Rational quantum secret sharing

Qin, Huawang; Tang, Wallace K. S.; Tso, Raylin

Published in:
Scientific Reports

Published: 01/01/2018

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.1038/s41598-018-29051-z

Publication details:
Qin, H., Tang, W. K. S., & Tso, R. (2018). Rational quantum secret sharing. *Scientific Reports*, *8*, [11115]. https://doi.org/10.1038/s41598-018-29051-z

SCIENTIFIC REPORTS

OPEN

Rational quantum secret sharing

Huawang Qin[1], Wallace K. S. Tang[2] & Raylin Tso[3]

Received: 22 January 2018
Accepted: 4 July 2018
Published online: 24 July 2018

The traditional quantum secret sharing does not succeed in the presence of rational participants. A rational participant's motivation is to maximize his utility, and will try to get the secret alone. Therefore, in the reconstruction, no rational participant will send his share to others. To tackle with this problem, we propose a rational quantum secret sharing scheme in this paper. We adopt the game theory to analyze the behavior of rational participants and design a protocol to prevent them from deviating from the protocol. As proved, the rational participants can gain their maximal utilities when they perform the protocol faithfully, and the Nash equilibrium of the protocol is achieved. Compared to the traditional quantum secret sharing schemes, our scheme is fairer and more robust in practice.

"Secret sharing" (SS) was first proposed by Shamir[1], suggesting a secure way to distribute information (secret) to a set of participants. SS splits the secret into several parts and distributes them to different participants, so that only qualified participants can recover the original secret. In Shamir's scheme, a participant is classified as "good" or "bad". A good participant always performs the protocol faithfully, while the bad one would try his best to break it. However, this kind of classification may not reflect practical situations. Indeed, a participant can be neither good nor bad, but rational and always try to maximize his utility. Hence, each rational participant aims to get the secret, but at the same time, prevents others to get it.

The involvement of rational participants leads to a major problem in SS. In SS, a participant can recover the secret alone even not sending his share to others, if others have sent out theirs. On the other hand, if participants did not send their shares, none can recover the secret. Therefore, from the viewpoint of a rational participant, not sending his share weakly dominates sending his share. This implies the Nash equilibrium corresponds to the case that nobody sends his share to others, resulting in a failure of Shamir's scheme in the presence of rational participants.

To mitigate this problem, Halpern *et al.*[2] introduced the concept of "rational secret sharing" (RSS), and it has become an active area of research in recent years[3–5]. In classical RSS, signed share is used to prevent cheating of participants, while another approach is to use verifiable secret sharing[6].

On the other hand, Hillery *et al.*[7] have proposed "Quantum secret sharing" (QSS), which can be considered as an extension of Shamir's SS into the area of quantum. In QSS, the secret is split, distributed and reconstructed by quantum operations. QSS provides more perfect security based on the quantum theory such as uncertainty principle and no-cloning theorem. Similar to SS schemes, the existing QSS schemes[8–21] do not consider the rational behavior of participants. However, it is natural for the last participant, if he is rational, to generate the secret and quit with it alone. Thus, rational participants in QSS would always prefer not to provide their shares, making the conventional QSS schemes fail.

It should be emphasized those approaches suggested in RSS, such as signed share or verifiable SS, are based on unproven assumptions such as the intractability of integer factorization. In the quantum domain, participants and adversaries are always assumed to have unbounded computational power. As a result, these methods are inadequate for the design of rational quantum secret sharing (RQSS). In addition, there are other technical hurdles to be overcome for the design of RQSS, for example, the existing quantum signature schemes[22,23] fail to deal with the entanglement among distributed shares, and a participant cannot generate copies of his share due to the no-cloning theorem.

Designing a workable RQSS is challenging but valuable, and it is also the main objective of this paper. In our proposal, the shared secret is assumed to be a d-dimensional quantum state. Some basic quantum operations, such as the quantum Fourier transform and quantum-controlled-not, are employed. Unlike our previous work[24] and other QSS schemes, here the issue of "rationality" is focused. Game theory is introduced to analyze the rational behavior of participants, based on the concepts of rationality, fairness and Nash equilibrium. As with most of the QSS schemes[7–12], the threshold structure of our scheme is (n, n) structure, meaning that all the n participants compose the only qualified set and any subset with fewer than n participants is a forbidden set. Our

[1]School of Automatization, Nanjing University of Science and Technology, Nanjing, 210094, China. [2]Department of Electronic Engineering, City University of Hong Kong, Kowloon Tong, Hong Kong. [3]Department of Computer Science, National Chengchi University, Taipei, 11605, Taiwan. Correspondence and requests for materials should be addressed to H.Q. (email: qin_h_w@163.com)

design can avoid rational participants to deviate from the protocol since an unfaithful act will not gain higher utility than a faithful one. As a result, the achieved Nash equilibrium corresponds to the case when all the rational participants perform the protocol faithfully, and eventually, the shared quantum state can be recovered with the involvement of all participants.

The rest of this paper is organized as follows. In Section 2, some correlative preliminaries are introduced. Section 3 describes the design of RQSS in details, while an example is provided in Section 4 to better illustrate the protocol. Section 5 proves the security of the proposal and Section 6 analyzes its Nash equilibrium. Section 7 compares the proposed scheme with our previous work. Finally, Section 8 concludes this paper.

Preliminaries

The preliminaries of underlying QSS have been introduced adequately in other existing schemes, and hence only the preliminaries of rational part are focused. They are formalized in terms of rationality, fairness and Nash equilibrium, while quantum operations to be used in this work are also introduced.

Rationality. The rationality of RQSS is specified by the following conditions. Considering two different strategies a and a',

- if $O_i(a) = 1$ and $O_i(a') = 0$, then $u_i(a) > u_i(a')$;
- if $O_i(a) = O_i(a')$ and $O_j(a') < O_j(a)$, then $u_i(a) > u_i(a')$.

$O_i(\cdot)$ is a binary function and $u_i(\cdot)$ is utility function of P_i. $O_i(a) = 1$ indicates that the participant P_i can recover the secret by applying strategy a, and $O_i(\cdot) = 0$ means that he can't.

Fairness. The fairness of RQSS is specified by the following conditions. Letting a_i^* be the suggested strategy of the protocol and a_i be other possible strategy for participant P_i,

- $u_1(a_1^*) = u_2(a_2^*) = \cdots = u_n(a_n^*)$;
- $u_i(a_i^*) > u_j(a_j)$.

Nash equilibrium. A RQSS protocol should achieve the Nash equilibrium such that no participant has any incentive to deviate from the protocol. A suggested strategy is said to be in Nash equilibrium when there is no incentive for any participant to deviate from it, given that everyone else is following this strategy. Formally, it can be described as follows.

For an arbitrary participant P_i, if $u_i(a_i^* | \underline{a}_{-i}^*) > u_i(a_i | \underline{a}_{-i}^*)$, then the strategy group $a^* = (a_1^*, a_2^*, \cdots, a_n^*)$ is the Nash equilibrium. Here, a_i^* and $\underline{a}_{-i}^* = (a_1^*, \cdots, a_{i-1}^*, a_{i+1}^*, \cdots, a_n^*)$ are the suggested strategy for participant P_i and all other participants, respectively; and $u_i(\cdot | \underline{a}_{-i}^*)$ represents P_i's utility given that all other P_j $(j \neq i)$ follow the suggested strategy.

Quantum operations. *Quantum Fourier transform.* For a d-dimensional quantum state $|j\rangle$, $j \in \{0, 1, \ldots, d-1\}$, the quantum Fourier transform is defined as

$$F(|j\rangle) = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle \tag{1}$$

where $\omega = e^{\frac{2\pi i}{d}}$. The corresponding quantum inverse Fourier transform is then given by

$$F^{-1}(|j\rangle) = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{-kj} |k\rangle \tag{2}$$

d-dimensional quantum-controlled-not. Consider two d-dimensional quantum states $|j_1\rangle$ and $|j_2\rangle$, the d-dimensional quantum-controlled-not operation is expressed by:

$$\mathrm{CNOT}(|j_1\rangle, |j_2\rangle) = (|j_1\rangle, |j_1 + j_2\rangle) \tag{3}$$

where $|j_1\rangle$ and $|j_2\rangle$ are referred as the control particle and target particle, respectively; and "+" is defined as the adder modulo d hereinafter.

Design of RQSS

In RQSS, similar to other SS or RSS, there is a dealer who would like to distribute a secret to a set of participants. However, there are some district features in RQSS.

Random structure. The dealer needs multiple rounds to distribute the shared secret to the participants. In each round, the dealer distributes the real secret (the shared secret) with a probability of γ, otherwise, a test secret is sent. Participants can only know whether the reconstructed secret is a real one or not after the dealer reveals the truth.

Post verification. Dishonest participant should be punished and hence the behavior of participants must be verified. However, the methods employed in classical RSS are inadequate for RQSS due to the unbounded computational power in quantum domain. Therefore, quantum operations are to be applied.

Generation of multiple same quantum states. In QSS, when the share is an unknown state, a participant cannot generate copies of his share due to the no-cloning theorem. If only one share is kept by a participant, only one secret can be reconstructed. Consequently, the participant who holds the reconstructed secret will have the privilege, breaking the fairness of RQSS. In order to resolve this problem, the dealer has to generate multiple same states and distribute to the participants, allowing all the qualified participants to get the reconstructed secret.

Parameters setting based on Nash equilibrium. The parameters of RQSS should be properly set to guarantee that each honest participant can gain his maximal utility under the suggested strategy. The Nash equilibrium is to be achieved to ensure that the protocol can be performed robustly in the presence of rational participants.

The details of the RQSS protocol are given as follows. For the sake of clarity, the dealer and the n rational participants are referred as Alice and $\{\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n\}$, respectively. The shared secret is assumed to be a d-dimensional quantum state, defined as $\varphi = \sum_{j=0}^{d-1}\alpha_j|j\rangle$, where α_j are complex amplitudes and $\sum_{j=0}^{d-1}\left|\alpha_j\right|^2 = 1$.

To share φ among the n rational participants, Alice performs the following procedures for each round.

(1) A specific coin having a probability of γ to be "1" (head) is tossed. If it is "1", Alice generates n same real quantum states; otherwise, she generates n same test quantum states. For convenience, every one of these n quantum states is denoted as φ.
(2) For each φ, the quantum inverse Fourier transform is applied to obtain φ'. For each φ', Alice generates $(n-1)$ single particles, $p_i = |d-1\rangle$ where $i = 1, 2, \ldots, (n-1)$, and then performs d-dimensional quantum-controlled-not operation onto φ' and each p_i in turns, where φ' and p_i are the control particle and the target particle, respectively. An n-particle entangled state Φ is then resulted. Finally, Alice performs the quantum Fourier transform on each particle of Φ to obtain Φ'.
(3) For every Φ', Alice sends one particle of Φ' to one participant sequentially. The particles transmission is protected by decoy particles, which are randomly selected from two bases, namely the Z-basis and the X-basis, as given in the following forms:

$$Z = \{|j\rangle, j = 0, 1, \ldots, d-1\}$$

and

$$X = \{|J_j\rangle, j = 0, 1, \ldots, d-1\}$$

where

$$|J_j\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}\,|k\rangle$$

(4) For reconstruction, all the particles of one Φ' will be sent to one of the participants, and eventually everyone will get one Φ'. The participant will perform the quantum inverse Fourier transform on every particle of his own Φ' and get back Φ. By performing d-dimensional quantum-controlled-not operations, the quantum state φ' and the $(n-1)$ single particles $\{p_1, p_2, \ldots, p_{n-1}\}$ can be separated from Φ. Then the original state φ can be obtained by applying quantum Fourier transform onto φ'. For an arbitrary participant Bob_i, the particles $\{p_1, p_2, \ldots, p_{n-1}\}$ come from other $(n-1)$ participants. If other participants perform the protocol faithfully, then the obtained particles $\{p_1, p_2, \ldots, p_{n-1}\}$ should all be in the state $|d-1\rangle$. Therefore, by measuring these particles, Bob_i can deduce whether the corresponding participant has sent the correct particle or not. However, it should also be remarked that, there is still a probability of $\frac{1}{d}$ that Bob_i will get the correct measurement result even if the received particle is incorrect.
(5) If a participant Bob_i finds that he did not receive any particle from Bob_j or the particle is not a correct one, Bob_i will publicize the cheating behavior of Bob_j. Other participants will then terminate the protocol. When the protocol is terminated by any of the participants, the dealer will not continue the next round. As a result, participants will not be able to get the secret if the current round is not the real one.
(6) If no cheating behavior is found, the dealer will reveal whether the secret in this round is the real secret or a test one. If it is the real secret, the protocol will be over. Otherwise, the dealer will start the next round.

Example

To better illustrate the RQSS protocol, we consider a simple case with a dealer sharing a 3-dimensional quantum state to three participants.

In each round, Alice firstly decides to distribute the real secret or a test secret, φ, according to the result of coin tossing. Three same quantum states are then generated, each specified by $\varphi = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$. By performing the quantum inverse Fourier transform as given in (2), Alice obtains

$$\varphi' = \frac{1}{\sqrt{3}}[(\alpha_0 + \alpha_1 + \alpha_2)|0\rangle + (\alpha_0 + \omega^2\alpha_1 + \omega\alpha_2)|1\rangle + (\alpha_0 + \omega\alpha_1 + \omega^2\alpha_2)|2\rangle] \tag{4}$$

Following the protocol, Alice generates two single particles, i.e. $\{p_1 = |2\rangle, p_2 = |2\rangle\}$. By applying 3-dimensional quantum-controlled-not operations onto φ' and each p_i in turns, it results in the following quantum state

$$\Phi = \frac{1}{\sqrt{3}}[(\alpha_0 + \alpha_1 + \alpha_2)|022\rangle + (\alpha_0 + \omega^2\alpha_1 + \omega\alpha_2)|100\rangle + (\alpha_0 + \omega\alpha_1 + \omega^2\alpha_2)|211\rangle] \tag{5}$$

The quantum Fourier transform is then performed for each particle of Φ and finally Alice obtains

$$\begin{aligned}\Phi' \;=\; & \frac{1}{3}(\alpha_0|000\rangle + \omega^2\alpha_1|001\rangle + \omega\alpha_2|002\rangle + \omega^2\alpha_1|010\rangle + \omega\alpha_2|011\rangle + \alpha_0|012\rangle \\ & + wa_2|020\rangle + a_0|021\rangle + w^2a_1|022\rangle + a_1|100\rangle + w^2a_2|101\rangle + wa_0|102\rangle \\ & + w^2a_2|110\rangle + wa_0|111\rangle + a_1|112\rangle + wa_0|120\rangle + a_1|121\rangle + w^2a_2|122\rangle \\ & + a_2|200\rangle + w^2a_0|201\rangle + wa_1|202\rangle + w^2a_0|210\rangle + wa_1|211\rangle + a_2|212\rangle \\ & + wa_1|220\rangle + a_2|221\rangle + w^2a_0|222\rangle)\end{aligned} \tag{6}$$

Based on the above operations, Alice will get three same entangled states and for simplicity, each one of them is denoted as Φ'. The three particles of each Φ' will be sent to Bob_1, Bob_2 and Bob_3, respectively. Consequently, each participant will have three particles which belong to one of the three entangled states.

In the reconstruction, the three particles of one Φ' will be sent to one participant, and every participant will get one Φ'. When Φ' is available, Bob_i will recover the original state φ by following Step (4) of the procedures as described in the last section. First, he gets back Φ by applying the quantum inverse Fourier transform on every particle of his Φ'. Then, two quantum-controlled-not operations are performed to separate the state φ' and two single particles $\{p_1, p_2\}$ from Φ. Finally, the original state $\varphi = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$ is obtained by applying the quantum Fourier transform onto φ'. Bob_i can verify the honesty of other two participants by measuring $\{p_1, p_2\}$. If they sent Bob_i the correct particles, $\{p_1, p_2\}$ should both be in the state $|2\rangle$.

If all the participants are honest, Alice will reveal whether the secret is a real one or not. If it is the real secret, the protocol will be over and all the participants obtain the secret. Otherwise, Alice will start again for the next round.

Security analysis

In this section, the security of the proposed RQSS protocol is analyzed.

Confidentiality. Given that the initial state Alice generated is $\varphi = \sum_{j=0}^{d-1}\alpha_j|j\rangle$, by applying the quantum inverse Fourier transform onto φ, one has

$$\varphi' = \sum_{j=0}^{d-1}\alpha_j\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{-kj}|k\rangle\right) = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\left(\sum_{j=0}^{d-1}\alpha_j\omega^{-kj}|k\rangle\right) \tag{7}$$

Then, with the $(n-1)$ quantum-controlled-not operations, Φ is obtained as follows

$$\Phi = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\left(\sum_{j=0}^{d-1}\alpha_j\omega^{-kj}|k\overbrace{(k+d-1),\ \cdots,\ (k+d-1)}^{n-1}\rangle\right) \tag{8}$$

Finally, after the n quantum Fourier transforms, one obtains

$$\begin{aligned}\Phi' \;=\; & \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\left\{\sum_{j=0}^{d-1}\alpha_j\omega^{-kj}\left[\left(\frac{1}{\sqrt{d}}\sum_{k_1=0}^{d-1}\omega^{k_1k}|k_1\rangle\right)\right.\right. \\ & \left.\left.\times\left(\frac{1}{\sqrt{d}}\sum_{k_2=0}^{d-1}\omega^{k_2(k+d-1)}|k_2\rangle\right)\cdots\left(\frac{1}{\sqrt{d}}\sum_{k_n=0}^{d-1}\omega^{k_n(k+d-1)}|k_n\rangle\right)\right]\right\} \\ = \; & \frac{1}{(\sqrt{d})^{n+1}}\sum_{k=0}^{d-1}\left[\sum_{j=0}^{d-1}\alpha_j\omega^{-kj}\left(\sum_{k_1,\cdots,k_n\in\{0,1,\cdots,d-1\}}\omega^{k_1k+k_2(k+d-1)+\cdots+k_n(k+d-1)}|k_1k_2\cdots k_n\rangle\right)\right] \\ = \; & \frac{1}{(\sqrt{d})^{n+1}}\sum_{k=0}^{d-1}\left[\sum_{j=0}^{d-1}\alpha_j\omega^{-kj}\left(\sum_{k_1,\cdots,k_n\in\{0,1,\cdots,d-1\}}\omega^{(k_1+\cdots+k_n)k+(k_2+\cdots+k_n)(d-1)}|k_1k_2\cdots k_n\rangle\right)\right] \\ = \; & \frac{1}{(\sqrt{d})^{n+1}}\sum_{k=0}^{d-1}\left[\sum_{k_1,\cdots,k_n\in\{0,1,\cdots,d-1\}}\left(\sum_{j=0}^{d-1}\alpha_j\omega^{-kj+(k_1+\cdots+k_n)k+(k_2+\cdots+k_n)(d-1)}|k_1k_2\cdots k_n\rangle\right)\right]\end{aligned} \tag{9}$$

Since $\omega = e^{\frac{2\pi i}{d}}$ and $\omega^d = 1$, one has $\omega^{(k_2+\cdots+k_n)(d-1)} = \omega^{d(k_2+\cdots+k_n)-(k_2+\cdots+k_n)} = \omega^{-(k_2+\cdots+k_n)}$. Therefore,

$$\begin{aligned}\Phi' &= \frac{1}{(\sqrt{d})^{n+1}}\sum_{k=0}^{d-1}\left[\sum_{k_1,\cdots,k_n\in\{0,1,\cdots,d-1\}}\left(\omega^{-(k_2+\cdots+k_n)}\sum_{j=0}^{d-1}\alpha_j\omega^{(k_1+\cdots+k_n-j)k}|k_1k_2\cdots k_n\rangle\right)\right]\\ &= \frac{1}{(\sqrt{d})^{n+1}}\sum_{j=0}^{d-1}\left[\sum_{k_1,\cdots,k_n\in\{0,1,\cdots,d-1\}}\left(\omega^{-(k_2+\cdots+k_n)}\sum_{k=0}^{d-1}\alpha_j\omega^{(k_1+\cdots+k_n-j)k}|k_1k_2\cdots k_n\rangle\right)\right]\end{aligned} \tag{10}$$

Since $\sum_{k=0}^{d-1}\omega^k = 0$, if $j \neq \sum_{i=1}^{n}k_i$, then $\sum_{k=0}^{d-1}\alpha_j\omega^{(k_1+k_2+\cdots+k_n-j)k} = 0$. Otherwise, $\sum_{k=0}^{d-1}\alpha_j\omega^{(k_1+k_2+\cdots+k_n-j)k} = \sum_{k=0}^{d-1}\alpha_j = d\alpha_j$. Therefore, only the item whose coefficient α_j with $j = \sum_{i=1}^{n}k_i$ in (10) can be retained, while other items will be disappeared. Therefore, the quantum state Φ' can be simplified as

$$\Phi' = \frac{1}{(\sqrt{d})^{n-1}}\sum_{k_1,\,k_2,\cdots,k_n\in\{0,1,\cdots,d-1\}}\omega^{-(k_2+\cdots+k_n)}\alpha_{k_1+k_2+\cdots+k_n}|k_1k_2\cdots k_n\rangle \tag{11}$$

From (11), we can see that Φ' is a symmetrical superposition state. Its particles can be in any state from $\{|0\rangle,|1\rangle, \ldots, |d-1\rangle\}$ with the same probability equal to $\frac{1}{d}\sum_{j=0}^{d-1}\left|\alpha_j\right|^2 = \frac{1}{d}$. It means that, if a participant measures his share, he will get a state from $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ with the same probability. The Von Neumann entropy of the share would approach its maximum, i.e. $S = -\frac{1}{d}\sum_{j=0}^{d-1}\log_2\left(\frac{1}{d}\right) = \log_2 d$, implying that the quantum state of shares is independent of that of the quantum secret. Therefore, participants cannot get any information of the quantum secret from their own shares, and our scheme can meet the confidentiality[25].

Security for outside eavesdropping. In our scheme, the transmission of particles is protected by decoy particles. The decoy particles are randomly selected from the Z-basis or the X-basis, and the secret particle is randomly inserted into the decoy particles.

Since an attacker does not know the positions and bases of the decoy particles, if he intends to steal information by measuring the secret particle, he will probably measure the decoy particles with a random basis and would bring errors into the decoy particles. The probability of selecting a wrong basis for a decoy particle is $\frac{1}{2}$ and the participant has a probability of $\frac{d-1}{d}$ to obtain a wrong value for the decoy particle. Therefore, the error rate of one decoy particle for eavesdropping is $\frac{d-1}{2d}$[26]. If there are l decoy particles, eavesdropping can be detected with a probability of $1-\left(\frac{d+1}{2d}\right)^l$. When l is sufficiently large, the probability will be close to 1.

Besides direct eavesdropping, another famous attack from outsider is known as "entangle-and-measure". The attacker will entangle an ancillary particle on the secret particle, and then measure the ancillary particle to steal information. It is remarked that, according to the results in[26], this attack can also be detected due to the errors of decoy particles.

Security for dishonest participant. In our scheme, the secret state φ is hidden in the entangled state Φ' as given in (11). As described in Section 5.1, Φ' is a symmetrical superposition state and each of its particles can be in any state from $\{|0\rangle, |1\rangle, \ldots, |d-1\}$ with the same probability. Even if $(n-1)$ participants work together, it is still impossible for them to get the initial secret state.

Without loss of generality, we assume $\{\text{Bob}_2, \text{Bob}_3, \ldots, \text{Bob}_n\}$ measure their particles and obtain results $\{r_2, r_3, \ldots, r_n\}$. Bob_1's particle will become the following state

$$\psi = \sum_{j=0}^{d-1}\omega^{-(r_2+\cdots+r_n)}\alpha_{j+r_2+\cdots+r_n}|j\rangle \tag{12}$$

From (12), we can see that $\{\text{Bob}_2, \text{Bob}_3, \ldots, \text{Bob}_n\}$ still cannot get the secret state φ without Bob_1. This confirms that the secret state can be recovered only if all participants are available, and hence collusion attack from dishonest participants will not succeed.

Nash equilibrium

In our scheme, there are four possible strategies when a rational participant performs the protocol.

- a_1: send the correct particles to other participants;
- a_2: remain silent, i.e., not send any particles to other participants;
- a_3: send the forged particles to other participants;
- a_4: measure the particles and then send them to other participants, i.e., the shared state will be destroyed.

The participant may have the following four utilities.

- U_1: he gets the secret but the other participants do not;
- U_2: he gets the secret and same for the other participants;
- U_3: he does not get the secret and neither the other participants;
- U_4: he does not get the secret but the other participants get the secret.

For a rational participant, it is obvious that $U_1 > U_2 > U_3 > U_4$.

Now, we analyze the utility of an arbitrary participant, Bob_i, performing different strategies in a round j.

(1) Perform strategy a_1: his utility is U_2.
(2) Perform strategy a_2: if the secret in this round is the real secret (the probability is γ), his utility is U_1; otherwise, his utility is U_3. So the utility under a_2 is $\gamma U_1 + (1-\gamma)U_3$.
(3) Perform strategy a_3: if the secret in this round is the real secret (the probability is γ), his utility is U_1; otherwise, his utility is $\alpha U_3 + (1-\alpha)U_2$, where α is the probability that his cheating behavior is detected by the others. As explained in Section 3, we have $\alpha = \frac{1}{d}$ in our scheme. Therefore, the utility under a_3 is $\gamma U_1 + (1-\gamma)\left[\frac{1}{d}U_3 + \left(1-\frac{1}{d}\right)U_2\right]$.
(4) Perform strategy a_4: it is similar to case (3) and the utility also equals to $\gamma U_1 + (1-\gamma)\left[\frac{1}{d}U_3 + \left(1-\frac{1}{d}\right)U_2\right]$.

The utility of Bob_i under different strategy is summarized below:

- $u_i(a_1) = U_2$
- $u_i(a_2) = \gamma U_1 + (1-\gamma)U_3$
- $u_i(a_3) = \gamma U_1 + (1-\gamma)\left[\frac{1}{d}U_3 + \left(1-\frac{1}{d}\right)U_2\right]$
- $u_i(a_4) = \gamma U_1 + (1-\gamma)\left[\frac{1}{d}U_3 + \left(1-\frac{1}{d}\right)U_2\right]$

Since $U_2 > U_3$, it can be easily deduced that $u_i(a_2)$ is always less than $u_i(a_3)$ or $u_i(a_4)$. Now, letting $U_2 > \gamma U_1 + (1-\gamma)\left[\frac{1}{d}U_3 + \left(1-\frac{1}{d}\right)U_2\right]$ or $\gamma < \frac{U_2 - U_3}{dU_1 - (d-1)U_2 - U_3}$, the rational participant Bob_i will always choose a_1 as his strategy since $u_i(a_1) > u_i(a_3) = u_i(a_4) > u_i(a_2)$.

Therefore, if the parameter γ is set to satisfy the inequality condition $\gamma < \frac{U_2 - U_3}{dU_1 - (d-1)U_2 - U_3}$, every rational participant will choose a_1 as his optimal strategy, which is the Nash equilibrium, and perform the protocol faithfully.

Comparison

In our scheme, it is assumed that the shared secret is a d-dimensional quantum state and quantum operations, such as the quantum Fourier transform and quantum-controlled-not, are employed. Although similar assumptions and operations are used in our previous work[24], the design and focus of this paper are totally different. The main feature of our scheme is to manage the "rationality". The scheme in[24] is only a traditional QSS scheme without considering the "rationality".

In particular, we introduce the game theory into the QSS to analyze the rational behavior of participant, based on respective definitions of rationality, fairness and Nash equilibrium. The proposed RQSS possesses some distinct features as discussed in Section 3, including the random structure, post verification based on quantum operation, and parameters setting based on Nash equilibrium. Furthermore, we analyze different strategies and utilities of the rational participant, and derive conditions to ensure rational participants to follow the protocol faithfully, by achieving the Nash equilibrium. All these novel contents do not appear in[24].

Indeed, the protocol of RQSS is also different from that suggested in[24]. In our scheme, the dealer applies the quantum inverse Fourier transform onto the shared state, and then performs the quantum-controlled-not operations and quantum Fourier transform to hide the shared state into an entangled state. For reconstruction, participants need to perform reverse operations, including the quantum inverse Fourier transform, the quantum-controlled-not and the quantum Fourier transform, to obtain the shared state and the verification states. In contrast, participants under the scheme in[24] only perform single-particle measurements and unitary operations to recover the shared state. Such a reconstruction process is not preferable, as participants cannot obtain the verification states to verify the faithfulness of other participants.

Conclusion

In this paper, we have proposed a RQSS scheme to manage rational participants who try to maximize their utilities. By using quantum operations, the dealer encodes the secret state into an entangled state and distributes to the participants, while participants can use reverse operations to recover the secret state. The behavior of the rational participant is analyzed with the use of Game theory, and suitable mechanisms are proposed to motivate rational participants to perform the protocol faithfully. As proved, our scheme is fair and secure, and the suggested strategy achieves the Nash equilibrium. Compared to the existing QSS schemes, our scheme is more practical in the presence of rational participants.

The entangled state is indispensable in our scheme. Compared with the single-qubit state, the multi-particles entangled state is harder to be prepared with the current technologies. However, as discussed in[27–32], some practical ways are possible to generate the entangled state. With the rapid development of quantum technology, generating entangled states would become easier in the future, making our scheme more practical.

References

1. Shamir, A. How to share a secret. *Communications of the ACM*. **22**, 612–613 (1979).
2. Halpern, J. & Teague, V. Rational secret sharing and multiparty computation. *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*. New York: ACM Press, 623–632 (2004).
3. Kol, G. & Naor, M. Cryptography and game theory: design protocols for exchanging information. *Proceedings of the 5th Theory of Cryptography Conference*. Berlin: Springer, 320–339 (2008).
4. Fuchsbauer, G., Katz, J. & Naccache, D. Efficient secret sharing in the standard communication model. *Proceedings of the 7th Theory of Cryptography Conference*. Berlin: Springer, 419–436 (2010).

5. Zhang, Z. F. & Liu, M. L. Rational secret sharing as extensive game. *Science China Information Sciences.* **56**, 1–13 (2013).
6. Feldman, P. A practical scheme for non-interactive verifiable secret sharing. *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*. New York: ACM Press, 427–437 (1987).
7. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. *Physical Review A.* **59**, 1829–1834 (1999).
8. Zhou, N. R., Song, H. C. & Gong, L. H. Continuous variable quantum secret sharing via quantum teleportation. *International Journal of Theoretical Physics.* **52**, 4174–4184 (2013).
9. Liao, C. H., Yang, C. W. & Hwang, T. Dynamic quantum secret sharing protocol based on GHZ state. *Quantum Information Processing.* **13**, 1907–1916 (2014).
10. Liu, F., Qin, S. J. & Wen, Q. Y. A quantum secret-sharing protocol with fairness. *Physica Scripta.* **89**, 075104 (2014).
11. Liu, L. L., Tsai, C. W. & Hwang, T. Quantum secret sharing using symmetric W state. *International Journal of Theoretical Physics.* **51**, 2291–2306 (2012).
12. Chen, R. K., Zhang, Y. Y., Shi, J. H. & Li, F. G. A multiparty error-correcting method for quantum secret sharing. *Quantum Information Processing.* **13**, 21–31 (2014).
13. Lau, H. K. & Weedbrook, C. Quantum secret sharing with continuous-variable cluster states. *Physical Review A.* **88**, 042313 (2013).
14. Rahaman, R. & Parker, M. G. Quantum scheme for secret sharing based on local distinguishability. *Physical Review A.* **91**, 022330 (2015).
15. Tavakoli, A., Herbauts, I., Zukowski, M. & Bourennane, M. Secret sharing with a single d-level quantum system. *Physical Review A.* **92**, 030302 (2015).
16. Lai, H. *et al*. Hybrid threshold adaptable quantum secret sharing scheme with reverse Huffman-Fibonacci-tree coding. *Scientific Reports.* **6**, 31350 (2017).
17. Tang, D. W., Wang, T. J., Mi, S. C., Geng, X. & Wang, M. C. High-dimensional circular quantum secret sharing. *International Journal of Theoretical Physics.* **55**, 4963–4971 (2016).
18. Cao, H. & Ma, W. P. (t, n) threshold quantum state sharing scheme based on linear equations and unitary operation. *IEEE Photonics Journal.* **9**, 7600207 (2017).
19. Chiawei, T. & Tzonelih, H. Multi-party quantum secret sharing based on two special entangled states. *SCIENCE CHINA: Physics, Mechanics & Astronomy.* **55**, 460–464 (2012).
20. Gao, G. Secure multiparty quantum secret sharing with the collective eavesdropping-check character. *Quantum Information Processing.* **12**, 55–68 (2013).
21. Sun, Y., Xu, S. W., Chen, X. B., Niu, X. X. & Yang, Y. X. Expansible quantum secret sharing network. *Quantum Information Processing.* **12**, 2877–2888 (2013).
22. Dunjko, V., Wallden, P. & Andersson, E. Quantum digital signatures without quantum memory. *Physical Review Letters.* **112**, 040502 (2014).
23. Bastidas, V. M., Omelchenko, I. & Zakharova, A. Quantum signatures of chimera states. *Physical Review E.* **92**, 062924 (2015).
24. Qin, H. W., Tso, R. L. & Dai, Y. W. Multi-dimensional quantum state sharing based on quantum Fourier transform. *Quantum Information Processing.* **17**, 48 (2018).
25. Ogawa, T., Sasaki, A., Iwamoto, M. & Yamamoto, H. Quantum secret sharing schemes and reversibility of quantum operations. *Physical Review A.* **72**, 032318 (2005).
26. Qin, H. W. & Dai, Y. W. d-dimensional quantum state sharing with adversary structure. *Quantum Information Processing.* **15**, 1689–1701 (2016).
27. Yukawa, M., Ukai, R., Loock, P. & Furusawa, A. Experimental generation of four-mode continuous-variable cluster states. *Physical Review A.* **78**, 012301 (2008).
28. Amselem, E. & Bourennane, M. Experimental four-qubit bound entanglement. *Nature Physics.* **5**, 748 (2009).
29. Huang, Y. F. *et al*. Experimental generation of an eight-photon Greenberger-Horne-Zeilinger state. *Nature Communications.* **2**, 546 (2011).
30. Su, X. L. *et al*. Experimental preparation of eight-partite cluster state for photonic qumodes. *Optics Letters.* **37**, 5178–5180 (2012).
31. Zhou, Y., Jia, X., Li, F., Xie, C. & Peng, K. Experimental generation of 8.4 dB entangled state with an optical cavity involving a wedged type-II nonlinear crystal. *Optics express.* **23**, 4952–4959 (2015).
32. Wang, X. L. *et al*. Experimental ten-photon entanglement. *Physical Review Letters.* **117**, 210502 (2016).

Acknowledgements

This study is supported by Natural Science Foundation of China (Grant No. 61602247) and Natural Science Foundation of Jiangsu Province (Grant No. BK20160840).

Author Contributions

Huawang Qin wrote the manuscript text. Wallace K.S. Tang and Raylin Tso reviewed the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.