(k)}_{101} - \$^{(k)}_{100}) + C_B(\bar{F}^{(k)}_C - \bar{G}^{(k)}_C)\\
&\quad +C_A(\bar{E}^{(k)}_C - \bar{G}^{(k)}_C) \ \text{ for Charlie}. && (58)
\end{aligned}
$$

We introduce the following symbol like the previous cases;

$$
\begin{aligned}
\bar{D}^{(k)}_A &= C_A\$^{(k)}_{000} + S_A\$^{(k)}_{100} & \bar{E}^{(k)}_A &= C_A\$^{(k)}_{101} + S_A\$^{(k)}_{001},\\
\bar{F}^{(k)}_A &= C_A\$^{(k)}_{001} + S_A\$^{(k)}_{101} & \bar{G}^{(k)}_A &= C_A\$^{(k)}_{100} + S_A\$^{(k)}_{000}, && (59)\\
\bar{D}^{(k)}_B &= C_B\$^{(k)}_{000} + S_B\$^{(k)}_{101} & \bar{E}^{(k)}_B &= C_B\$^{(k)}_{100} + S_B\$^{(k)}_{001},\\
\bar{F}^{(k)}_B &= C_B\$^{(k)}_{001} + S_B\$^{(k)}_{100} & \bar{G}^{(k)}_B &= C_B\$^{(k)}_{101} + S_B\$^{(k)}_{000}, && (60)\\
\bar{D}^{(k)}_C &= C_C\$^{(k)}_{000} + S_C\$^{(k)}_{001} & \bar{E}^{(k)}_C &= C_C\$^{(k)}_{101} + S_C\$^{(k)}_{100},\\
\bar{F}^{(k)}_C &= C_C\$^{(k)}_{10}0 + S_C\$^{(k)}_{101} & \bar{G}^{(k)}_C &= C_C\$^{(k)}_{001} + S_C\$^{(k)}_{100}. && (61)
\end{aligned}
$$

The expressions of these equations are changed each others under the following transformations;

$$
\begin{aligned}
\text{Bob} \Longleftrightarrow \text{Charlie} &: \quad 101 \longleftrightarrow 001 \qquad X_B \longleftrightarrow X_C, && (62)\\
\text{Bob} \Longleftrightarrow \text{Alice} &: \quad 100 \longleftrightarrow 101 \qquad X_B \longleftrightarrow X_A, && (63)\\
\text{Alice} \Longleftrightarrow \text{Charlie} &: \quad 100 \longleftrightarrow 001 \qquad X_A \longleftrightarrow X_C. && (64)
\end{aligned}
$$

For example, when Alice opens C_A and P_A to the public, Bob and Charlie can find the strategies of their opponents, respectively;

$$
\begin{aligned}
C_C &= \frac{P^A - C_A(F^{(A)}_B - G^{(A)}_B) + G^{(A)}_B}{C_A(\$_{000} + \$_{101} - \$_{100} - \$_{001}) + (E^{(A)}_B - G^{(A)}_B)}, \qquad \text{for Bob.} && (65)\\
C_B &= \frac{P^A - C_A(F^{(A)}_C - G^{(A)}_C) + G^{(A)}_C}{C_A(\$_{000} + \$_{001} - \$_{100} - \$_{101}) + (E^{(A)}_B - G^{(A)}_B)}, \qquad \text{for Charlie.} && (66)\\
& && (67)
\end{aligned}
$$

As result, they find full information of this game.

Even if Alice opens P_A and P_B based on her observation, Bob and Charlie can also find full information of this game. However, the expressions are too complicate to describe them and they are not so available. We consider the following symmetric cases.

$$
\begin{aligned}
&\text{(I)} & E^{(k)}_B &= G^{(k)}_B & &, \$_{001} = \$_{101} \text{ and } \$_{100} = \$_{000}, && (68)\\
&\text{(II)} & F^{(k)}_B &= G^{(k)}_B & &, \$_{100} = \$_{101} \text{ and } \$_{001} = \$_{000}, && (69)\\
&\text{(III)} & E^{(k)}_B = F^{(k)}_B &= G^{(k)}_B & &, \$_{001} = \$_{101} = \$_{100} = \$_{000}. && (70)
\end{aligned}
$$

Case (I);
we obtain

$$
\begin{aligned}
C_C &= \frac{P^A - \$_{110} + C_B(\$_{100} - \$_{001})}{(2C_B - 1)(\$_{100} - \$_{001})}, \qquad \text{for Bob.} && (71)\\
C_B &= \frac{P^A - \$_{110} + C_C(\$_{100} - \$_{001})}{(2C_C - 1)(\$_{100} - \$_{001})}. \qquad \text{for Charlie.} && (72)\\
& && (73)
\end{aligned}
$$

As result, Bob and Charlie can find full information of this game only when P^A is opened to the public.

Case (II);
we obtain

$$C_A = \frac{P^A - \$_{000} - C_B(\$_{100} - \$_{000})}{(2C_B - 1)(\$_{100} - \$_{000})}, \qquad \text{for Bob.} \tag{74}$$

$$C_A = \frac{P^A - \$_{000} + C_C(\$_{100} - \$_{001})}{(2C_C - 1)(\$_{100} - \$_{001})}. \qquad \text{for Charlie.} \tag{75}$$

$$\tag{76}$$

So essentially this case is as same as the case (I). Knowing P^A makes all players find full information of this game. Thus knowing P^A is only needed to hold full information of the game in common in both Case(I) and (II). That such economical point can be realize is a notable feature in the partially entangled case.

Case (iii); we only obtain a trivial result;

$$P^k = G^k_{k'} = 1. \tag{77}$$

4 Brief Comment of Robustness for Eavesdrop

4.1 Phase Damping Model for Eavesdropper

There may be an eavesdropper, Eva, in a quantum line from Alice to Bob or Charlie. She may perform the measurement on the qubit that Alice (Bob or Charlie) transmits to Bob or Charlie (Alice). We follow Ramzan and Khan [10] in the discussion as to security against bugging.

An action of measurement performed by Eva on the qubit can be modeled as the action of phase damping channel [1]. After measurement by Eva, the quantum state with 1 qubit that Alice transmitted to Bob and Charlie is transformed into

$$\rho_1 = \sum_{i=0}^{2} A_i \rho_{in} A_i^\dagger, \tag{78}$$

where $A_0 = \sqrt{p}|0 >< 0|$, $A_1 = \sqrt{p}|1 >< 1|$ and $A_2 = \sqrt{1-p}\hat{I}$ with the identity operator $\hat{I}$ are the Kraus operators[1]. This can be extended to

$$\rho_N = \sum_{i=0}^{2} A_{i_1} \otimes A_{i_2} \cdots \otimes A_{i_N} \otimes \rho_{in} A^\dagger_{i_N} \otimes \cdots A^\dagger_{i_2} \otimes A^\dagger_{i_1} \tag{79}$$

for N qubits, when each qubit is measured. Then the payoff is given by the following replacement in Eq.(8);

$$\begin{aligned} \xi &\Longrightarrow \xi\mu_p, \\ (-1)^{(a+b+c)} &\Longrightarrow \mu_p(-1)^{(a+b+c)}. \end{aligned} \tag{80}$$

4.2 Non-Entangled and Maximally Entangled Cases

In this subsection we focus our attention to the non-entangled case ($\gamma = \delta = \xi = 0$) and maximally entangled case ($\gamma = \delta = \pi/2$ and $\xi = 1/2$). Then the payoff is obtained for both cases by

$$\begin{aligned} P^k(\theta_k, \alpha_k, \beta_k) &= C_A C_B C_C \Big(\eta_1 \$^{(k)}_{000} + \eta_2 \$^{(k)}_{111} + \xi\mu_p(\$^{(k)}_{000} - \$^{(k)}_{111}) \cos 2(\alpha_A + \alpha_B + \alpha_C)\Big) \\ &+ S_A S_B S_C \Big(\eta_2 \$^{(k)}_{000} + \eta_1 \$^{(k)}_{111} - \xi\mu_p(\$^{(k)}_{000} - \$^{(k)}_{111}) \cos 2(\beta_A + \beta_B + \beta_C)\Big) \\ &+ C_A C_B S_C \Big(\eta_1 \$^{(k)}_{001} + \eta_2 \$^{(k)}_{110} + \xi\mu_p(\$^{(k)}_{001} - \$^{(k)}_{110}) \cos 2(\alpha_A + \alpha_B - \beta_C)\Big) \\ &+ S_A S_B C_C \Big(\eta_2 \$^{(k)}_{001} + \eta_1 \$^{(k)}_{110} - \xi\mu_p(\$^{(k)}_{001} - \$^{(k)}_{110}) \cos 2(\beta_A + \beta_B - \alpha_C)\Big) \\ &+ S_A C_B C_C \Big(\eta_1 \$^{(k)}_{100} + \eta_2 \$^{(k)}_{011} - \xi\mu_p(\$^{(k)}_{100} - \$^{(k)}_{011}) \cos 2(-\beta_A + \alpha_B + \alpha_C)\Big) \\ &+ C_A S_B S_C \Big(\eta_2 \$^{(k)}_{100} + \eta_1 \$^{(k)}_{011} + \xi\mu_p(\$^{(k)}_{100} - \$^{(k)}_{011}) \cos 2(-\alpha_A + \beta_B - \beta_C)\Big) \\ &+ S_A C_B S_C \Big(\eta_1 \$^{(k)}_{101} + \eta_2 \$^{(k)}_{010} - \xi\mu_p(\$^{(k)}_{101} - \$^{(k)}_{010}) \cos 2(\beta_A - \alpha_B + \beta_C)\Big) \\ &+ C_A S_B C_C \Big(\eta_2 \$^{(k)}_{101} + \eta_1 \$^{(k)}_{010} + \xi\mu_p(\$^{(k)}_{101} - \$^{(k)}_{010}) \cos 2(\alpha_A - \beta_B + \alpha_C)\Big), \end{aligned} \tag{81}$$

where $\mu_p = 1 - p$. In such as the previous cases, taking $\alpha_k = \beta_k = 0$, the payoffs are obtained for the non-entangled case and maximally entangled case as the follows;

$$\begin{aligned} P^k(\theta_k, 0, 0) &= C_A C_B C_C \$^{(k)}_{000} + S_A S_B S_C \$^{(k)}_{111} + C_A C_B S_C \$^{(k)}_{001} + S_A S_B C_C \$^{(k)}_{110} + S_A C_B C_C \$^{(k)}_{100} \\ &+ C_A S_B S_C \$^{(k)}_{011} + S_A C_B S_C \$^{(k)}_{101} + C_A S_B C_C \$^{(k)}_{010}, \text{ for non-entangled case,} \end{aligned} \tag{82}$$

$$\begin{aligned} P^k(\theta_k, 0, 0) &= \frac{1}{2}\Big[C_A C_B C_C \Big(\$^{(k)}_{000} + \$^{(k)}_{111} + \mu_p(\$^{(k)}_{000} - \$^{(k)}_{111})\Big) + S_A S_B S_C \Big(\$^{(k)}_{000} + \$^{(k)}_{111} - \mu_p(\$^{(k)}_{000} - \$^{(k)}_{111})\Big) \\ &+ C_A C_B S_C \Big(\$^{(k)}_{001} + \$^{(k)}_{110} + \mu_p(\$^{(k)}_{001} - \$^{(k)}_{110})\Big) + S_A S_B C_C \Big(\$^{(k)}_{001} + \$^{(k)}_{110} - \mu_p(\$^{(k)}_{001} - \$^{(k)}_{110})\Big) \\ &+ S_A C_B C_C \Big(\$^{(k)}_{100} + \$^{(k)}_{011} - \mu_p(\$^{(k)}_{100} - \$^{(k)}_{011})\Big) + C_A S_B S_C \Big(\$^{(k)}_{100} + \$^{(k)}_{011} + \mu_p(\$^{(k)}_{100} - \$^{(k)}_{011})\Big) \\ &+ S_A C_B S_C \Big(\$^{(k)}_{101} + \$^{(k)}_{010} - \mu_p(\$^{(k)}_{101} - \$^{(k)}_{010})\Big) + C_A S_B C_C \Big(\$^{(k)}_{101} + \$^{(k)}_{010} + \mu_p(\$^{(k)}_{101} - \$^{(k)}_{010})\Big)\Big], \\ &\qquad \text{for maximally entangled case.} \end{aligned} \tag{83}$$

We observe that μ_p vanishes from P^k in the non-entangled case. So we can not detect the influence of wiretapping. But P^k depends on μ_p in the maximally entangled case. Thus we can detect a wiretapper by comparing two payoffs (one has original value and another has a deviate value from it). Notice that when $\alpha_k\beta_k \neq 0$, tuning the values of α_k and β_k obscures μ_p dependence on the payoff. As result, detecting wiretappers is available only at $\alpha_k = \beta_k = 0$.

Though the maximally entangled case and the non-entangled case provided essentially equivalent way as QKD in the previous section, the latter is not available in the case with wiretappers.

4.3 Partially Entangled Cases

In this cases, (i) $\delta = 0$ and $\gamma = \pi/2$ or (ii) $\delta = \pi/2$ and $\gamma = 0$. Moreover $\theta_A\theta_B\theta_C \neq 0$, $\alpha_k = 0 = \beta_C$, $\beta_A - \beta_B = \pi$ and $\beta_A + \beta_B = 2\pi$ are chosen for simplicity like in the subsection 3.4.

Then we obtain the following expressions for the last term in Eq. (8);

$$\begin{aligned} P^k(\theta_k, 0, \beta_k)_{last} &= \frac{1}{8}\mu_p \sin[\theta_A, \theta_B, \theta_C]\Big\{\sin\big(\delta - \gamma\big) \sum_{a,b,c\in\{0,1\}} \$^{(k)}_{abc}(-1)^{(a+b+c)}\Big\}, \text{ for } (\delta, \gamma) = (0, \pi/2), \\ &= -\frac{1}{8}\sin[\theta_A, \theta_B, \theta_C]\Big\{\sin\big(\delta - \gamma\big) \sum_{a,b,c\in\{0,1\}} \$^{(k)}_{abc}(-1)^{(a+b+c)}\Big\}, \text{ for } (\delta, \gamma) = (\pi/2, 0). \end{aligned} \tag{84}$$

So the payoff is obtained by

$$\begin{aligned} P^k(\theta_k, \alpha_k, \beta_k) &= \frac{1}{2}\Big[C_A C_B C_C \Big(\$^{(k)}_{000} + \$^{(k)}_{111}\Big) + S_A S_B S_C \Big(\$^{(k)}_{000} + \$^{(k)}_{111}\Big) + C_A C_B S_C \Big(\$^{(k)}_{001} + \$^{(k)}_{110}\Big) \\ &+ S_A S_B C_C \Big(\$^{(k)}_{001} + \$^{(k)}_{110}\Big) + S_A C_B C_C \Big(\$^{(k)}_{100} + \$^{(k)}_{011}\Big) + C_A S_B S_C \Big(\$^{(k)}_{100} + \$^{(k)}_{011}\Big) \\ &+ S_A C_B S_C \Big(\$^{(k)}_{101} + \$^{(k)}_{010}\Big) + C_A S_B C_C \Big(\$^{(k)}_{101} + \$^{(k)}_{010}\Big)\Big] + Eq.(84). \end{aligned} \tag{85}$$

Thus the payoff depends on $\mu_p = 1 - p$ only in the case (a) from Eq. (84) and (85). In principle, we can detect an eavesdropper, only when the parameters are (i) $\delta = 0$ and $\gamma = \pi/2$. From 4.2 and 4.3, we find that when $\gamma = \pi/2$ where the initial state is an entangled state, we can detect an eavesdropper.

5 Summary and Consideration

In this article we propose a new QKD method. This method is different from the scheme proposed by [10], though it essentially takes our ground on three-player quantum games and Greenberg-Horne-Zeilinger triplet entangled state (GHZ state) [16] is used.

Alice , Bob and Charlie join the game. Alice prepares the initial quantum state, and sends the second qubit and third qubit to Bob and Charlie, respectively, but keeps the first qubit for herself. After Bob and Charlie accept their qubits, they locally manipulate their individual qubits by some unitary operator, respectively. Three players can choose a favorite parameter set of the unitary operators. After that, Bob and Charlie return their qubit manipulated by their unitary operators to Alice. Alice performs a measure of the total state (3 qubits)to determine the payoffs, and conveys some information to Bob and Charlie or opens to the public. By the information, Bob and Charlie can find opponent's strategy and payoff of the game. Thus everyone has common information. There are not any arbiters in our scheme, since existence of an arbiter increases the risk of wiretapping. For it is difficult to detect wiretapping, when an arbiter sends classical information.

We investigated by dividing our protocol into three cases, non-entangled cases, maximally entangled cases and partially entangled cases, to analyze it. We see that non-entangled cases and maximally entangled ones are essentially equivalent, since they are converted by a linear transformation each other. On the contrary, the partially entangled case has a little particular property and produces a sort of dense coding method.

Lastly we discussed robustness for eavesdrop so that we showed that though maximally entangled case and non-entangled case provided essentially equivalent way as QKD, the latter is not available in the case there are eavesdroppers. The effect of eavesdropping disappears from the payoff in the non-entangled case. In partially entangled case, we find that we can detect an eavesdropper by choosing some suitable parameter for δ and γ, especially $\gamma = \pi/2$, in principle. So this case gives a robust protocol. As summary, we find an entangled initial state ($\gamma \neq 0$) gives robust protocols in the all cases of this article.

References

[1] M.A. Nielsen and I.L.Chuang, "Quantum Computational and Quantum Information, Cambridge University Press, 2000

[2] D.A. Meyer, "Quantum Strategies", Phys.Rev.Lett.82, 1052(1999)

[3] J.Eisert, M.Wilkens and M.Lewenstein, "Quantum Games and Quantum Strategies", Phys.Rev.Lett.83, 3077(1999)

[4] A.F.H. Rosero, "Classification quantum symmetric nonzero-sum 2 X2 games in the Eisert scheme", quant-ph/0402117(2004)

[5] L.Marinatto and T.Weber, "A Quantum Approach To Static Games Of Complete Information", Phys.Lett. A, 272, 291-303 (2000); quant-ph/0004081(2000)

[6] A. Iqbal, "Studies in the theory of quantum games", quant-ph/0503176(2006)

[7] J.O. Grabbe, "An introduction to quantum game theory", quant-ph/0506219(2005)

[8] Nawaz and A.H. Toor, "Generalized Quantization Scheme for Two-Person Non-Zero-Sum Games", J. Phys. A: Math. Gen. 37, 11457-11463 (2004); quant-ph/0409046(2004)

[9] AM.Ramzan and M.K. Khan, "Communication aspects of a three-player Prisoner's Dilemma quantum game", J. Phys. A: Math. Theor. 42, 025301 (2009); 0902.4760quant-ph (2009)

[10] AM.Ramzan and M.K. Khan, "Multiparty quantum cryptographic protocol", Chinese Phys. Lett. 25 3543-3546 (2008); 0902.2528quant-ph (2009)

[11] R. Rivest, A. Shamir and L. Adelman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, vol.21,120(1978)

[12] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM J. Comput. 26 (5), 1484-1509(1997); doi:10.1137/S0036144598347011; arXiv:quant-ph/9508027v2 . Revised version of the original paper by Peter Shor ("28 pages, LaTeX. This is an expanded version of a paper that appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994. Minor revisions made January, 1996").

[13] Bennett, C.H. and G. Brassard, "Public key distribution and coin tossing", in Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York), p. 175(1984).

[14] Ekert, A.K., gQuantum cryptography based on Bellfs theoremh,Phys. Rev. Lett. 67, 661(1991).

[15] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus and Momtchil Peev, "The Security of Practical Quantum Key Distribution", Rev. Mod. Phys. 81, 1301 (2009)

[16] Daniel M. Greenberger, Michael A. Horne, Anton Zeilinger, "Going Beyond Bell's Theorem", Phys.Rev.Lett. 82, 1345-1349(1999); arXiv:quant-ph/9810035 (1998)

[17] A. Nawaz and A.H. Toor. "The Role of Measurement in Quantum Games", ;J. Phys. A: Math. Gen. 39, 2791(2006); quant-th/0602111(2006)