SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2018, Vol. 61 022501:1–022501:12
doi: 10.1007/s11432-016-9151-x

A secure rational quantum state sharing protocol

Zhao DOU[1], Gang XU[1,2], Xiu-Bo CHEN[1,5*], Xin LIU[3,4] & Yi-Xian YANG[1,5]

[1]*Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[2]*School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing* 100876*, China;*
[3]*School of Computer Science, Shaanxi Normal University, Xi'an* 710062*, China;*
[4]*School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou* 014010*, China;*
[5]*GuiZhou University, Guizhou Provincial Key Laboratory of Public Big Data, Guiyang* 550025*, China*

Received 11 December 2016/Accepted 16 January 2017/Published online 28 September 2017

Abstract A novel rational protocol to share two arbitrary qubits among multiple parties is investigated in this paper. First, the protocol is presented, which is learned from Li et al.'s protocol. Second, the utility, security, correctness, fairness, Nash equilibrium, and Pareto optimality of our scheme are discussed in detail, where the utility, correctness, and fairness of rational quantum state sharing protocols are creatively given because the agent who recovers the state plays a different and more important role. Another important point is that assumptions about our protocol are more practical and suitable than existing protocols.

Keywords rational, quantum state sharing, Nash equilibrium, secure, correct

Citation Dou Z, Xu G, Chen X-B, et al. A secure rational quantum state sharing protocol. Sci China Inf Sci, 2018, 61(2): 022501, doi: 10.1007/s11432-016-9151-x

1 Introduction

In the secret sharing (SS) problem, there exists a dealer Alice and some agents Bob_i. Alice owns a secret or some bits, which are split by her and shared by all the agents. Since the secret is fatal, Alice will send part of it to each agent, instead of the integrated secret. Only sufficient agents can recover the secret with the help of each other. This problem was first investigated by Shamir [1] and Blakley [2] in 1979. The quantum secret sharing (QSS) protocol is the quantum version solution of the SS problem. Quantum mechanics was introduced to ensure the unconditional security of the protocol [3, 4]. In 1999, Hillery et al. [5] proposed a QSS scheme with the Greenberger-Horne-Zeilinger (GHZ) state.

At the same time, Cleve et al. [6] studied how to share quantum information (a quantum secret), instead of classical bits, among different agents. This kind of protocol is called quantum state sharing (QSTS). Owing to the quantum no-cloning principle [7], an unknown quantum state cannot be copied as several ones. Only one agent, who is named Bob_k or Charlie, can obtain the state with the help of the others. In 2004, Li et al. [8] proposed a QSTS protocol to share an arbitrary unknown qubit via sharing Bell states and multi-particle GHZ basis measurement. Lance et al. [9] investigated a (2, 3) threshold quantum state sharing scheme in the same year. They demonstrated that average fidelity is equal to 0.73 ± 0.04.

In 2005, Deng et al. [10] proposed a multi-party controlled scheme to teleport an arbitrary two-particle state. In this scheme, a three-particle GHZ state were utilized as the quantum resource. Actually, most

* Corresponding author (email: flyover100@163.com)

controlled teleportation could be regarded as a QSTS protocol with or without a little modification [11]. The same is true of Deng et al.'s scheme [10]. After that, Li et al. [11] simplified the process of this scheme. Participants in [11], do not need to perform multi-party entanglement measurement or two-qubit joint operation, which makes their protocol easier to implement. They also expanded the scheme to a multi-particle version to extend its use. Later, Muralidharan and Panigrahi [12] designed a perfect QSTS protocol to share arbitrary single- and two-qubit states via maximally entangled five-qubit states. To complete the task, multi-particle measurements are needed. Recently, Li et al. [13] investigated how to share an arbitrary two-qubit state by using a cluster state and a Bell state. There are two agents in this scheme. Security analysis shows that it is safe. In addition, the deterministic QSTS in cavity quantum electrodynamics was investigated.

Halpern and Teague [14] considered a rational classical SS protocol in 2004. Rational players are not supposed to be honest or malicious. On the contrary, they only pay attention to their own benefit, and make decisions to maximize it. They will cooperate with others or not depending on which choice is more advantageous for themselves. Another all-important standpoint is that no rational multi-party computation protocol can be accomplished in a deterministic time [14].

In the view of assumption about players, we rechecked all the above QSTS protocols [6, 8–12], and found that agents are supposed to accomplish the sharing faithfully even if they are malicious. Indeed, the same assumption also holds in the general case. We do not think this is reasonable enough. Players actually will also have incentive to obstruct the accomplishment of sharing if they can benefit more.

Maitra et al. [15] investigated the rational QSTS scheme for the first time in 2015. The state is encoded by CSS code. A (3, 7) rational QSTS scheme was investigated first. In this scheme, the dealer is semi-offline. The generation to a (t, n) version scheme was given second. Correctness, fairness, and the existence of Nash equilibrium were analyzed. A (t, n) QSTS protocol with the offline dealer and the corresponding analysis were also described.

Another important assumption is whether the dealer knows the information about the state or not. In Maitra et al.'s protocol [15], the dealer does know, so she can copy the state and distribute the same particles to different agents. In addition, t agents can obtain the state simultaneously. However, it makes the protocol more like a remote state preparing (RSP) protocol, instead of the QSTS. In general, the dealer does not know the state, much less copy it. Only one agent can recover the state accordingly. The general case is more reasonable indeed.

The third assumption of a protocol is whether the setting of agents is Byzantine or fail-stop. In the fail-stop setting, a player will only fulfill his duty or drop out, depending on which choice is more beneficial. In contrast, a Byzantine agent may deviate from the protocol, such as sending false bits. It is evident that Byzantine agents are more practical and harder to investigate.

In this paper, we follow the work of Li et al. [11] and Maitra et al. [15], and design a novel rational QSTS protocol. The processes are learned from [11]. Some delicate and necessary modifications are made, which makes players prefer the strategy *Cooperating*. The properties of rational multi-party computation are also ensured: correctness, fairness, and the existence of Nash equilibrium. Furthermore, *Cooperating* is also the strategy which satisfies the Pareto optimality. In addition, our protocol is also as safe as Li et al.'s [11].

Compared with Maitra et al.'s protocol [15], on the one hand, we suppose that only one agent can obtain the state, instead of all t agents. On the other hand, the setting is Byzantine, rather than fail-stop. Our assumptions are more practical. A detailed discussion is also given.

The rest of paper is arranged as follow. Preliminaries, including a random electoral method, quantum mechanics, Li et al.'s scheme [11], and the basic concepts of the rational multi-party protocol are introduced in Section 2. Our novel rational QSTS protocol and analysis are shown in Sections 3 and 4, respectively. Discussion is described in Section 5. Finally, conclusion is given in Section 6.

2 Preliminaries

2.1 A simple method to randomly elect one player among N

For N players P_j $(1 \leqslant j \leqslant N)$, a simple way to elect a representative among themselves randomly could be described as follows.

[E-1] $2^{\lfloor \log_2^N \rfloor} - N$ virtual players are added. These players will not do anything. Now, there are $2^{\lfloor \log_2^N \rfloor}$ players in the election.

[E-2] Each of N real players randomly publishes one bit c_j. Then they can compute the XOR of c_j, $C = \bigoplus_{j=1}^{N} c_j$. Here, $\bigoplus$ denotes the addition module 2.

[E-3] If $C = 0$, then the first half of $2^{\lfloor \log_2^N \rfloor}$ players will still have the right to be elected, the others will lose, and vice versa.

(1) If all the players who have the rights are virtual, the election will be restarted.

(2) If more than one player has the right, and at least one of them is real, they will reperform the Steps [E-2] and [E-3] until only one exists.

(3) If only one player has the right, and is real, he will be the chosen one.

Although this way is not the true random in the quantum case [16], it is simple and easy to perform. More importantly, the result is co-determined by all the players instead of part of them. If this election is considered as a game, we can show that it is fair. The analysis is given in Subsection 4.4.

2.2 Quantum mechanics

Some vital quantum states and bases in our paper are now introduced.

(1) Bell states and Bell basis. Four Bell states are written as follows:

$$\begin{aligned} |\Phi^{0\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) = \frac{1}{\sqrt{2}}(|+\pm\rangle + |-\mp\rangle), \\ |\Phi^{1\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) = \frac{1}{\sqrt{2}}(|+\pm\rangle - |-\mp\rangle). \end{aligned} \tag{1}$$

They could be denoted as $|\Phi^{VP}\rangle$ with different V and P, and constructed as the Bell basis. Similarly, $|+\rangle$ and $|-\rangle$ could be rewritten as $|P\rangle$, and constructed as the X basis.

(2) GHZ states. In the three-particle case, there are $8 = 2^3$ GHZ states in total. They are listed as follows:

$$\begin{aligned} |\Psi^{00\pm}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), \quad |\Psi^{01\pm}\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle), \\ |\Psi^{10\pm}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), \quad |\Psi^{11\pm}\rangle = \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle). \end{aligned} \tag{2}$$

The best known state of these eight is $|\Psi^{00+}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. In the $(n+2)$-particle case, the counterpart is $|\Psi^n\rangle = \frac{1}{\sqrt{2}}(\prod_{i=1}^{n+2}|0\rangle + \prod_{i=1}^{n+2}|1\rangle)$.

2.3 Review of Li et al.'s QSTS protocol

In 2006, Li et al. [11] proposed a multi-party QSTS protocol. In the protocol, there are $n+1$ agents Bob_i $(1 \leqslant i \leqslant n+1)$ and a boss Alice. Suppose that the quantum state they want to share is an arbitrary two-particle state:

$$|\Upsilon\rangle_{xy} = (a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle)_{xy}, \tag{3}$$

where, $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. The processes are simply reviewed as follows.

[L-1] Alice prepares two $(n+2)$-particle GHZ states $|\Psi\rangle_{s_1} = |\Psi\rangle_{s_2} = \frac{1}{\sqrt{2}}(\prod_{i=1}^{n+2}|0\rangle + \prod_{i=1}^{n+2}|1\rangle)$, and shares them with the $n+1$ agents. The whole system is shown as

$$\begin{aligned} |\Psi\rangle_S &\equiv |\Upsilon\rangle_{xy} \otimes |\Psi\rangle_{s_1} \otimes |\Psi\rangle_{s_2} \\ &= (a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle)_{xy} \end{aligned}$$

$$\otimes \frac{1}{\sqrt{2}}\left(\prod_{i=1}^{n+2}|0\rangle_{a_i}+\prod_{i=1}^{n+2}|1\rangle_{a_i}\right)\otimes\frac{1}{\sqrt{2}}\left(\prod_{i=1}^{n+2}|0\rangle_{b_i}+\prod_{i=1}^{n+2}|1\rangle_{b_i}\right). \tag{4}$$

Alice sends the photons a_i and b_i to the agent Bob_i, respectively.

[L-2] Alice performs the Bell basis measurement on her photon x and a_{n+2}, y and b_{n+2}, respectively. The rest of the system becomes

$$|\Psi\rangle_{\mathrm{sub}}=\alpha\prod_{i=1}^{n+1}|00\rangle_{a_ib_i}+\beta\prod_{i=1}^{n+1}|01\rangle_{a_ib_i}+\gamma\prod_{i=1}^{n+1}|10\rangle_{a_ib_i}+\delta\prod_{i=1}^{n+1}|11\rangle_{a_ib_i}. \tag{5}$$

The parameter set $\{\alpha,\beta,\gamma,\delta\}$ is the permutation of $\{\pm a,\pm b,\pm c,\pm d\}$, and is related to the measurement results $V_{xa_{n+2}}$, $V_{yb_{n+2}}$, $P_{xa_{n+2}}$, and $P_{yb_{n+2}}$.

[L-3] Suppose that Bob_1 will recover the state, then Bob_i $(2\leqslant i\leqslant n+1)$ will perform X basis measurement to help him. The measurements they performed can be expressed as follows: $M\equiv[(\langle+|)^{n-t}(\langle-|)^t]_a\otimes[(\langle+|)^{n-q}(\langle-|)^q]_b$, where, $[(\langle+|)^{n-t}(\langle-|)^t]_a$ denotes the measurement operation related to the particles a_i, $[(\langle+|)^{n-q}(\langle-|)^q]_b$ is related to b_i. The symbols t and q are the numbers of agents who obtain the result $\langle-|$, respectively.

[L-4] After previous measurements, the state collapsed into

$$|\Psi\rangle_{a_1b_1}=(\alpha|00\rangle+(-1)^q\beta|01\rangle+(-1)^t\gamma|10\rangle+(-1)^{(q+t)}\delta|11\rangle)_{a_1b_1}. \tag{6}$$

Bob_i will perform local operations to recover the state $|\Upsilon\rangle$ according to the public measurement results $V_{xa_{n+2}}$, $V_{yb_{n+2}}$, P_a, and P_b. Here, $P_a=P_{xa_{n+2}}\otimes\prod_{i=2}^{n+1}P_{a_i}$, $P_b=P_{yb_{n+2}}\otimes\prod_{i=2}^{n+1}P_{b_i}$.

2.4 Rational multi-party computation protocol

Let $\Gamma=(\{P_i\}_{i=1}^n,\{A_i\}_{i=1}^n,\{u_i\}_{i=1}^n)$ denote a game which contains n players. Concretely, P_i is the ith player. The strategy set player P_i may perform is A_i. Let $A\equiv A_1\times A_2\times\cdots\times A_n$, then $\boldsymbol{a}=(a_1,a_2,\ldots,a_n)\in A$ is called as a strategy vector of this game. Here, a_i is the strategy of P_i and $\{u_i\}_{i=1}^n$ denotes the utility function. If P_i prefers strategy $\boldsymbol{a}$ to $\boldsymbol{a}'$, then we say $u_i(\boldsymbol{a})>u_i(\boldsymbol{a}')$. In addition, the outcome of this game is denoted as $\boldsymbol{o}(\boldsymbol{a})=(o_1,o_2,\ldots,o_n)$.

Further, for a given strategy $\boldsymbol{a}=(a_1,a_2,\ldots,a_n)$, $\boldsymbol{a}_{-i}$ is defined as $\boldsymbol{a}_{-i}\equiv(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)$, and naturally we have $(a_i',\boldsymbol{a}_{-i})=(a_1,\ldots,a_{i-1},a_i',a_{i+1},\ldots,a_n)$.

Nash equilibrium and Pareto optimality are two vital definitions about the game. The general descriptions are also given below.

Definition 1 (Strict Nash equilibrium)**.** A strategy vector $\boldsymbol{a}$ in the game Γ is a *strict Nash equilibrium*, if for each player P_i and his any other strategy a_i' we have

$$u_i(a_i',\boldsymbol{a}_{-i})<u_i(\boldsymbol{a}). \tag{7}$$

Definition 2 (Pareto optimality)**.** A strategy vector $\boldsymbol{a}$ in the game Γ is a *Pareto optimality* if it is impossible to improve anyone's utility without reducing at least one other's. In other word, if $u_i(\boldsymbol{a}')>u_i(\boldsymbol{a})$, then there exists at least one player j which has $u_j(\boldsymbol{a}')<u_j(\boldsymbol{a})$.

In contrast, if $u_i(\boldsymbol{a}')\geqslant u_i(\boldsymbol{a})$ for each player P_i, and there exists at least one player j which has $u_j(\boldsymbol{a}')>u_j(\boldsymbol{a})$, we say $\boldsymbol{a}'$ is a Pareto improvement of $\boldsymbol{a}$.

Since only one agent can obtain the state in our protocol, the utility, correctness, and fairness of our protocol are different from general protocols. The details are given in Section 4.

3 Our new rational QSTS protocol

In this section, we propose a new rational QSTS protocol. The processes follow Li et al.'s [11]. There is also a boss (dealer) Alice and $n+1$ agents. The protocol contains r rounds. The processes Alice and Bob_i need to perform are described as follows.

Dealer's protocol

[D-1] The dealer (Alice) prepares an ordered list, which contains r bits. More specifically, only one bit is 1, and the others are 0, such as

$$\text{list} = \{\underbrace{0\ldots0}_{p}1\underbrace{0\ldots0}_{r-1-p}\}.$$

In the ith round, if $\text{list}_i = 1$, she goes to Step [D-2]. Otherwise, she goes to Step [D-2′].

[D-2] The dealer prepares two $(n+3)$-particle GHZ states (instead of $(n+2)$-particle states). The whole system is

$$\begin{aligned}|\Psi\rangle_S &\equiv |\Upsilon\rangle_{xy}\otimes|\Psi\rangle_{s_1}\otimes|\Psi\rangle_{s_2}\\ &= (a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle)_{xy}\\ &\quad\otimes\frac{1}{\sqrt{2}}\left(\prod_{i=1}^{n+3}|0\rangle_{a_i}+\prod_{i=1}^{n+3}|1\rangle_{a_i}\right)\otimes\frac{1}{\sqrt{2}}\left(\prod_{i=1}^{n+3}|0\rangle_{b_i}+\prod_{i=1}^{n+3}|1\rangle_{b_i}\right).\end{aligned}\tag{8}$$

Alice sends the particles a_i and b_i $(1\leqslant i\leqslant n+1)$ to the agent Bob_i.

[D-3] Then, the dealer takes the Bell basis measurement on the photons x and a_{n+3}, y and b_{n+3}, respectively. Following this, the state becomes

$$|\Psi\rangle_{\text{sub}} = \alpha\prod_{i=1}^{n+2}|00\rangle_{a_ib_i}+\beta\prod_{i=1}^{n+2}|01\rangle_{a_ib_i}+\gamma\prod_{i=1}^{n+2}|10\rangle_{a_ib_i}+\delta\prod_{i=1}^{n+2}|11\rangle_{a_ib_i}.\tag{9}$$

[D-4] Later, she asks all $n+1$ agents to perform X basis measurement. The measurement could be expressed as M'. Here, $M' = [(\langle+|)^{n+1-t}(\langle-|)^t]_a\otimes[(\langle+|)^{n+1-q}(\langle-|)^q]_b$. The collapsed state is

$$|\Psi\rangle_{a_{n+2}b_{n+2}} = (\alpha|00\rangle+(-1)^q\beta|01\rangle+(-1)^t\gamma|10\rangle+(-1)^{(q+t)}\delta|11\rangle)_{a_{n+2}b_{n+2}}.\tag{10}$$

We should note that the particles a_{n+2} and b_{n+2} are in the dealer's hand now. Then, she tells agents to publish the measurement results.

[D-5] She sends the particles $|\Psi\rangle_{a_{n+2}b_{n+2}}$ to the elected Bob_k (Charlie) via quantum teleportation [17, 18]. The game has ended for her.

[D-2′] The dealer shares two arbitrary Bell states with each agent. The whole system is

$$|\Psi'\rangle_S \equiv \prod_{i=1}^{n+1}|\Phi^{V_{i1}P_{i1}}\rangle_{a_ic_i}|\Phi^{V_{i2}P_{i2}}\rangle_{b_id_i},\tag{11}$$

where, she keeps the particles c_i and d_i, while P_i keeps a_i and b_i.

[D-3′] She asks all the agents to announce the measurement result as Step [D-4]. The dealer measures the particles in her hand, and analyzes the correlation between different results. She can judge whether these agents are cheating or not, and publish their ID. Then, she goes to the next round.

Agent's protocol

[A-1] In each round, all agents perform the X basis measurement on their received particles.

[A-2] They announce the result as the dealer's claim.

[A-3] If $\text{list}_i = 0$, some agents may be informed that they are forbidden to participate in the next λ $(\lambda < r)$ round because they are cheating in measurement results. The others will go to the next round.

Otherwise, they will randomly elect one of them to recover the state. Suppose the chosen one is Bob_k. He is also renamed as Charlie.

[A-4] Charlie recovers the state $|\Phi\rangle_{xy}$ by the local operations which are related with all the measurement results. The protocol is accomplished.

4 Analysis

4.1 Security

When we discuss the security of a QSTS protocol, there are two types of attack we need to consider: outside attack [19–21] and participants' attack [19, 21, 22]. Analysis shows that our protocol is safe.

4.1.1 *Outside attack*

Consider the faked states attack, time-shift attack, and detector blinding attack: extra equipment [23–25] could be utilized to resist these attacks. Since the transmission of particles is one-way, Trojan horse attacks, such as the invisible photons eavesdropping (IPE) Trojan horse attack and the delay-photon Trojan horse attack, are invalid.

In addition to the intercept-resend attack, measurement-resend attack, and entanglement-measure attack, decoy states could also play an important role. These attacks will be detected with a non-zero probability [26].

After all the agents announce the results, the operations to recover the state are evident. Thus, the player who receives the particles a_{n+2} and b_{n+2} can gain the state easily. Under these circumstances, all the outside attackers, even agents, will be incentivized to steal these particles. Fortunately, teleportation is the method to transmit them. Only Charlie can obtain the state.

4.1.2 *Participants' attack*

The analysis of the reduced matrix and collusion attack are the two branches of participants' attack in general.

(1) For any agent Bob_i, the reduced matrix may be a valuable tool to steal the information. The whole system after Alice's measurement is $|\Psi\rangle_{\mathrm{sub}}$. The reduced matrix of Bob_i's particle is

$$\rho_i = \mathrm{tr}_{-i}(|\Psi\rangle_{\mathrm{sub}}\langle\Psi|_{\mathrm{sub}}) = (|\alpha|^2|00\rangle\langle 00| + |\beta|^2|01\rangle\langle 01| + |\gamma|^2|10\rangle\langle 10| + |\delta|^2|11\rangle\langle 11|)_{a_i b_i}. \tag{12}$$

Since the set $\{\alpha, \beta, \gamma, \delta\}$ is the permutation of $\{\pm a, \pm b, \pm c, \pm d\}$, and a, b, c, d are unknown, Bob_i cannot obtain the details of them.

(2) Another considerable attack is the collusion attack for the multi-party protocol.

First, Charlie is more powerful than the other agents. He also has an incentive to gain the state without the help of any others, or only with the help of part of them.

Fortunately, the Pauli operations he needs to perform are related with $V_{xa_{n+2}}$, $V_{yb_{n+2}}$, P_a, and P_b. Here, P_a (P_b) is the product of $P_{xa_{n+2}}$ ($P_{yb_{n+2}}$) and all the agents' result P_{a_i} (P_{b_i}). Charlie cannot deduce whether P_a or $P_b = +/-$ without all the agents' help. In addition, the other possible attacks would be detected as an outside attack.

Second, several Bob_i may also want to obtain the state instead of Charlie. However, their classical bits will be published, they cannot do anything else without the particles a_{n+2} and b_{n+2}. Nonetheless, if they decide to steal these particles, they will also be detected as an outside attacker.

Third, if some agents want to analyze the reduced matrix, the result is similar to the single-agent case. Suppose that m agents are colluded, they are denoted as $G = \{i_1, i_2, i_3, \ldots, i_m\}$, $i_j \in \{1, \ldots, n+1\}$:

$$\begin{aligned}\rho_G &= \mathrm{tr}_{-G}(|\Psi\rangle_{\mathrm{sub}}\langle\Psi|_{\mathrm{sub}}) \\ &= |\alpha|^2 \prod_{j=1}^{m} |00\rangle\langle 00|_{a_{i_j} b_{i_j}} + |\beta|^2 \prod_{j=1}^{m} |01\rangle\langle 01|_{a_{i_j} b_{i_j}} \\ &\quad + |\gamma|^2 \prod_{j=1}^{m} |10\rangle\langle 10|_{a_{i_j} b_{i_j}} + |\delta|^2 \prod_{j=1}^{m} |11\rangle\langle 11|_{a_{i_j} b_{i_j}}.\end{aligned} \tag{13}$$

Agents in G also cannot deduce anything more. This attack is fruitless.

In summary, our protocol is safe from the above attacks.

Table 1 The detailed strategies, outcomes, and utilities

The value of list_i	Role	Strategy	Outcome	Explanation	Utility
0	Any agent	*Cooperating*	*Passed*	The agent passes the check.	U_g
0	Any agent	*Cheating*	*Failed*	The agent does not pass the check.	U_f
1	Bob_k	*Recovering*	*True state*	The agent Bob_k obtains the true state successfully.	U_s
1	Bob_k	*Recovering*	*False state*	The agent Bob_k obtains a false state.	U_e
1	Bob_i $(i{\neq}k)$	*Cheating*	*Threatening*	The agent Bob_i $(i{\neq}k)$ threatens that his results are wrong.	U_t
1	Bob_i $(i{\neq}k)$	*Cooperating*	*Successfully helping*	The agent Bob_i $(i{\neq}k)$ helps Bob_k obtain the state successfully.	U_{ps}
1	Bob_i $(i{\neq}k)$	*Cooperating*	*Unsuccessfully helping*	The agent Bob_i $(i{\neq}k)$ wants to help Bob_k, but Bob gets a false state since some-one else is threatening.	U_{pe}

Table 2 The strategies and utilities in a two-agent version

	Cheating	*Cooperating*
Cheating	(U_A, U_A)	(U_B, U_C)
Cooperating	(U_C, U_B)	(U_D, U_D)

4.2 Utilities

The utility of each agent P_i is defined by the corresponding outcomes of this game. They are shown in Table 1.

Some necessary explanations about the utilities are given here. (1) Apparently, U_f is the minimum in all the utilities. We can deduce that $U_f < U_g$. Further, in the ith round, if an agent does not pass the check, he will be forbidden from participating in the next λ round. The probability that he cannot participate in the sharing is $\frac{\lambda}{r-i}$. We have $U_f = -\frac{k\lambda}{r-i}$ $(k > 0)$ here. (2) Obtaining a false state is disadvantageous for an agent, hence $U_e < U_s$. (3) A cooperating Bob_i $(i \neq k)$ should not be responsible for other agents' cheating. In other words, when Bob_i chooses to cooperate, his utility will not be affected by other Bob_j $(j \neq k)$, i.e., $U_{ps} = U_{pe}$. (4) All the Bob_i cannot obtain the state, but they are needed to help Charlie in the protocol. In this situation, Charlie may pay to Bob_i to make $U_{ps} + \varepsilon \leqslant U_s$. Here, ε is a negligible value. (5) The motivation for Bob_i's cheating is that he gains more by cooperating with than by threatening Charlie. It is easy to obtain that $U_t > U_{ps} = U_{pe}$. (6) For simplicity's sake, we suppose that only U_f is proportional to $\frac{\lambda}{r-i}$. The other utilities are independent with λ and $r - i$.

Next, we describe the utility of agents when they choose the strategy *Cheating* or *Cooperating* in a two-agent version as an example (Table 2).

Here,

$$\begin{aligned}
U_A &= \frac{r-i}{r-i+1}U_f + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_t + \frac{1}{n+1}U_e\right),\\
U_B &= \frac{r-i}{r-i+1}U_f + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_t + \frac{1}{n+1}U_s\right),\\
U_C &= \frac{r-i}{r-i+1}U_g + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_{pe} + \frac{1}{n+1}U_e\right),\\
U_D &= \frac{r-i}{r-i+1}U_g + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_{ps} + \frac{1}{n+1}U_s\right).
\end{aligned} \tag{14}$$

Since the election occurs after the publication of measurement results, all the agents need to choose whether to cheat or cooperate when publishing. The computational process used to obtain U_A, U_B, U_C,

and U_D for the ith round is

$$\begin{aligned}U_A =& \Pr[\text{list}_i = 0] \cdot \{\Pr[\text{passes the check}] \cdot U_g + \Pr[\text{does not pass the check}] \cdot U_f\} \\ &+ \Pr[\text{list}_i = 1] \cdot \{\Pr[\text{is not chosen as Charlie}] \cdot U_t + \Pr[\text{is chosen as Charlie}] \cdot U_e\} \\ =& \frac{r-i}{r-i+1}(0 \cdot U_g + 1 \cdot U_f) + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_t + \frac{1}{n+1}U_e\right) \\ =& \frac{r-i}{r-i+1}U_f + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_t + \frac{1}{n+1}U_e\right), \end{aligned} \tag{15}$$

$$\begin{aligned}U_B =& \Pr[\text{list}_i = 0] \cdot \{\Pr[\text{passes the check}] \cdot U_g + \Pr[\text{does not pass the check }] \cdot U_f\} \\ &+ \Pr[\text{list}_i = 1] \cdot \{\Pr[\text{is not chosen as Charlie}] \cdot U_t + \Pr[\text{is chosen as Charlie}] \cdot U_s\} \\ =& \frac{r-i}{r-i+1}(0 \cdot U_g + 1 \cdot U_f) + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_t + \frac{1}{n+1}U_s\right) \\ =& \frac{r-i}{r-i+1}U_f + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_t + \frac{1}{n+1}U_s\right), \end{aligned} \tag{16}$$

$$\begin{aligned}U_C =& \Pr[\text{list}_i = 0] \cdot \{\Pr[\text{passes the check}] \cdot U_g + \Pr[\text{does not pass the check }] \cdot U_f\} \\ &+ \Pr[\text{list}_i = 1] \cdot \{\Pr[\text{is not chosen as Charlie}] \cdot U_{pe} + \Pr[\text{is chosen as Charlie}] \cdot U_e\} \\ =& \frac{r-i}{r-i+1}(1 \cdot U_g + 0 \cdot U_f) + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_{pe} + \frac{1}{n+1}U_e\right) \\ =& \frac{r-i}{r-i+1}U_g + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_{pe} + \frac{1}{n+1}U_e\right), \end{aligned} \tag{17}$$

$$\begin{aligned}U_D =& \Pr[\text{list}_i = 0] \cdot \{\Pr[\text{passes the check}] \cdot U_g + \Pr[\text{does not pass the check}] \cdot U_f\} \\ &+ \Pr[\text{list}_i = 1] \cdot \{\Pr[\text{is not chosen as Charlie}] \cdot U_{ps} + \Pr[\text{is chosen as Charlie}] \cdot U_s\} \\ =& \frac{r-i}{r-i+1}(1 \cdot U_g + 0 \cdot U_f) + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_{ps} + \frac{1}{n+1}U_s\right) \\ =& \frac{r-i}{r-i+1}U_g + \frac{1}{r-i+1}\left(\frac{n}{n+1}U_{ps} + \frac{1}{n+1}U_s\right). \end{aligned} \tag{18}$$

If the noise is not considered, the probability that a cheating Bob_i passes the check is zero. In contrast, the probability that a cooperating Bob_i passes the check is one. Another point we need to explain is, before the ith round, agents have played the game for $i-1$ rounds, in which all $\text{list}_j = 0$ $(1 \leqslant j \leqslant i-1)$. Hence, $\Pr[\text{list}_i = 1] = \frac{1}{r-(i-1)} = \frac{1}{r-i+1}$.

4.3 Correctness

Definition 3 (Correctness)**.** A rational QSTS game Γ is called *correct* if for each Bob_i's arbitrary strategy $a_i \in \{Cooperating, Cheating\}$, the following holds

$$\Pr[\boldsymbol{o}_k(\Gamma, (a_i, \boldsymbol{a}_{-i})) = False\ state\ ] \leqslant \varepsilon, \tag{19}$$

where ε is a negligible value.

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

Proof. Bob_k (Charlie) needs the results announced by Bob_i to recover the state $|\Upsilon\rangle_{xy}$. Fortunately, Bob_i does not have incentive to make Charlie gain a false state. Since each agent is rational, his purpose is to benefit more. Although he may announce a false result at first, he will no longer cheat after getting more from Charlie. In addition, $\text{list}_i = 0$ in most cases, so Bob_i is less likely to cheat.

Therefore, the protocol is correct.

4.4 Fairness

In general, the fairness of a protocol means that all the players can obtain the value of the multi-party computation function [27]. However, only one player can obtain the state in our protocol, but he will pay the others for his assistance.

The fairness of our protocol or game is defined as follows.

Definition 4 (Fairness)**.** A rational QSTS game Γ is called $fair$ if it satisfies the following conditions.

(1) If we treat the election in Subsection 2.1 as a sub-game Γ', the strategies of players are publishing 1 or 0 in each round. Then, for any strategy the player Bob_j $(1 \leqslant j \leqslant n)$ chooses, the following holds

$$\Pr[\boldsymbol{o}_j(\Gamma', (a_j, \boldsymbol{a}_{-j})) = \text{ Charlie}] \leqslant \Pr[\boldsymbol{o}_{-j}(\Gamma', (a_j, \boldsymbol{a}_{-j})) = \text{ Charlie}]. \tag{20}$$

(2) For any Bob_i $(1 \leqslant i \leqslant n)$ and any strategy he chooses, if he is elected as Charlie, compared with the situation that any other Bob_j $(j \neq i)$ is elected as Charlie, the following holds

$$\Pr[\boldsymbol{o}_i(\Gamma, (a_i, \boldsymbol{a}_{-i})) = True \ \ state] \leqslant \Pr[\boldsymbol{o}_j(\Gamma, (a_i, \boldsymbol{a}_{-i})) = True \ \ state]. \tag{21}$$

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

Proof. (1) The values of all the c_j are random, which means that the entropy of c_j is $H(c_j) = 1$. Since $C = \bigoplus_{j=1}^{N} c_j$, we also know that $H(C) = 1$. Obviously, each player has the same influence on the value of C.

More importantly, even if $N-1$ players colluded except for P_k, the value of C is still unknown and completely random for them. Suppose that the addition module 2 of their bits are C_{-k}. It is easy to obtain that the conditional entropy $H(C|C_{-k}) = 1$.

In this case, the probability of each player being chosen as Charlie is equal. The sub-game Γ' is certainly fair.

(2) If the utility of strategy *Cheating* is less than that of *Cooperating*, the player will have no incentive to cheat. He will always cooperate with the others and publish his measurement results faithfully. Since all the players will cooperate with each other, the fairness is achieved.

Here, we can say $U_{Cheating} < U_{Cooperating}$ if $U_A < U_C$ and $U_B < U_D$ hold simultaneously, i.e., no matter what strategy the other player chooses, each tends to cooperate. The conditions of $U_A < U_C$ and $U_B < U_D$ are discussed below:

$$\begin{aligned} U_A - U_C &= \frac{r-i}{r-i+1}(U_f - U_g) + \frac{1}{r-i+1}\frac{n}{n+1}(U_t - U_{pe}) \\ &= \frac{1}{r-i+1}\left[(r-i)(U_f - U_g) + \frac{n}{n+1}(U_t - U_{pe})\right] \\ &= \frac{1}{r-i+1}\left[(r-i)\left(-\frac{k\lambda}{r-i} - U_g\right) + \frac{n}{n+1}(U_t - U_{pe})\right] \\ &= \frac{1}{r-i+1}\left[-k\lambda - (r-i)U_g + \frac{n}{n+1}(U_t - U_{pe})\right]. \end{aligned} \tag{22}$$

We know that $U_f - U_g < 0$ and $U_t - U_{pe} > 0$. If λ or $r-i$ is large enough, then $U_A < U_C$. The dealer can increase the number of forbidden rounds λ or the number of total rounds r to ensure that

$$\begin{aligned} U_B - U_D &= \frac{r-i}{r-i+1}(U_f - U_g) + \frac{1}{r-i+1}\frac{n}{n+1}(U_t - U_{ps}) \\ &= \frac{1}{r-i+1}\left[(r-i)(U_f - U_g) + \frac{n}{n+1}(U_t - U_{ps})\right] \\ &= \frac{1}{r-i+1}\left[-k\lambda - (r-i)U_g + \frac{n}{n+1}(U_t - U_{ps})\right]. \end{aligned} \tag{23}$$

Since $U_{pe} = U_{ps}$, the condition that ensures $U_B < U_D$ is the same as ensuring $U_A < U_C$.

Thus, we have shown how to ensure the fairness of our protocol.

4.5 Strict Nash equilibrium

Theorem 3. There exist some values of r and λ that make the protocol achieve strict Nash equilibrium.

Proof. As the designer of a protocol, our aim is for the strategy vector (*Cooperating*, *Cooperating*) to be a strict Nash equilibrium of this game. The corresponding utilities are (U_D, U_D) in this case.

In this game, if $U_A < U_C$ and $U_B < U_D$ hold at the same time, we have $u_1(Cheating, a_2) < u_1(Cooperating, a_2)$ and $u_2(a_1, Cheating) < u_2(a_1, Cooperating)$ for Bob$_i$'s any given strategy $a_i \in \{Cooperating, Cheating\}$. The agent will choose to cooperate regardless of which strategy the others adopt.

Conditions are the same as in Subsection 4.4. The strict Nash equilibrium of our protocol is also ensured.

4.6 Pareto optimality

Theorem 4. There exist some values of r and λ that make the protocol achieve Pareto optimality.

Proof. Reviewing Table 2, in the following we describe the condition of how to make strategy vector (*Cooperating*, *Cooperating*) Pareto optimal.

Since we know that $U_B < U_D$, the strategy vector (*Cooperating*, *Cheating*) and (*Cheating*, *Cooperating*) cannot be the Pareto improvement of $(Cooperating, Cooperating)$. The only possible vector is (*Cheating*, *Cheating*). In other words, if $U_A < U_D$, the strategy vector $(Cooperating, Cooperating)$ will be Pareto optimal.

$$\begin{aligned} U_A - U_D &= \frac{r-i}{r-i+1}(U_f - U_g) + \frac{1}{r-i+1}\left[\frac{n}{n+1}(U_t - U_{ps}) + \frac{1}{n+1}(U_e - U_s)\right] \\ &= \frac{1}{r-i+1}\left[(r-i)(U_f - U_g) + \frac{n}{n+1}(U_t - U_{ps}) + \frac{1}{n+1}(U_e - U_s)\right] \\ &= U_B - U_D + \frac{1}{r-i+1}\frac{n}{n+1}(U_e - U_s). \end{aligned} \tag{24}$$

Since $U_e < U_s$ and $U_B < U_D$, we naturally have $U_A < U_D$.

In conclusion, there exist some appropriate r and λ which make the strategy vector (*Cooperating*, *Cooperating*) Pareto optimal. This vector is also the Nash equilibrium. Hence, we say that agents are all-win in this game.

5 Discussion

Here, we discuss our protocol and the future work we need to do.

First, and most importantly, we assume that the dealer Alice does not know the secret state, while Maitra et al.'s [15] does know. In fact, if the dealer knows the state, on the one hand, it is more like an RSP protocol instead of QSTS. On the other hand, she can also share classical information about the state with agents. Thus, agents can prepare the state by themselves. Sharing of the quantum state is not necessary. From this aspect, our assumption is more practical and reasonable. Furthermore, this assumption is the same with most of the QSTS protocol [6, 8–12].

Second, in [15], the dealer could be semi-offline or offline. An offline dealer only needs to distribute particles at the beginning. A semi-offline dealer also needs to interact with agents when the game is over [15]. Maitra et al. [15] considered these two kinds of cases successively. In contrast, the dealer in our protocol is online, so she needs to interact with all the agents in the processes. If the dealer is semi-offline or offline, she only does a little in the protocol. The protocol will be more dealer-free. This gives us a direction for our future work, i.e., how to design a rational QSTS protocol with a semi-offline or offline dealer.

Third, we suppose that the agent Charlie can only choose to recover the secret state in this paper. Charlie will bargain with cheating agents to agree a suitable price for the real measurement results. This

is called a Rubinstein bargain model [28]. In fact, refusing is another strategy. He may also refuse to recover the state when the cheating agents ask too much. If he refuses, he will get nothing, as well all the other agents. In the future, a different model, such as the ultimatum game model [29] or finite bargain model [30], can be considered.

Last, but not least, the processes of our protocol is drawn from [11]. Li et al. [11] also generalized their scheme to share an arbitrary multi-particle state. Our protocol also has the multi-particle counterpart naturally. In addition, numerous QSTS schemes have been proposed in recent years [12, 13]. A rational protocol that is learned from other QSTS schemes, or independently designed, should also be studied. Further, rational protocols are mainly aimed at the SS problem. With the development of computer science and the corresponding applications [31–36], the security of data has been attracting a lot of attention. The other branches of secure multi-party computation, such as the multi-party summation problem [37] and private comparison problem [38], can also be investigated.

6 Conclusion

In this paper, we have proposed a novel rational QSTS protocol based on [11, 15]. Assumptions about our protocol are more reasonable than Maitra et al.'s [15]. Concretely, on the one hand, the dealer does not know the information about the quantum state. On the other hand, all the agents are in a Byzantine setting. At the same time, players in our protocol are also rational. The agents choose to follow or deviate from the process depending on which choice can maximize their benefit. The security, correctness, fairness, the existence of Nash equilibrium, and Pareto optimality were each analyzed in turn. Our protocol is a standard and safe rational QSTS protocol.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61671087, 61272514, 61170272), National Development Foundation for Cryptological Research (Grant No. MMJJ201401012), Fok Ying Tung Education Foundation (Grant No. 131067), Natural Science Foundation of Inner Mongolia (Grant No. 2017MS0602), University Scientific Research Project of Inner Mongolia (Grant No. NJZY17164), and Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2017BDKFJJ007).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Shamir A. How to share a secret. Commun ACM, 1979, 22: 612–613
2 Blakley G R. Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference 1979, New York, 1979. 313–317
3 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
4 Mayers D. Unconditional security in quantum cryptography. J ACM, 2001, 48: 351–406
5 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829
6 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648
7 Wootters W K, Zurek W H. A single quantum cannot be cloned. Nature, 1982, 299: 802–803
8 Li Y, Zhang K, Peng K. Multiparty secret sharing of quantum information based on entanglement swapping. Phys Lett A, 2004, 324: 420–424
9 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. Phys Rev Lett, 2004, 92: 177903
10 Deng F G, Li C Y, Li Y S, et al. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 022338
11 Li X H, Zhou P, Li C Y, et al. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J Phys B-At Mol Opt, 2006, 39: 1975
12 Muralidharan S, Panigrahi P K. Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. Phys Rev A, 2008, 77: 032321
13 Li D, Wang R, Zhang F, et al. Quantum information splitting of arbitrary two-qubit state by using four-qubit cluster state and Bell-state. Quantum Inf Proc, 2015, 14: 1103–1116
14 Halpern J, Teague V. Rational secret sharing and multiparty computation. In: Proceedings of the 36th Annual ACM Symposium on Theory of Computing, New York, 2004. 623–632

15 Maitra A, Joyee de S, Paul G, et al. Proposal for quantum rational secret sharing. Phys Rev A, 2015, 92: 022305
16 Stefanov A, Gisin N, Guinnard O, et al. Optical quantum random number generator. J Mod Opt, 2000, 47: 595–598
17 Rigolin G. Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement. Phys Rev A, 2005, 71: 032303
18 Zha X W, Song H Y. Non-Bell-pair quantum channel for teleporting an arbitrary two-qubit state. Phys Lett A, 2007, 369: 377–379
19 Li Y B, Wang T Y, Chen H Y, et al. Fault-tolerate quantum private comparison based on GHZ states and ECC. Int J Theor Phys, 2013, 52: 2818–2825
20 Li Y B. Analysis of counterfactual quantum key distribution using error-correcting theory. Quantum Inf Proc, 2014, 13: 2325–2342
21 Li Y B, Qin S J, Yuan Z, et al. Quantum private comparison against decoherence noise. Quantum Inf Proc, 2013, 12: 2191–2205
22 Li Y B, Wen Q Y, Gao F, et al. Information leak in Liu et al.'s quantum private comparison and a new protocol. Eur Phys J D, 2012, 66: 1–6
23 Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. Phys Rev A, 2006, 74: 022313
24 Jain N, Stiller B, Khan I, et al. Attacks on practical quantum key distribution systems (and how to prevent them). Contemp Phys, 2016, 5: 51–61
25 Qi B, Fung C H F, Lo H K, et al. Time-shift attack in practical quantum cryptosystems. Quantum Inf Comput, 2007, 7: 73–82
26 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441
27 Groce A, Katz J. Fair computation with rational players. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012. 81–98
28 Rubinstein A. Perfect equilibrium in a bargaining model. Econometrica, 1982, 50: 97–109
29 Thaler R H. Anomalies: the ultimatum game. J Econ Perspect, 1988, 2: 195–206
30 Ståhl I. Bargaining Theory. Stockholm: Stockholm School of Economics, 1972
31 Xia Z, Wang X, Sun X, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans Parall Distr, 2016, 27: 340–352
32 Fu Z, Ren K, Shu J, et al. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans Parall Distr, 2016, 27: 2546–2559
33 Chen Y D, Hao C Y, Wu W, et al. Robust dense reconstruction by range merging based on confidence estimation. Sci China Inf Sci, 2016, 59: 092103
34 Shen J, Shen J, Chen X F, et al. An efficient public auditing protocol with novel dynamic structure for cloud data. IEEE Trans Inf Forensics Secur, 2017, 12: 2402–2415
35 Fu Z, Wu X, Guan C, et al. Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement. IEEE Trans Inf Foren Sec, 2016, 11: 2706–2716
36 Fu Z, Sun X, Ji S, et al. Towards efficient content-aware search over encrypted outsourced data in cloud. In: Proceedings of the 35th Annual IEEE International on Conference Computer Communications, San Francisco, 2016. 1–9
37 Chen X B, Xu G, Yang Y X, et al. An efficient protocol for the secure multi-party quantum summation. Int J Theor Phys, 2010, 49: 2793–2804
38 Chen X B, Xu G, Niu X X, et al. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt Commun, 2010, 283: 1561–1565