Copyright © 2019 Tech Science Press CMC, vol.58, no.2, pp.335-347, 2019

Rational Non-Hierarchical Quantum State Sharing Protocol

Zhao Dou[1], Gang Xu[1, *], Xiubo Chen[1] and Kaiguo Yuan[2]

Abstract: Rational participants want to maximize their benefits. The protocol with rational participants will be more realistic than the protocol with honest, semi-honest and dishonest participants. We research the rational non-hierarchical quantum state sharing in this paper. General steps of some known quantum state sharing protocol are summarized. Based on these steps, a new rational protocol is proposed. It means that lots of common protocols could be modified to rational protocols. Our protocol is widely applicable. Analyses show that the proposed protocol is rational and secure. It is also all-win for agents. Furthermore, number of deceiving agents is considered to redefine the utilities of agents.

Keywords: Quantum secret sharing, rational protocol, general steps.

1 Introduction

Secret sharing (SS) is one of the most important topics in cryptography. Unfortunately, classical cryptography can usually only achieve provable security or computational security. A possible tool to achieve unconditional security is quantum mechanics.

In 1984, Bennett et al. [Bennett and Brassard (1984)] firstly proposed the concept of quantum cryptography, and designed a quantum key distribution (QKD) protocol. In this protocol, only single particle state is needed. It is easy to perform the protocol. After that, quantum cryptography protocols were widely researched [Jiang, Jiang and Ling (2014); Qu, Chen, Zhou et al. (2010); Qu, Wu, Wang et al. (2017); Qu, Chen, Ji et al. (2018)]. QKD protocols based on continuous variable were also investigated. In 1995, Huttner et al. [Huttner, Imoto, Gisin et al. (1995)] used generalized measurements to design the protocol, and considered photon-number-splitting (PNS) attack. Recently, Gong et al. [Gong, Song, He et al. (2014)] proposed a QKD protocol based on entanglement properties of two-mode squeezed states. The protocol could be utilized to transmit the pre-determined key, which is pretty secure and effective and will become a research focus.

Not only key distribution, SS problem could also be solved by quantum mechanics. In 1999, Hillery et al. [Hillery, Bužek and Berthiaume (1999)] investigated the quantum secret sharing (QSS) protocol based on Greenherger-Horne-Zeilinger (GHZ) state for the first time. Two protocols were given to share classical secrets and quantum secrets (i.e.,

[1] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[*] Corresponding Author: Gang Xu. Email: gangxu_bupt@163.com.

CMC. doi:10.32604/cmc.2019.04159 www.techscience.com/cmc

unknown quantum states), respectively. The QSS protocol utilized to share quantum secret is also called as quantum state sharing (QSTS) or quantum information splitting (QIS) sometimes. Since quantum state is the most important part in quantum information processing, sharing quantum state is naturally necessary so that no agent can obtain the key secret alone.

From the view of agents' authority, QSTS could be divided into two parts: non-hierarchical QSTS (NQSTS) and hierarchical QSTS (HQSTS). The latter is usually called as hierarchical QIS (HQIS). Hillery et al.'s protocol [Hillery, Bužek and Berthiaume (1999)] is an NQSTS protocol. In this kind of protocol, all the agents are equal. Concretely, they have the same authority to recover the state. Their measurement results are equally important. This case is similar to the network system [Lu, Wang and Wang (2012); Lv and Wang (2017); Pang, Liu, Zhou et al. (2017); Qu, Keeney, Robitzsch et al. (2016)]. In 2010, Wang et al. [Wang, Xia, Wang et al. (2010)] firstly proposed an HQIS protocol, in which agents are divided into two grades. Agents in different grades have different authorities to recover the state.

There are two points ignored in common QSTS protocols [Li, Zhang and Peng (2004); Deng, Li, Li et al. (2005a); Deng, Li, Li et al. (2005b); Li, Zhou, Li et al. (2006); Li, Deng and Zhou (2007); Liu, Liu and Zhang (2008); Muralidharan and Panigrahi (2008); Xiu, Dong, Gao et al. (2008); Shi, Huang, Yang et al. (2011); Kang, Chen and Yang (2014); Huang (2015); Li, Wang, Zhang et al. (2015); Wang, Wang, Chen et al. (2015); Ramírez, Falaye, Sun et al. (2017)]. On one hand, only the agent who recovers the state (here we denote him as Bob_k) will obtain the secret state. So his role is more important than the others'. This role is delegated by authors directly in general. But in fact, it is vital to consider the person who recovers the secret state. On the other hand, the others may deviate from the protocol. In this case, they may deceive Bob_k in order to gain more benefits.

Rational protocol is a kind of solutions to solve these problems. Halpern et al. [Halpern and Teague (2004)] investigated a rational secret sharing protocol in 2006. Random numbers are introduced to affect the behaviors of players. The expected rounds of the three-party protocol are $5/\alpha^3$. Here, α is the probability of each player cooperating. After that, Groce et al. [Groce and Katz (2012)] showed that whenever computing the function is a strict Nash equilibrium in the ideal world, then it is possible to construct a rational fair protocol computing the function in the real world. In 2016, Wang et al. [Wang, Chen, Leung et al. (2016)] investigated the fairness in secure computing protocols based on incentives. New utility definitions are given according to incentives for rational players.

In 2015, Maitra et al. [Maitra, Joyee, Paul et al. (2015)] firstly introduced the concept of rational agent to QSS (to be exact, NQSTS). A rational protocol to share a known quantum state among *n* agents is investigated. Since the state is known, and can be copied by the dealer, all the agents will obtain the secret state at the end of protocol. In 2017, another rational NQSTS protocol was proposed by Dou et al. [Dou, Xu, Chen et al. (2018)]. This protocol is based on Li et al.'s common multi-party NQSTS protocol [Li, Zhou, Li et al. (2006)]. In Dou et al. [Dou, Xu, Chen et al. (2018)], just like most of QSTS protocols, the state is supposed to be unknown. Hence, only one agent will obtain the state finally. Another difference between protocols in Maitra et al. [Maitra, Joyee, Paul et al. (2015)] and Dou et al. [Dou, Xu, Chen et al. (2018)] is that Byzantine assumption holds in the latter protocol, but fail-stop assumption holds in the former one.

However, steps in Dou et al.'s protocol [Dou, Xu, Chen et al. (2018)] are learned from Li et al.'s protocol [Li, Zhou, Li et al. (2006)]. As we mentioned above, there exist numerous NQSTS protocols up to now. Different protocols have different ranges of application. The rational protocol whose steps are learned from the other QSTS protocols should be researched.

In this paper, we follow the work in Dou et al. [Dou, Xu, Chen et al. (2018)], and research the rational NQSTS protocol more deeply. Firstly, we summarize the general steps of aforementioned NQSTS protocols. Secondly, corresponding rational protocols which are based on these steps are proposed. The common protocols whose steps could be summarized as steps in Subsection 2.2 could be utilized in our protocol. The modification is simple and easy to be performed. Our protocol is compatible with common protocols. The agent who recovers the quantum state is not predetermined, or determined by the dealer. In fact, it is elected by all the agents randomly. Thirdly, security, utilities, correctness, fairness, Nash equilibrium and Pareto optimality of our rational protocol are analyzed in detail. Especially, utilities of agents are redefined. In this paper, for any agent, influences of the others' threat are weighed by the number of threateners. If more agents choose to threaten, then Bob$_k$ will hold less utility. This is more realistic since he needs the help of all the others, and will pay to each of them. This also is an improvement from protocol in Dou et al. [Dou, Xu, Chen et al. (2018)].

The following sections are organized as follow. In Section 2, some preliminaries are introduced one by one. After that, a new rational QSTS protocol is given in Section 3. Later, analyses of proposed protocols are shown in Section 4. Finally, conclusions are given in Section 5.

2 Preliminaries

In this section, some preliminaries are given. Notations of our protocols are listed in Subsection 2.1. Later, general steps of NQSTS protocols are summarized in Subsection 2.1. Hereafter, some basic concepts of rational multi-party computation protocols are introduced in Subsection 2.3. Finally, a simple random election method is described in Subsection 2.4. All of these preliminaries will be employed in the next sections.

2.1 Notations

Table 1: The Notations in this paper

Notation	Description
$\|\Phi\rangle$	Quantum Carrier
$\|\Psi\rangle$	Secret state
Alice	The boss/dealer
Bob$_j$ ($1 \leq j \leq N$)	Agents
Bob$_k$	The agent who recovers the state

2.2 General steps of an NQSTS protocol

We reread abovementioned common NQSTS protocols, and summarize the general steps of an (*N*+1)-party protocols as follows. Here, eavesdropping checking and some other non-core steps are omitted.

[N-1] Suppose that $\left|\Phi\right\rangle$ is an (*aN*+*a*+*b*)-particle state, the secret $\left|\Psi\right\rangle$ is an *a*-particle state. Alice prepares enough states $\left|\Phi\right\rangle$, and shares them with agents respectively. Concretely, each agent holds *a* particles, and Alice keeps *b* particles.

[N-2] Alice measures $\left|\Psi\right\rangle$ and her *b* carrier particles in basis B_1. Agents Bob$_j$ ($j \neq k$) also measure their *a* particles in basis B_2.

[N-3] According to above measurement results, Bob$_k$ performs corresponding operations to recover $\left|\Psi\right\rangle$.

2.3 Rational multi-party computation protocol

Mathematics provides many tools [Dong, Zhang, Zhang et al. (2014)] to solve practical problems. In game theory, an *n*-party game could be denoted by $\Gamma = (\{P_i\}_{i=1}^n, \{A_i\}_{i=1}^n, \{U_i\}_{i=1}^n)$. P_i is the *i*th player, his strategy set is A_i. One of his strategy is a_i, so we have $a_i \in A_i$. Let $A \equiv A_1 \times A_2 \times ... \times A_n$, then $\boldsymbol{a} = (a_1, a_2, ..., a_n) \in A$ is a strategy vector of game Γ. Further, P_i's utility for $\boldsymbol{a}$ is $U_i(\boldsymbol{a})$. If he prefers strategy vector $\boldsymbol{a}$ than $\boldsymbol{a}'$, then we say $U_i(\boldsymbol{a}) > U_i(\boldsymbol{a}')$.

In addition, for a given strategy vector $\boldsymbol{a} = (a_1, a_2, ..., a_n)$, $\boldsymbol{a}_{-i}$ could be denoted as $(a_1, ..., a_{i-1}, a_{i+1}, ..., a_n)$, then $(a_i', \boldsymbol{a}_{-i}) = (a_1, ..., a_{i-1}, a_i', a_{i+1}, ..., a_n)$.

Definition 1 (Strict Nash Equilibrium) [Maitra, Joyee, Paul et al. (2015)]. A strategy vector $\boldsymbol{a}$ in the game Γ is a strict Nash equilibrium, if we have $U_i(a_i', \boldsymbol{a}_{-i}) < U_i(\boldsymbol{a})$ for each player P_i and his any other strategy a'.

Definition 2 (Pareto Optimality) [Osborne and Rubinstein (1994)]. A strategy vector $\boldsymbol{a}$ in the game Γ is a Pareto optimality if it is impossible to increase the utility of a player without decreasing any others. In other word, if $U_i(\boldsymbol{a}') > U_i(\boldsymbol{a})$ ($i \in \{i_1, i_2, ..., i_c\}$, $c < n$), then $U_j(\boldsymbol{a}') < U_j(\boldsymbol{a})$, $\exists\ j$ ($j \notin \{i_1, i_2, ..., i_c\}$).

2.4 A simple method to randomly elect one player among N players

For *N* players P_j ($1 \leq j \leq N$), a simple way to randomly elect a representative is given as follows.

[E-1] All the players P_j ($1 \leq j \leq N$) randomly publish a number c_j ($0 \leq c_j \leq N-1$) at the same time.

[E-2] The publishing time of each number will be checked one by one. If a number is not published on time, the player will be disqualified. The other players will restart the election game.

[E-3] If all the publishing times are the same, players can compute $C = \sum_N c_j$. Here, $\sum_N$ denotes summation modulo *N*. P_{C+1} will be the chosen one.

3 The proposed rational NQSTS protocol

In this section, a new rational NQSTS protocol is proposed. An (*N*+1)-party common NQSTS protocol could be modified into an *N*-party rational protocol. The processes are given here. Since processes of different participants are described severally in general rational protocol, processes of our proposed protocol are also shown according to this way.

3.1 The dealer's protocol

[D-1] The dealer prepares an *r*-length bit list, in which only one bit is 1. For example, $list = \{\underbrace{0...0}_{p}1\underbrace{0...0}_{r-1-p}\}$. In the *i*th round, if $list_i = 1$, she goes to step [D-2], otherwise step [D-$2'$].

[D-2] Then, the dealer prepares enough (*aN*+*a*+*b*)-particle states $\left|\Phi\right\rangle$. She shares them with all the agents. Each agent holds *a* particles, and Alice keeps the reminding *a*+*b* particles.

[D-3] The dealer measures $\left|\Psi\right\rangle$ and the *b* carrier particles in basis B_1 .

[D-4] She asks all the *N* agents Bob$_j$ to measure particles in basis B_2 . Then, she tells agents to publish the measurement results.

[D-5] She sends the reminding *a* particles to the elected Bob$_k$ via quantum teleportation [Rigolin (2005); Zha and Song (2007)]. Alice finishes her work.

[D-$2'$] The dealer shares arbitrary *a* Bell states with each agent.

[D-$3'$] She asks all the *N* agents Bob$_j$ to measure particles and publish the results just like in step [D-4].

[D-$4'$] After that, she measures corresponding particles in her hand, and analyzes all the results. Further, she can deduce which agent is deceiving, and publish the ID of deceiving agents. Then, she goes to the next round.

3.2 Bobj's protocol

[B-1] In each round, all the agents perform B_2 basis measurement on their *a* particles, and announce the results as the dealer's claim, respectively. If $list_i = 1$, they go to step [B-2], otherwise, step [B-$2'$].

[B-2] They randomly elect one of them using the random election method. The chosen one, i.e., Bob$_k$, will recover the state afterwards.

[B-3] Bob$_k$ performs some local operations to recover $\left|\Psi\right\rangle$. These operations are related to all the other agents' measurement results. The protocol is accomplished.

[B-$2'$] Some agents may be informed that they are forbidden to participate in the next λ rounds because they are deceiving. The others go to the next round.

4 Analysis of proposed NQSTS protocol

In this section, security, utilities, correctness, fairness, Nash equilibrium and Pareto optimality of our rational NQSTS protocol are analyzed one by one.

4.1 Security

With the development of computer science, security of data has attracted more and more attention. Security of our protocol is analyzed below.

On one hand, our protocol is based on common NQSTS protocols. Any secure QSTS protocol, which can be generalized to protocol in Section 0, can be modified to a rational version. On the other hand, comparing our rational protocol with common protocols, the only key change is that teleportation is performed between the dealer and Bob$_k$. If a secure teleportation protocol is performed here, this process is secure too.

In conclusion, the security of our rational protocol is equivalent to the original common protocol. If the original common protocol is secure, our rational protocol is also secure.

4.2 Utilities

As is well known, the agent who recovers the state plays a different role from the helpers. His utility is different from the other's further. Therefore, utilities of Bob$_k$ and Bob$_j$ ($j \neq k$) are listed respectively.

Here, *COO* represents the strategy *Cooperating*, which means that the agent will choose to cooperate with the others and fulfill the protocol honestly. *DEC* denotes *Deceiving*. it denotes that the agent will deceive the others. For example, he may report a false measurement result. *REC* denotes *Recovering*, which means that Bob$_k$ will recover the state.

Discussions about these utilities are given below. (1) Since he will be punished if he does not pass the check, we have $U_g > U_f$. Further, if he doesn't pass the check in the *i*th round, he will be forbidden to participate in the protocol in the next λ rounds. The probability of not participating in the sharing is $\lambda/(r-i)$. So we could suppose that $U_f = -k\lambda/(r-i)$ ($k > 0$). (2) Because getting a true state is naturally better than a false one, it is easy to obtain that $U_s > U_e$. (3) A cooperator is not responsible for deceivers' behaviors, so $U_{ps} = U_{pe}$. For the rest of the paper, no differentiation is made between U_{ps} and U_{pe}. (4) The motivation of agents choosing to threaten is he may benefit more than to help, so $U_t > U_{ps}$. In summary, we know that $U_g > U_f = -k\lambda/(r-i)$, $U_s > U_e$ and $U_t > U_{ps} = U_{pe}$.

Table 2: Utilities of agents in our rational QSTS protocol

$List_i$	Role	Strategy	Outcome	Explanation	Utility
0	Any agent	*COO*	Passed	He passes the check.	U_g
0	Any agent	*DEC*	Failed	He does not pass the check.	U_f
1	Bob$_k$	*REC*	True state	He obtains the true state successfully.	U_s
1	Bob$_k$	*REC*	False state	He obtains a false state.	U_e
1	Bob$_j$ ($j \neq k$)	*DEC*	Threatening	He threatens that his results are wrong.	U_t
1	Bob$_j$ ($j \neq k$)	*COO*	Successful helping	He helps Bob$_k$ obtain the state successfully.	U_{ps}
1	Bob$_j$ ($j \neq k$)	*COO*	Unsuccessful helping	He wants to help Bob$_k$, but Bob$_k$ gets a false state since someone else is threatening.	U_{pe}

Table 3: Utilities matrix of agents

	Bob$_3$	*DEC*	*COO*
Bob$_1$	Bob$_2$		
DEC	*DEC*	$U_A(2), U_A(2), U_A(2)$	$U_A(1), U_A(1), U_B(2)$
	COO	$U_A(1), U_B(2), U_A(1)$	$U_A(0), U_A(0), U_B(1)$
COO	*DEC*	$U_B(2), U_A(1), U_A(1)$	$U_B(1), U_A(0), U_B(1)$
	COO	$U_B(1), U_B(1), U_A(0)$	$U_B(0), U_B(0), U_B(0)$

In addition, U_e is employed to describe the utility of Bob$_k$ if he is threatened. Since he needs the help of all the agents, his utility will be impacted by all the deceiving agents. Here, x denotes the number of deceiving agents, except for himself (if he is also deceiving). Suppose Δ is the reduction of Bob$_k$'s utility when one more agent chooses deceiving. We further have $U_e = U_s - x\Delta$.

Next, take the three-party QSTS game as an example, utilities matrix of agents in our protocol could be described in Tab. 3.

$U_A(x)$ and $U_B(x)$ represent the utilities of Bob$_j$ ($1 \le j \le N$) when he chooses to deceive and to cooperate, respectively.

$$\begin{aligned} U_A(x) &= \Pr[list_i = 0] * \{\Pr[\text{passes the check}] * U_g + \Pr[\text{does not pass the check}] * U_f\} \\ &\quad + \Pr[list_i = 1] * \{\Pr[\text{is not chosen as Bob}_k] * U_t + \Pr[\text{is chosen as Bob}_k] * U_e\} \\ &= \frac{r-i}{r-i+1} U_f + \frac{1}{r-i+1} (\frac{N-1}{N} U_t + \frac{1}{N} U_e) \\ &= \frac{r-i}{r-i+1} U_f + \frac{1}{r-i+1} [\frac{N-1}{N} U_t + \frac{1}{N} (U_s - x\Delta)]. \end{aligned} \tag{1}$$

$$\begin{aligned} U_B(x) &= \Pr[list_i = 0] * \{\Pr[\text{passes the check}] * U_g + \Pr[\text{does not pass the check}] * U_f\} \\ &\quad + \Pr[list_i = 1] * \{\Pr[\text{is not chosen as Bob}_k] * U_t + \Pr[\text{is chosen as Bob}_k] * U_e\} \\ &= \frac{r-i}{r-i+1} U_g + \frac{1}{r-i+1} [\frac{N-1}{N} U_{pe} + \frac{1}{N} (U_s - x\Delta)]. \end{aligned} \tag{2}$$

Here, in the ith round, $\frac{r-i}{r-i+1}$ is the probability of $list_i = 1$. $\frac{1}{N}$ is the probability of any agent chosen to be Bob$_k$.

4.3 Correctness

Definition 3 (Correctness) [Dou, Xu, Chen et al. (2018)]. A rational QSTS game Γ is correct if the following holds

$$\Pr[o_k(\Gamma, (a_j, \boldsymbol{a}_{-j})) = \text{False state}] \le \varepsilon \tag{3}$$

for each Bob$_j$'s arbitrary strategy $a_j \in \{DEV, COO\}$.

Theorem 1. The correctness of the protocol holds if all the agents are rational.

Proof. As a rational agent, Bob$_j$ ($1 \le j \le N$) wants to maximize his benefit. If he is chosen as Bob$_k$, he will recover the state faithfully. Otherwise, he will be a helper. In the second case, if he helps Bob$_k$ loyally, correctness of protocol will be affected. If he wants to threaten, he will mislead Bob$_k$ at first. But if he has obtained expected benefit, he will tell the true measurement result to Bob$_k$. The correctness is also ensured. In one word, the correctness of the protocol holds.

4.4 Fairness

Definition 4 (Fairness) [Dou, Xu, Chen et al. (2018)]. A rational QSTS game Γ is fair if the following hold

$$\Pr[o_j(\Gamma_1,(a_j,\boldsymbol{a}_{-j}))=\text{Bob}_k]\leq\Pr[o_{-j}(\Gamma_1,(a_j,\boldsymbol{a}_{-j}))=\text{Bob}_k], \tag{4}$$

$$\Pr[o_j(\Gamma_2,(a_j,\boldsymbol{a}_{-j}))=\text{True state}]\leq\Pr[o_{-j}(\Gamma_2,(a_j,\boldsymbol{a}_{-j}))=\text{True state}] \tag{5}$$

for any Bob$_j$ ($1\leq j\leq N$). Here, the game Γ is divided into two parts: the random election game Γ_1 and the sharing game Γ_2.

Theorem 2. There exist some values of λ and *r* that make the protocol achieve fairness.

Proof. Since each agent chooses a number randomly, entropy of c_j is $H(c_j)=\log_2 N$. Let the summation of all the other numbers is $C_{-j}=\sum_{k\neq j}^{N} c_k$. The condition entropy is $HC(C\,|\,C_{-j})=\log_2 N$, too. We also know that $H(C)=\log_2 N$. It means that even if *N*-1 agents colluded except for Bob$_j$, the value of *C* is still completely random for them. The probability of each agent chosen as Bob$_k$ is equal. Therefore, the fairness of game Γ_1 is proved.

As for the game Γ_2, any agent will not have incentive to deceive if the utility of *DEC* is less than that of *COO* when the other agents' strategies are fixed. In other word, the inequation $U_A(x)<U_B(x)$ needs to be satisfied.

$$\begin{aligned}U_A(x)-U_B(x)&=\frac{r-i}{r-i+1}(U_f-U_g)+\frac{1}{r-i+1}\frac{N-1}{N}(U_t-U_{pe})\\&=\frac{1}{r-i+1}[(r-i)U_f-(r-i)U_g+\frac{N-1}{N}(U_t-U_{pe})]\\&=\frac{1}{r-i+1}[-k\lambda-(r-i)U_g+\frac{N-1}{N}(U_t-U_{pe})].\end{aligned} \tag{6}$$

Since $U_f<U_g$ and $U_t>U_{pe}$, the relationship of size between $U_A(x)$ and $U_B(x)$ is uncertain. But if λ and $r-i$ are big enough, then we have $U_A(x)<U_B(x)$. Since i is alterable, we need to find a big *r* to ensure that $r-i$ is big enough. The fairness of Γ_2 will hold in this case.

In conclusion, if λ and *r* are big enough, the fairness of our protocol holds.

4.5 Strict Nash equilibrium

Theorem 3. There exist some values of λ and *r* that make the protocol achieve fairness.

Proof. As the designer of a protocol, we hope that strategy vector (*COO*, *COO*, *COO*) will be the Nash equilibrium. In this case, an agent will choose to cooperate for other agents' any given strategies. Therefore, the following conditions need to be satisfied:

$$U_A(x)<U_B(x). \tag{7}$$

Likewise, we can find some values of λ and *r* to ensure the Eq. (7). The conditions are the same as that in Subsection 4.5. The strict Nash equilibrium of our protocol also holds.

4.6 Pareto optimality

Theorem 4. There exist some suitable coefficients λ and *r* so that Pareto optimality is achieved.

Proof. The utilities of strategy vector (*COO*, *COO*, *COO*) are $(U_B(0), U_B(0), U_B(0))$. In order to make this strategy vector Pareto optimality, we need to ensure the following conditions:

(P1) One of $U_B(1), U_A(0)$ is smaller than $U_B(0)$.

(P2) One of $U_B(2), U_A(1)$ is smaller than $U_B(0)$.

(P3) $U_A(2)$ is smaller than $U_B(0)$.

On one hand, in the former subsection, we have showed the conditions of $U_B(x) > U_A(x)$. On the other hand, from Eqs. (1) and (2), it's easy to have $U_A(0) > U_A(1) > U_A(2)$ and $U_B(0) > U_B(1) > U_B(2)$.

Hence, we have $U_B(0) \geq U_B(x)$ and $U_B(0) > U_A(x)$. The conditions (P1)-(P3) are also hold naturally.

In summary, the strategy vector (*COO*, *COO*, *COO*) is the Pareto optimality for some suitable *r* and λ. Since each agent will choose to cooperate, and $U_B(0)$ is the maximum among utilities, all agents will have maximum utility in this case. In other word, they are all-win.

5 Conclusions

In this work, rational NQSTS protocol was researched. Firstly, lots of NQSTS protocols were restudied. General steps of them were summarized further. Secondly, a new rational NQSTS protocol was proposed, in which steps are learned from general steps of aforementioned protocols. Thirdly, analyses of proposed protocol were given. Particularly, utilities of agents are being redefined by the number of deceiving agents. The results show that our protocol is rational and secure. Besides that, agents will all win in our protocol.

Acknowledgement: Project supported by NSFC (Grant Nos. 61671087, 61272514, 61170272, 61003287, U1636106), the Fok Ying Tong Education Foundation (Grant No. 131067) and BUPT Excellent Ph.D. Students Foundation (Grant No. CX2018310).

References

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 7-11.

Chen, Y. (2015): Bidirectional quantum controlled teleportation by using a genuine six-qubit entangled state. *International Journal of Theoretical Physics*, vol. 54, no. 1, pp. 269-272.

Deng, F. G.; Li, C. Y.; Li, Y. S.; Zhou, H. Y.; Wang, Y. (2005a): Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. *Physical Review A*, vol. 72, no. 2, pp. 022338.

Deng, F. G.; Li, X. H.; Li, C. Y.; Zhou, P.; Zhou, H. Y. (2005b): Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. *Physical Review A*, vol. 72, no. 4, pp. 044301.

Dong, H. H.; Zhang, Y. F.; Zhang, Y. F.; Yin, B. S. (2014): Generalized bilinear differential operators, binary Bell polynomials, and exact periodic wave solution of Boiti-Leon-Manna-Pempinelli equation. *Abstract and Applied Analysis*, vol. 2014, no. 1, pp. 1-6.

Dou, Z.; Xu, G.; Chen, X. B.; Liu, X.; Yang, Y. X. (2018): A secure rational quantum state sharing protocol. *Science China Information Sciences*, vol. 61, no. 2, pp. 022501.

Gong, L. H.; Song, H. C.; He, C. S.; Liu, Y.; Zhou, N. R. (2014): A continuous variable quantum deterministic key distribution based on two-mode squeezed states. *Physica Scripta*, vol. 89, no. 3, pp. 035101.

Groce, A.; Katz, J. (2012): Fair computation with rational players. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 81-98.

Halpern, J.; Teague, V. (2004): Rational secret sharing and multiparty computation. *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, pp. 623-632.

Hillery, M.; Bužek, V.; Berthiaume, A. (1999): Quantum secret sharing. *Physical Review A*, vol. 59, no. 3, pp. 1829.

Huang, Z. (2015): Quantum state sharing of an arbitrary three-qubit state by using a seven-qubit entangled state. *International Journal of Theoretical Physics*, vol. 54, no. 9, pp. 3438-3441.

Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. (1995): Quantum cryptography with coherent states. *Physical Review A*, vol. 51, no. 3, pp. 1863.

Jiang, T. S.; Jiang, Z. W.; Ling, S. T. (2014): An algebraic method for quaternion and complex Least Squares coneigen-problem in quantum mechanics. *Applied Mathematics and Computation*, vol. 249, no. 1, pp. 222-228.

Kang, S. Y.; Chen, X. B.; Yang, Y. X. (2014): Multi-party quantum state sharing of an arbitrary multi-qubit state via χ-type entangled states. *Quantum Information Processing*, vol. 13, no. 9, pp. 2081-2098.

Li, X. H.; Deng, F. G.; Zhou, H. Y. (2007): Controlled teleportation of an arbitrary multi-qudit state in a general form with d-dimensional Greenberger-Horne-Zeilinger states. *Chinese Physics Letters*, vol. 24, no. 5, pp. 1151.

Li, D.; Wang, R. J.; Zhang, F. L.; Deng, F. H.; Baagyere, E. (2015): Quantum information splitting of arbitrary two-qubit state by using four-qubit cluster state and Bell-state. *Quantum Information Processing*, vol. 14, no. 3, pp. 1103-1116.

Li, Y.; Zhang, K.; Peng, K. (2004): Multiparty secret sharing of quantum information based on entanglement swapping. *Physics Letters A*, vol. 324, no. 5-6, pp. 420-424.

Li, X. H.; Zhou, P.; Li, C. Y.; Zhou, H. Y.; Deng, F. G. (2006): Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 39, no. 8, pp. 1975.

Liu, J.; Liu, Y. M.; Zhang, Z. J. (2008): Generalized multiparty quantum single-qutrit-state sharing. *International Journal of Theoretical Physics*, vol. 47, no. 9, pp. 2353-2362.

Lu, X.; Wang, H. X.; Wang, X. (2012): On Kalman smoothing for wireless sensor networks systems with multiplicative noises. *Journal of Applied Mathematics*, vol. 2012, no. 1, pp. 71750.

Lv, W. S.; Wang, F. (2017): Adaptive tracking control for a class of uncertain nonlinear systems with infinite number of actuator failures using neural networks. *Advances in Difference Equations*, vol. 2017, no. 1, pp. 374.

Maitra, A.; Joyee, de, S. J.; Paul, G.; Pal, A. K. (2015): Proposal for quantum rational secret sharing. *Physical Review A*, vol. 92, no. 2, pp. 022305.

Muralidharan, S.; Panigrahi, P. K. (2008): Perfect teleportation, quantum-state sharing, and super-dense coding through a genuinely entangled five-qubit state. *Physical Review A*, vol. 77, no. 3, pp. 032321.

Osborne, M. J.; Rubinstein, A. (1994): *A Course in Game Theory*. MIT press.

Pang, Z. H; Liu, G. P.; Zhou, D. H.; Sun D. H. (2017): Data-based predictive control for networked nonlinear systems with packet dropout and measurement noise, *Journal of Systems Science & Complexity*, vol. 30, no. 5, pp. 1072-1083.

Qu, Z.; Chen, S. Y.; Ji, S; Ma, S. Y.; Wang, X. J. (2018): Anti-noise bidirectional quantum steganography protocol with large payload, *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1-25.

Qu, Z.; Chen, X. B.; Zhou, X. J.; Niu, X. X.; Yang, Y. X. (2010): Novel quantum steganography with large payload, *Optics Communications*, vol. 283, no. 1, pp. 4782-4786.

Qu, Z.; Keeney, J.; Robitzsch, S.; Zaman, F.; Wang, X. (2016): Multilevel pattern mining architecture for automatic network monitoring in heterogeneous wireless communication networks. *China Communications*, vol. 13, no. 7, pp. 108-116.

Qu, Z.; Wu, S. Y.; Wang, M. M.; Sun, L.; Wang, X. J. (2017): Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels. *Quantum Information Processing*, vol. 16, no. 306, pp. 1-25.

Ramírez, M. D. G.; Falaye, B. J.; Sun, G. H.; Cruz-Irisson, M.; Dong, S. H. (2017): Quantum teleportation and information splitting via four-qubit cluster state and a Bell state. *Frontiers of Physics*, vol. 12, no. 5, pp. 120306.

Rigolin, G. (2005): Quantum teleportation of an arbitrary two-qubit state and its relation to multi-partite entanglement. *Physical Review A*, vol. 71, no. 3, pp. 032303.

Shi, R.; Huang, L. S.; Yang, W.; Zhong, H. (2011): Efficient symmetric five-party quantum state sharing of an arbitrary m-qubit state. *International Journal of Theoretical Physics*, vol. 50, no. 11, pp. 3329.

Wang, Y.; Chen, L.; Leung, H.; Chen, B. (2016): Fairness in secure computing protocols based on incentives. *Soft Computing*, vol. 20, no. 10, pp. 3947-3955.

Wang, M. M.; Wang, W.; Chen, J. G.; Farouk, A. (2015): Secret sharing of a known arbitrary quantum state with noisy environment. *Quantum Information Processing*, vol. 14, no. 11, pp. 4211-4224.

Wang, X. W.; Xia, L. X.; Wang, Z. Y.; Zhang, D. Y. (2010): Hierarchical quantum-information splitting. *Optics Communications*, vol. 283, no. 6, pp. 1196-1199.

Xiu, X. M.; Dong, L.; Gao, Y. J.; Chi, F. (2008): A theoretical scheme for multiparty multi-particle state sharing. *Communications in Theoretical Physics*, vol. 49, no. 5, pp. 1203.

Zha, X. W.; Song, H. Y. (2007): Non-Bell-pair quantum channel for teleporting an arbitrary two-qubit state. *Physics Letters A*, vol. 369, no. 5-6, pp. 377-379.