

A rational quantum state sharing protocol with semi-off-line dealer

Hua-Li Zhang(张花丽), Bi-Chen Che(车碧琛), Zhao Dou(窦钊), Yu Yang(杨榆), and Xiu-Bo Chen(陈秀波)
Citation: Chin. Phys. B, 2022, 31 (**5**): 050309. DOI: 10.1088/1674-1056/ac4e02
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Phase-matching quantum key distribution with light source monitoring

Wen-Ting Li(李文婷), Le Wang(王乐), Wei Li(李威), and Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2022, 31 (**5**): 050310. DOI: 10.1088/1674-1056/ac4101

Efficient quantum private comparison protocol based on one direction discrete quantum walks on the circle

Jv-Jie Wang(王莒杰), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Chin. Phys. B, 2022, 31 (**5**): 050308. DOI: 10.1088/1674-1056/ac5a3f

Analysis and improvement of verifiable blind quantum computation

Min Xiao(肖敏) and Yannan Zhang(张艳南)
Chin. Phys. B, 2022, 31 (**5**): 050305. DOI: 10.1088/1674-1056/ac2f34

Self-error-rejecting multipartite entanglement purification for electron systems assisted by quantum-dot spins in optical microcavities

Yong-Ting Liu(刘永婷), Yi-Ming Wu(吴一鸣), and Fang-Fang Du(杜芳芳)
Chin. Phys. B, 2022, 31 (**5**): 050303. DOI: 10.1088/1674-1056/ac4489

Quantum private comparison of arbitrary single qubit states based on swap test

Xi Huang(黄曦), Yan Chang(昌燕), Wen Cheng(程稳), Min Hou(侯敏), and Shi-Bin Zhang(张仕斌)
Chin. Phys. B, 2022, 31 (**4**): 040303. DOI: 10.1088/1674-1056/ac4103

A rational quantum state sharing protocol with semi-off-line dealer

Hua-Li Zhang(张花丽)[1], Bi-Chen Che(车碧琛)[1], Zhao Dou(窦钊)[1,†], Yu Yang(杨榆)[2], and Xiu-Bo Chen(陈秀波)[1]

[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*

(Received 31 August 2021; revised manuscript received 4 December 2021; accepted manuscript online 24 January 2022)

A rational quantum state sharing protocol with the semi-off-line dealer is proposed. Firstly, the dealer Alice shares an arbitrary two-particle entangled state with the players by Einstein–Podolsky–Rosen (EPR) pairs and Greenberger–Horne–Zeilinger (GHZ) states. The EPR pairs are prepared by Charlie instead of the dealer, reducing the workload of the dealer. Secondly, all players have the same probability of reconstructing the quantum state, guaranteeing the fairness of the protocol. In addition, the dealer is semi-off-line, which considerably reduces the information exchanging between the dealer and the players. Finally, our protocol achieves security, fairness, correctness, and strict Nash equilibrium.

Keywords: rational quantum state sharing, game theory, semi-off-line, Nash equilibrium

PACS: 03.67.Dd, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/ac4e02

1. Introduction

The classical secret sharing (SS) protocol is used to share the secret among multiple players.[1–4] Each player reconstructs the shared secret by a certain number of shares (*e.g.* at least t shares) from other players. The quantum secret sharing (QSS) protocol is also used to share the secret among multiple players. Unlike the SS protocol, the QSS protocol can share the quantum information as well as classical information, while the SS protocol can only share classical information. The QSS protocol for sharing quantum information is also called the quantum state sharing (QSTS) protocol or the quantum information splitting (QIS) protocol. Because of the quantum no-cloning theorem, only one player Charlie can obtain the quantum state shared by the dealer Alice. But Charlie needs the help of all the other players due to the correlation of entangled states. Especially, according to the authorities of the players, the QSTS protocol can be divided into hierarchical QSTS (HQSTS)protocol[5–9] and non-hierarchical QSTS (NQSTS) protocol.[10–14] And in this paper, the NQSTS protocol is discussed.

In 1999, Cleve *et al.*[10] firstly proposed a QSTS scheme with quantum error correction codes.[11] Later, Li *et al.*[12] proposed a QSTS protocol based on entanglement swapping. Lance *et al.*[13] investigated a (2, 3) threshold QSTS protocol based on continuous variable tripartite entanglement. Then, multiparty QSTS of an arbitrary two-particle entangled state was investigated in Deng *et al.*'s,[14,15] Li *et al.*'s,[16] and Liu *et al.*'s[17] protocols. In 2005, Zhang *et al.*[18] proposed a QSTS protocol for continuous variables by two-mode squeezed state and single-mode squeezed state. Muralidharan and Panigrahi[19] designed a QSTS protocol based on a five-particle entangled state.[20] There are also QSTS protocols by cluster states.[21–25] In 2013, Jiang and Dong[26] proposed a multiparty QSTS protocol of an arbitrary multi-qubit state based on various probabilistic channels. Wang *et al.*[27] investigated a multiparty QSTS scheme of an arbitrary known qubit under two noisy environments. In 2017, Cao and Ma[28] presented a (t, n) threshold QSTS scheme based on linear equations and unitary operation. Later, the first verifiable threshold QSTS scheme was proposed by Cao and Ma.[29] In 2020, Song *et al.*[30] studied a verifiable (t, n) threshold QSTS scheme on IBM quantum cloud platform.

With more extensive and further research on cryptography, the rational SS (RSS) protocol has been proposed according to the actual needs.[31–36] In the RSS protocol, players are not honest or destructive, but rational, executing their strategies to maximize their utilities. The game theory is introduced to analyze the behavior of the players. Correspondingly, the rational QSTS (RQSTS) protocol was also explored. In 2015, the first RQSTS protocol was proposed by Maitra *et al.*[37] They respectively demonstrated a (t, n) RQSTS protocol with the semi-off-line dealer and the off-line dealer by Calderbank–Shor–Steane (CSS) code. In 2018, Dou *et al.*[38] proposed a rational QSTS (RQSTS) protocol with the online dealer. Qin *et al.*[39] proposed an RQSTS protocol based on the quantum Fourier transform.

In this paper, we propose an RQSTS protocol with the semi-off-line dealer inspired by Refs. [15,38]. First of all, in our protocol, the EPR pairs and GHZ states are used to share an arbitrary two-particle entangled state between the dealer and the rational players. Instead of the dealer in Ref. [15], the EPR pairs are prepared by player Charlie. Charlie is responsible for reconstructing the shared quantum state. So our protocol reduces the workload of the dealer. Secondly, the

†Corresponding author. E-mail: dou@bupt.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

dealer Alice does not know the shared quantum state,[37] so she cannot clone the state. Ultimately only one player Charlie can reconstruct the quantum state. Moreover, Charlie is jointly elected by all players, rather than designated by the dealer Alice,[37] which also guarantees the fairness of the protocol. Finally, compared with the protocol in Ref. [38], the dealer is of semi-off-line in our protocol, meaning that the dealer only needs to interact with the players twice: The first is to publish the number of rounds and the second is to publish the revelation round and the measurement results. Thus our protocol considerably reduces the information exchanging between the dealer and the players. In addition, our protocol also satisfies correctness, security and strict Nash equilibrium required by RQSTS.

The rest of this paper is organized as follows. In Section 2, we introduce the quantum states and quantum operators related to our protocol, the QSTS protocol proposed by Deng *et al.*, and basic game theory knowledge. In Section 3, our rational quantum state sharing protocol with the semi-off-line dealer is proposed in detail. In Section 4, our protocol is proved to achieve security, fairness, correctness, and strict Nash equilibrium. Finally, some conclusions are drawn and future work is also mentioned in Section 5.

2. Preliminaries

Because the players are rational in our protocol, both the QSTS and the game theory will be introduced in this section.

2.1. Quantum states and quantum operators

2.1.1. EPR pairs

An EPR pair is in one of the four Bell states shown below[40]

$$\left|\psi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle),\quad \left|\phi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle). \tag{1}$$

2.1.2. GHZ states

The three-particle GHZ states are written as follows:

$$\begin{aligned}\left|G_{ij+}\right\rangle&=\frac{1}{\sqrt{2}}(|0ij\rangle+\left|1\bar{i}\bar{j}\right\rangle),\\ \left|G_{ij-}\right\rangle&=\frac{1}{\sqrt{2}}(|0ij\rangle-\left|1\bar{i}\bar{j}\right\rangle),\end{aligned} \tag{2}$$

where $i,\ j\in\{0,\ 1\}$, $\bar{i}=1-i$, and $\bar{j}=1-j$. Then $(n+2)$-particle GHZ states are

$$\begin{aligned}\left|\mathrm{G}_{\underbrace{ij\ldots k}_{n+1}+}\right\rangle&=\frac{1}{\sqrt{2}}(|0\underbrace{ij\ldots k}_{n+1}\rangle+|1\underbrace{\bar{i}\bar{j}\ldots\bar{k}}_{n+1}\rangle),\\ \left|\mathrm{G}_{\underbrace{ij\ldots k}_{n+1}-}\right\rangle&=\frac{1}{\sqrt{2}}(|0\underbrace{ij\ldots k}_{n+1}\rangle-|1\underbrace{\bar{i}\bar{j}\ldots\bar{k}}_{n+1}\rangle),\end{aligned} \tag{3}$$

correspondingly, $i,\ j,\ k\in\{0,\ 1\}$, $\bar{i}=1-i$, $\bar{j}=1-j$, and $\bar{k}=1-k$.

2.1.3. Pauli operators

The Pauli operators represented by the computational basis are

$$\begin{aligned}&U_0=I=|0\rangle\langle 0|+|1\rangle\langle 1|,\quad U_1=\mathrm{Z}=|0\rangle\langle 0|-|1\rangle\langle 1|,\\ &U_2=\mathrm{X}=|0\rangle\langle 1|+|1\rangle\langle 0|,\quad U_3=\mathrm{i}Y=|0\rangle\langle 1|-|1\rangle\langle 0|.\end{aligned} \tag{4}$$

2.2. Review of Deng *et al.*'s QSTS protocol

In Deng *et al.*'s protocol,[15] it is supposed that there is a dealer Alice and $(n+1)$ players Bob_i $(1\le i\le n+1)$. And the two-particle entangled state $|\Phi\rangle_{xy}$ is

$$|\Phi\rangle_{xy}=\alpha|00\rangle_{xy}+\beta|01\rangle_{xy}+\gamma|10\rangle_{xy}+\delta|11\rangle_{xy}, \tag{5}$$

where $|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1$.

The basic process of Deng *et al.*'s protocol is as follows:

(i) Alice prepares $2(n+1)$ EPR pairs $|\phi^+\rangle_{a_ib_i}$ and $|\phi^+\rangle_{c_id_i}$ $(1\le i\le n+1)$ as in Eq. (1), and then sends the particles b_i and d_i to Bob_i $(1\le i\le n+1)$. The state of the composite quantum system can be written as

$$|\Phi\rangle_S=|\Phi\rangle_{xy}\otimes\prod_{i=1}^{n+1}\left|\phi^+\right\rangle_{a_ib_i}\otimes\left|\phi^+\right\rangle_{c_id_i}. \tag{6}$$

Because Alice performs the joint measurement of the $(n+2)$-particle GHZ states on the particles x, $a_1,\ \ldots\ ,\ a_{n+1}$, y, $c_1,\ \ldots,\ c_{n+1}$, respectively, the state $|\Phi\rangle_S$ can be rewritten as

$$\begin{aligned}|\Phi\rangle_S\ =\ &|\Psi\rangle_{xa_1\ldots a_{n+1}}\otimes|\Psi\rangle_{yc_1\ldots c_{n+1}}\\ &\otimes\left(\prod_{i=1}^{n+1}|\Psi\rangle_{b_i}\right)\otimes\left(\prod_{i=1}^{n+1}|\Psi\rangle_{d_i}\right),\end{aligned} \tag{7}$$

where $|\Psi\rangle_{xa_1\ldots a_{n+1}}\otimes$, $|\Psi\rangle_{yc_1\ldots c_{n+1}}\in\{\left|\mathrm{G}_{\underbrace{ij\ldots k}_{n+1}+}\right\rangle,\ \left|\mathrm{G}_{\underbrace{ij\ldots k}_{n+1}-}\right\rangle\}$ are the results of the joint measurements performed by Alice.

(ii) After Alice completes the joint measurements, the state of the subsystem (without being normalized) can be written as

$$\begin{aligned}|\Phi\rangle_s\ =\ &\alpha|ij\ldots k\rangle_{b_1b_2\ldots b_{n+1}}|mn\ldots l\rangle_{d_1d_2\ldots d_{n+1}}\\ &\pm\beta|ij\ldots k\rangle_{b_1b_2\ldots b_{n+1}}\left|\bar{m}\bar{n}\ldots\bar{l}\right\rangle_{d_1d_2\ldots d_{n+1}}\\ &\pm\gamma\left|\bar{i}\bar{j}\ldots\bar{k}\right\rangle_{b_1b_2\ldots b_{n+1}}|mn\ldots l\rangle_{d_1d_2\ldots d_{n+1}}\\ &\pm\delta\left|\bar{i}\bar{j}\ldots\bar{k}\right\rangle_{b_1b_2\ldots b_{n+1}}\left|\bar{m}\bar{n}\ldots\bar{l}\right\rangle_{d_1d_2\ldots d_{n+1}}.\end{aligned} \tag{8}$$

Because

$$|0\rangle=\frac{1}{\sqrt{2}}(|+x\rangle+|-x\rangle)\quad\text{and}\quad|1\rangle=\frac{1}{\sqrt{2}}(|+x\rangle-|-x\rangle),$$

we can obtain

$$|i\rangle=\frac{1}{\sqrt{2}}[|+x\rangle+(-1)^i|-x\rangle]\ (i,\ j,\ \ldots,\ k,\ m,\ n,\ \ldots,\ l\in\{0,\ 1\}).$$

(iii) Suppose that Bob_{n+1} (Charlie) is the player reconstructing $|\Phi\rangle_{xy}$ the expression of the X basis measurements performed by n players Bob_i $(1 \le i \le n)$ can be written as

$$M = [(\langle +x|)^{n-t}(\langle -x|)^t]_{b_i} \otimes [(\langle +x|)^{n-q}(\langle -x|)^q]_{d_i}, \quad (9)$$

where $[(\langle +x|)^{n-t}(\langle -x|)^t]_{b_i}$ and $[(\langle +x|)^{n-q}(\langle -x|)^q]_{d_i}$ are the measurement operations related to the particles b_i and d_i, respectively; t and q are the numbers of measurement results $|-x\rangle$ obtained by n players Bob_i $(1 \le i \le n)$ performing X basis measurements on b_i and d_i respectively.

(iv) After Bob_i $(1 \le i \le n)$'s measurements, the state of Charlie's particles b_{n+1}, d_{n+1} can be written as

$$\begin{aligned}\Phi_{b_{n+1}d_{n+1}} &= M|\Phi\rangle_s = (\alpha|kl\rangle + (-1)^q\beta|k\bar{l}\rangle \\ &+ (-1)^t\gamma|\bar{k}l\rangle + (-1)^{t+q}\delta|\bar{k}\bar{l}\rangle)_{b_{n+1}d_{n+1}}. \quad (10)\end{aligned}$$

According to the measurement results, Charlie performs the unitary operations $U_i \otimes U_j$ $(i, j \in \{0, 1, 2, 3\})$ to reconstruct $|\Phi\rangle_{xy}$. The measurement results can be expressed as $V_{xa_1\ldots a_{n+1}}, V_{yc_1\ldots c_{n+1}}, P_{xa_1\ldots a_{n+1}} \otimes (-1)^t$, and $P_{yc_1\ldots c_{n+1}} \otimes (-1)^q$, where $V_{xa_1\ldots a_{n+1}} = V_{|G_{ij\ldots k\pm}\rangle} = k$, $V_{yc_1\ldots c_{n+1}} = V_{|G_{mn\ldots l\pm}\rangle} = l$, $P_{xa_1\ldots a_{n+1}} = P_{|G_{ij\ldots k\pm}\rangle} = \pm$, $P_{yc_1\ldots c_{n+1}} = P_{|G_{mn\ldots l\pm}\rangle} = \pm$.

2.3. Game theory

In the game theory, all players are rational. The quantum state sharing protocol is regarded as a pair (Γ, σ), where Γ is the game with n players and $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ is the strategies of n players. There are also the notations $\boldsymbol{\sigma}_{-i} = (\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n)$ and $(\sigma_i', \boldsymbol{\sigma}_{-i}) = (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i', \sigma_{i+1}, \ldots, \sigma_n)$. The outcome of the game is denoted as $o(\boldsymbol{\sigma}) = (o_1, \ldots, o_n)$, and the utility function u_i of each player P_i is defined over the set of possible outcomes for the game, which is a polynomial with the security parameter k.

Definition 1 Fairness

A rational quantum state sharing protocol $(\Gamma, \boldsymbol{\sigma})$ is said to be completely fair, if for each arbitrary alternative strategy $\boldsymbol{\sigma}_i'$ is followed by player P_i, there exists a negligible function $\mu(k)$ in the security parameter k such that the following holds:

$$\begin{aligned}&\Pr[o_i(\Gamma, (\sigma_i', \boldsymbol{\sigma}_{-i})) = \text{Right Result}] \\ \le\ &\Pr[o_{-i}(\Gamma, (\sigma_i', \sigma_{-i})) = \text{Right Result}] + \mu(k). \quad (11)\end{aligned}$$

Definition 2 Correctness

A rational quantum state sharing protocol (Γ, σ) is said to be correct, if for each arbitrary alternative strategy $\boldsymbol{\sigma}_i'$ is followed by player P_i, there exists a negligible function $\mu(k)$ in the security parameter k such that the following holds:

$$\Pr[o_{\text{Charlie}}(\Gamma, (\sigma_i', \sigma_{-i})) = \text{False Result}] \le \mu(k). \quad (12)$$

Definition 3 Strict Nash equilibrium

The strategy $\boldsymbol{\sigma}$ suggested in the mechanism $(\Gamma, \boldsymbol{\sigma})$ is a strict Nash equilibrium, if any strategy σ_i' for each P_i satisfies the following inequality:

$$u_i(\sigma_i', \boldsymbol{\sigma}_{-i}) < u_i(\boldsymbol{\sigma}). \quad (13)$$

3. Rational quantum state sharing protocol with semi-off-line dealer

In our protocol, there is a dealer Alice and $(n+1)$ players Bob_i $(1 \le i \le n)$, and the quantum shared by Alice is $|\Phi\rangle_{xy}$ as indicated in Eq. (5). The detailed process of rational quantum state sharing protocol with the semi-off-line dealer is as follows.

3.1. Dealer's protocol

Since the dealer is of semi-off-line, Alice only needs to interact with the players twice: the first is at the beginning of the protocol and the second is at the end of the protocol.

[D1] Alice determines the number of rounds $(r+w)$ and the real position r according to a geometric distribution $\mathcal{G}(\gamma)$, which is completely unknown to the players Bob_i $(1 \le i \le n+1)$. The parameter γ is determined according to the players' utilities. Then Alice announces that the players need to perform $(r+w)$ rounds.

[D2] After receiving the sig $= 1$ sent by Charlie in the last round, Alice announces the position r of the real revelation round. If Charlie pays the cooperating players Bob_i $(1 \le i \le n+1,\ i \ne s')$ in the r-th round, Alice will perform the joint measurements of the $(n+2)$-particle GHZ states according to the remaining particles sent by Charlie. Then, Alice announces the measurement results. Otherwise, Alice aborts the protocol.

3.2. Player's protocol

The process of each player in the j-th round $(1 \le j \le r+w)$ is as follows.

[P1] Each player Bob_i publishes an integer p_i $(1 \le i \le n+1)$ at the same time. If any player does not publish it, he cannot participate in this round nor the remaining rounds of the protocol.

[P2] Calculates the sum $s = \sum_{i=1}^{n+1} p_i$ based on the integer published by each player.

[P3] Takes the remainder of s by calculating, then $s = s \bmod (n+1)$, $s' = s+1$ $(1 \le s' \le n+1)$, $\text{Bob}_{s'}$ is Charlie. Since the dealer is of semi-off-line, Alice no longer needs to prepare shares for the players. The task of share generation is completed by Charlie.

[P4] Charlie prepares $2(n+1)$ EPR pairs, $|\phi^+\rangle_{a_ib_i}$ and $|\phi^+\rangle_{c_id_i}$. Here $|\phi^+\rangle_{a_ib_i} = (1/\sqrt{2})(|00\rangle + |11\rangle)_{a_ib_i}$, $|\phi^+\rangle_{c_id_i} = (1/\sqrt{2})(|00\rangle + |11\rangle)_{c_id_i}$ $(1 \le i \le n+1)$.

[P5] Charlie sends the particles b_i and d_i to Bob$_i$ $(i \neq s')$.

[P6] Each player Bob$_i$ $(i \neq s')$ performs X basis measurement on particles b_i and d_i and then publishes the measurement results.

[P7] Charlie judges whether the players Bob$_i$ $(i \neq s')$ are cheated based on the measurement results announced by them. Then Charlie publishes the number of the cheating players. These cheating players cannot participate in this round nor the remaining rounds of the protocol.

[P8] If $j = r + w$, Charlie sends a sign sig $= 1$ to Alice. Otherwise, the players finish the current round and proceed to the next round.

[P9] According to the position r of the revelation round published by Alice, Charlie in the r-th round pays the cooperating players Bob$_i$ $(i \neq s')$. And the total remuneration paid to them does not change depending on the number of the cooperating players Bob$_i$ $(i \neq s')$. According to the measurement results of Alice and the players Bob$_i$ $(i \neq s')$, Charlie will perform corresponding unitary operations on his particles b_s and d_s and successfully reconstruct $|\Phi\rangle_{xy}$.

4. Analyses

4.1. Utilities and preferences

In this protocol, only Charlie in the revelation round can reconstruct the quantum state $|\Phi\rangle_{xy}$, so the strategies and benefits of Charlie and Bob$_i$ $(i \neq s')$ will be slightly different.

(I) The strategies of the players are as follows:

Charlie:

c_1 Chooses to cooperate

When Alice announces the revelation round, Charlie pays the corresponding remuneration to the players Bob$_i$ $(i \neq s')$ who chooses to cooperate.

c_2 Chooses to cheat

When Alice announces the revelation round, Charlie refuses to pay the players Bob$_i$ $(i \neq s')$ who chooses to cooperate.

Bob$_i$ $(i \neq s')$:

b_1 Chooses to cooperate and publishes the correct measurement results.

b_2 Chooses to cheat and publishes the wrong measurement results, or remain silent.

(II) The utilities of the players are as follows:

Charlie:

$U_{c_1}^+$: Chooses to cooperate and successfully reconstructs $|\Phi\rangle_{xy}$.

$U_{c_2}^-$: Fails due to own cheating behavior.

U_{c_1} : Fails due to cheating by other players.

Bob$_i$ $(i \neq s')$:

$U_{b_1}^+$: Chooses to cooperate and successfully helps Charlie reconstruct $|\Phi\rangle_{xy}$.

U_{b_1} : Chooses to cooperate but fails to help Charlie reconstruct $|\Phi\rangle_{xy}$.

$U_{b_2}^-$: His cheating is discovered by Charlie.

U_{b_2} : His cheating is not discovered by Charlie.

For a rational player, Charlie has the following preference: $U_{c_1}^+ > U_{c_1} > U_{c_2}^-$; Bob$_i$ $(i \neq s')$ has the following preference: $U_{b_2} > U_{b_1}^+ = U_{b_1} > U_{b_2}^-$.

Firstly, the goal of the players is to obtain $|\Phi\rangle_{xy}$. For Charlie, he is the only one who can reconstruct $|\Phi\rangle_{xy}$. Obviously Charlie will obtain a higher utility when he successfully reconstructs $|\Phi\rangle_{xy}$, so $U_{c_1}^+ > U_{c_1}$. In fact, U_{c_1} is influenced by other players who cheated. The U_{c_1} can be expressed by $U_{c_1} = U_{c_1}^+ - x\Delta$, where x is the number of players Bob$_i$ $(i \neq s')$ who cheated, and Δ is Charlie's loss when Bob$_i$ $(i \neq s')$ successfully cheats. Secondly, for Bob$_i$ $(i \neq s')$, although he cannot reconstruct $|\Phi\rangle_{xy}$, he can get paid by helping Charlie reconstruct $|\Phi\rangle_{xy}$ then $U_{b_1}^+ \leq U_{c_1}^+ + \mu(k)$, where $\mu(k)$ is a negligible function with parameter k. In addition, if Bob$_i$ $(i \neq s')$ chooses to cooperate, his utility should not be affected by other players, so $U_{b_1}^+ = U_{b_1}$. Finally, whether Charlie or Bob$_i$ $(i \neq s')$ chooses to cheat among the players, their utilities should be the lowest and the same, so $U_{c_2}^- = U_{b_2}^-$. In addition, if Bob$_i$ $(i \neq s')$ successfully cheats, his utility would be higher than cooperation, so $U_{b_2} > U_{b_1}^+ = U_{b_1}$.

4.2. Security

A QSTS protocol can be attacked by the eavesdropper or the players, so the security of the protocol is analyzed from the outside attack and the participants' attack.

4.2.1. Outside attack

In the outside attack, the eavesdropper may attempt to destroy or steal the secret message of communication in the protocol. Accordingly, the outside attack is divided into the active attack and the passive attack.

Several active attacks on QSTS include fake-signal attack, entangled additional particle attack, intercept-resend attack, and correlation-elicitation attack.[41–44] Thus a secure quantum channel is set up by the method in Ref. [43], ensuring that the communication between the dealer and the players is not threatened. In short, before the protocol begins, the dealer Alice will conduct security detection, that is, insert the decoy qubits into the qubits sent to the players and publish the location of the decoy particles. Then, the players perform X basis or Z basis measurements on the decoy particles. Finally, Alice compares the measurement results of the decoy qubits published by the player with the initial states of the decoy qubits. If the error rates are lower than the set threshold, the quantum channel is safe; otherwise, Alice will restart the security detection until she is sure that the quantum channel is safe.

In the entangled additional particle attack, an eavesdropper Eve intercepts the particles sent by Charlie to other players and performs unitary operations on the particles. It is supposed that there are three players, who are Bob$_1$, Bob$_2$,

and Charlie. Charlie prepares six EPR pairs $|\phi^+\rangle_{a_ib_i}$ and $|\phi^+\rangle_{c_id_i}$ $(1\le i\le 3)$, then sends the particles b_i and d_i to Bob$_i$ $(1\le i\le 2)$. Alice performs the joint measurements on x, a_1, a_2, a_3, and y, c_1, c_2, c_3. If Alice's measurement result is $|G_{000+}\rangle=(1/\sqrt{2})(|0000\rangle+|1111\rangle)$, the quantum state of the system becomes

$$\begin{aligned}|\Phi\rangle_S^{\mathrm{E}} = \frac{1}{\sqrt{2}}[&\alpha|00\rangle_{b_1d_1}|00\rangle_{b_2d_2}|000\rangle_{b_3d_3\mathrm{E}}\\ &+\alpha|00\rangle_{b_1d_1}|00\rangle_{b_2d_2}|001\rangle_{b_3d_3\mathrm{E}}\\ &+\beta|01\rangle_{b_1d_1}|01\rangle_{b_2d_2}|010\rangle_{b_3d_3\mathrm{E}}\\ &+\beta|01\rangle_{b_1d_1}|01\rangle_{b_2d_2}|011\rangle_{b_3d_3\mathrm{E}}\\ &+\gamma|10\rangle_{b_1d_1}|10\rangle_{b_2d_2}|100\rangle_{b_3d_3\mathrm{E}}\\ &+\gamma|10\rangle_{b_1d_1}|10\rangle_{b_2d_2}|101\rangle_{b_3d_3\mathrm{E}}\\ &+\delta|11\rangle_{b_1d_1}|11\rangle_{b_2d_2}|110\rangle_{b_3d_3\mathrm{E}}\\ &+\delta|11\rangle_{b_1d_1}|11\rangle_{b_2d_2}|111\rangle_{b_3d_3\mathrm{E}}].\end{aligned}\tag{14}$$

If the measurement results of Bob$_1$ and Bob$_2$ are $|+x\rangle|+x\rangle$ and $|+x\rangle|-x\rangle$ respectively, the combined quantum state of Charlie and Eve becomes

$$\begin{aligned}\Phi_{b_3d_3}^{\mathrm{E}} = &(\alpha|00\rangle-\beta|01\rangle+\gamma|10\rangle\\ &-\delta|11\rangle)_{b_3d_3}\frac{1}{\sqrt{2}}(|0\rangle+\beta|1\rangle)_{\mathrm{E}}.\end{aligned}\tag{15}$$

According to Eq. (15), Eve cannot steal any information about $|\Phi\rangle_{xy}$.

For the intercept-resend attack, the eavesdropper intercepts the particles sent to the player by the dealer in the channel. And then the eavesdropper sends the players the particles he prepared. In order not to break the coherence between the players' particles, Eve sends the player $2(n+1)$ EPR pairs as in Eq. (3), which are prepared by himself. However, he does not know the position nor the quantum state of the decoy particles in the particles sent by Alice, so the error rate will exceed the threshold and be detected by Alice.

In the passive attack, the QSTS is threatened by information leakage. Since our protocol has a secure quantum channel, all unauthorized users cannot obtain any information about the shared quantum state. So for an eavesdropper, he knows only the measurement results published by Alice and the players Bob$_i$ $(i\neq s')$. In addition, owing to the quantum no-cloning theorem, the eavesdropper cannot obtain the quantum state by Charlie.

4.2.2. Participants' attack

Compared with an eavesdropper, a player can destroy or steal the information through the participants' attack, or the outside attack. The outside attack launched by a player will be regarded as the outside attack launched by an eavesdropper. And the analysis of the outside attack has been given in Subsubsection 4.2.1. This subsubsection is devoted to the participants' attack.

In our protocol, the players are divided into Charlie (the player who will reconstruct $|\Phi\rangle_{xy}$) and the players Bob$_i$ $(i\neq s')$ who help Charlie.

Owing to the quantum no-cloning theorem, only Charlie can obtain $|\Phi\rangle_{xy}$ in the end. For Charlie, he may want to reconstruct $|\Phi\rangle_{xy}$ without the help of other players Bob$_i$ $(i\neq s')$. According to Eq. (10), after Alice and other players complete the measurements, Charlie's density matrix is

$$\begin{aligned}\rho_{\mathrm{Charlie}} &= \Phi_{b_{s'}d_{s'}}(\Phi_{b_{s'}d_{s'}})^{\dagger}\\ &= \alpha^2|kl\rangle\langle kl|+\beta^2|k\bar{l}\rangle\langle k\bar{l}|\\ &\quad+\gamma^2|\bar{k}l\rangle\langle\bar{k}l|+\delta^2|\bar{k}\bar{l}\rangle\langle\bar{k}\bar{l}|,\end{aligned}\tag{16}$$

where $k,\ l\in\{+,\ -\}$, $\overline{+}=-$, $\overline{-}=+$. According to Eq. (16), Charlie does not know any information about $|\Phi\rangle_{xy}$. So if Charlie does not obtain the measurement results of other players Bob$_i$ $(i\neq s')$, which are closely related to the final unitary operations performed by Charlie, Charlie cannot succeed in reconstructing $|\Phi\rangle_{xy}$

For Bob$_i$ $(i\neq s')$, they may want to obtain $|\Phi\rangle_{xy}$. In each round, Bob$_i$ $(i\neq s')$ are required to perform X basis measurements on their particles and publish their measurement results. On the contrary, Alice performs the joint measurements on $|\Phi\rangle_{xy}$ and the remaining quantum states at the end of this protocol. In fact, during the whole execution of this protocol, Bob$_i$ $(i\neq s')$ cannot obtain any information about $|\Phi\rangle_{xy}$. Meanwhile, since Charlie performs the unitary operations on particles b_s and d_s, it is also impossible for Bob$_i$ $(i\neq s')$ to reconstruct $|\Phi\rangle_{xy}$.

Furthermore, if Bob$_i$ $(i\neq s')$ send the wrong measurement results, Charlie will discover their cheating behaviors by the EPR pairs $(|\phi^+\rangle=(1/\sqrt{2})(|00\rangle+|11\rangle)=(1/\sqrt{2})(|{+}{+}\rangle+|{-}{-}\rangle))$ shared with them. So our protocol achieves security.

4.3. Fairness

Owing to the unknown quantum state for the dealer Alice and the quantum no-cloning theorem, in the end, only one player Charlie can reconstruct $|\Phi\rangle_{xy}$. But instead of the dealer's appointment,[36] Charlie is randomly elected by all players Bob$_i$ $(1\le i\le n+1)$ in each round. Therefore, Charlie's generation event in our protocol is fair.

Theorem 1 If a player's utility from cooperation is higher than the utility from cheat, this protocol achieves fairness.

Proof In this protocol, if a player deviates from the suggested strategy during executing the protocol, the protocol will not be aborted. But the cheating player cannot participate in this round nor the remaining rounds.

The player Bob$_i$ $(1\le i\le n+1)$'s strategy in the j-th round is taken for example, and the probability that this round is the revelation round is $\Pr(j=r)$ denoted by λ. When the player chooses to cheat, if $j=r$, his utility is $[1/(n+1)](U_{c_1}^{+}-x\Delta)+[n/(n+1)]U_{b_1}$. If $j\neq r$, his utility

is $[1/(n+1)]U_{c_2}^- + [n/(n+1)]U_{b_2}^-$. On the contrary, when the player chooses to cooperate, if $j = r$, his utility is $[1/(n+1)](U_{c_1}^+ - x\Delta) + [n/(n+1)]U_{b_1}$. Otherwise his utility is $[1/(n+1)]U_{c_1}^+ + [n/(n+1)]U_{b_1}^+$. Therefore, the expected utility of the player choosing to cheat is

$$\begin{aligned} U_{\text{Cheating}}(x) \;=\; & \lambda\left[\frac{1}{n+1}(U_{c_1}^+ - x\Delta) + \frac{n}{n+1}U_{b_2}\right] \\ & + (1-\lambda)\left(\frac{1}{n+1}U_{c_2}^- + \frac{n}{n+1}U_{b_2}^-\right), \end{aligned}$$

and the expected utility of the player choosing to cooperate is

$$\begin{aligned} U_{\text{Cooperating}}(x) \;=\; & \lambda\left[\frac{1}{n+1}(U_{c_1}^+ - x\Delta) + \frac{n}{n+1}U_{b_1}\right] \\ & + (1-\lambda)\left(\frac{1}{n+1}U_{c_1}^+ + \frac{n}{n+1}U_{b_1}^+\right). \end{aligned}$$

$$\begin{aligned} & U_{\text{Cooperating}}(x) - U_{\text{Cheating}}(x) \\ =\; & \frac{1}{n+1}[U_{c_1}^+ - U_{c_2}^- + n(U_{b_1} - U_{c_2}^-)] \\ & - \lambda\frac{1}{n+1}[U_{c_1}^+ - U_{c_2}^- + n(U_{b_2} - U_{c_2}^-)]. \end{aligned} \tag{17}$$

Since $U_{c_1}^+ > U_{c_2}^-$ and $U_{b_1} > U_{c_2}^-$, in order to ensure the fairness of the protocol, the player's utility $U_{\text{Cooperating}}(x)$ from cooperation must be higher than the utility $U_{\text{Cheating}}(x)$ from cheat. Then λ should satisfy the condition

$$\lambda < \frac{U_{c_1}^+ - U_{c_2}^- + n(U_{b_1} - U_{c_2}^-)}{U_{c_1}^+ - U_{c_2}^- + n(U_{b_2} - U_{c_2}^-)}.$$

Thus, when

$$\lambda < \frac{U_{c_1}^+ - U_{c_2}^- + n(U_{b_1} - U_{c_2}^-)}{U_{c_1}^+ - U_{c_2}^- + n(U_{b_2} - U_{c_2}^-)},$$

our protocol achieves fairness.

4.4. Correctness

Theorem 2 If all players in this protocol are rational, the protocol can achieve correctness.

Proof In this protocol, the players do not know the position of the real revelation round r. On the one hand, if the players Bob_i $(i \neq s')$ send the wrong measurement results or remain silent in one round, they cannot participate in this round nor the remaining rounds. On the other hand, if Charlie, who reconstructs the quantum state in the revelation round, refuses to cooperate, his utility will be greatly reduced. In the rational quantum state protocol, as the players' purpose is to maximize their utilities, no player will have an incentive to cheat. And eventually, Charlie will reconstruct the quantum state with 100% probability. Therefore, our protocol achieves correctness.

4.5. Strict Nash equilibrium

Theorem 3 If

$$\lambda < \frac{U_{c_1}^+ - U_{c_2}^- + n(U_{b_1} - U_{c_2}^-)}{U_{c_1}^+ - U_{c_2}^- + n(U_{b_2} - U_{c_2}^-)},$$

this protocol achieves strict Nash equilibrium.

Proof From the perspective of game theory, if the protocol achieves strict Nash equilibrium, no matter what other players' implementation strategies are, the utility of each player when cheating should be less than his or her utility when cooperating.

In the j-th round of the protocol, when a player Bob_i $(1 \leq i \leq n+1)$ executes the deviation strategy σ_i', his utility is

$$\begin{aligned} U_{\text{Cheating}}(x) \;=\; & \lambda\left[\frac{1}{n+1}(U_{c_1}^+ - x\Delta) + \frac{n}{n+1}U_{b_1}\right] \\ & + (1-\lambda)\left(\frac{1}{n+1}U_{c_2}^- + \frac{n}{n+1}U_{b_2}^-\right). \end{aligned}$$

And when he follows the protocol, his utility is

$$\begin{aligned} U_{\text{Cooperating}}(x) \;=\; & \lambda\left[\frac{1}{n+1}(U_{c_1}^+ - x\Delta) + \frac{n}{n+1}U_{b_2}\right] \\ & + (1-\lambda)\left(\frac{1}{n+1}U_{c_1}^+ + \frac{n}{n+1}U_{b_1}^+\right). \end{aligned}$$

Then $u_i(\sigma_i', \boldsymbol{\sigma}_{-i}) = U_{\text{Cheating}}(x)$ and $u_i(\boldsymbol{\sigma}) = U_{\text{Cooperating}}(x)$. When

$$\lambda < \frac{U_{c_1}^+ - U_{c_2}^- + n(U_{b_1} - U_{c_2}^-)}{U_{c_1}^+ - U_{c_2}^- + n(U_{b_2} - U_{c_2}^-)},$$

there is $u_i(\sigma_i, \boldsymbol{\sigma}_{-i}) < u_i(\boldsymbol{\sigma})$. So our protocol achieves the strict Nash equilibrium.

4.6. Comparison of results among protocols

The comparison of results among the protocols is shown in Table 1.

Table 1. Comparison of results among the protocols.

Protocols	Whether the players are rational	Whether Alice knows the secret	Whether Charlie is chosen by Alice	Whether Alice is online
Deng *et al.*[15]	No	No	–	–
Maitra *et al.*[37]	Yes	Yes	Yes	No
Qin *et al.*[39]	Yes	Yes	–	No
Dou *et al.*[38]	Yes	No	No	Yes
Our protocol	Yes	No	No	No

For the first condition "Whether the players are rational", from a practical perspective, a player should be rational. In a rational protocol, a player will choose to participate in the protocol honestly or dishonestly based on his own utility. Therefore, the rational protocol is more practical with the actual situation. In Deng *et al.*'s[15] and the other general QSTS protocols, a player is either an honest player or a dishonest player. On the contrary, in rational protocols, such as Maitra *et al.*'s,[37] Qin *et al.*'s,[39] Dou *et al.*'s,[38] and ours, they start from themselves and judge how to choose strategies to maximize their own utilities.

For the second condition "Whether Alice knows the secret", if Alice knows the shared quantum state, the protocol is like the remote preparation state. So Alice can clone the shares of the shared quantum state. Ultimately, not only one player can obtain the shared quantum state. In general, a dealer should be unknown to the shared quantum state, so only one player can obtain the shared quantum state, which is very much in line with the idea that multiple players share a quantum state. In Maitra *et al.*'s[37] and Qin *et al.*'s[39] protocols, Alice knows the information about the shared quantum state. While in Dou *et al.*'s[38] protocol and ours, Alice does not know the information about the shared quantum state.

For the third condition "Whether Charlie is chosen by Alice", if Charlie is chosen by Alice, it is unfair to other players, which may cause rational players to give up participating in the protocol. In Maitra *et al.*'s[37] protocol, Charlie is chosen by Alice. In Qin *et al.*'s[39] protocol, each player can obtain the shared quantum state, because the shared quantum state is known to the dealer Alice. While in Dou *et al.*'s protocol[38] and ours, Charlie is elected by all the players, which ensures that every player has the same chance to become Charlie and thus making the protocol fair in Charlie's election.

For the last condition "Whether Alice is online", an online dealer Alice must interact with all players in each round, which leads to excessive information exchanging between the dealer and the players. A semi-off-line dealer Alice only needs to interact with the player twice. An off-line dealer Alice only needs to distribute the shares.[37] For a protocol with the semi-off-line or off-line dealer, it reduces the information exchanging between the dealer and the players.[37] In Dou *et al.*'s[38] and Qin *et al.*'s[39] protocols, the dealer is online. In Ref. [15], Deng *et al.* respectively demonstrated a (t, n) RQSS protocol with the semi-off-line dealer and the off-line dealer. In our protocol, the dealer is of semi-off-line.

5. Conclusions and future work

In this work, we propose a rational quantum state sharing protocol with the semi-off-line dealer. In our protocol, the dealer Alice shares an arbitrary two-particle entangled state with the players by EPR pairs and GHZ states. Especially, the EPR pairs are prepared by Charlie. Compared with the preparation by the dealer, the preparation by Charlie can reduce the workload of the dealer. Meanwhile, each player has the same chance to become Charlie. In other words, Charlie is randomly elected by all players. Then, the fairness of the protocol is ensured. In addition, comparing with the quantum state sharing protocol with the online dealer,[38] the dealer appears only twice. Thus, the information about the shared quantum state cannot be directly provided for the players by the dealer.[37] Moreover, our protocol also proves to be correct and achieve a strict Nash equilibrium.

Our protocol is a non-hierarchical QSTS protocol. In fact, hierarchical QSTS protocol is a more general than non-hierarchical QSTS protocol.[10–14] In hierarchical QSTS protocol, since the players are in different grades, they have different capabilities to reconstruct the shared quantum state. Therefore, the future work that is worth doting is to investigate a hierarchical QSTS protocol in which the players are rational.

Acknowledgements

Project supported by the National Key Research and Development Program of China (Grant No. 2020YFB1805405), the 111 Project, China (Grant No. B21049), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data, China (Grant No. 2019BDKFJJ014), and the Fundamental Research Funds for the Central Universities, China (Grant No. 2020RC38).

References

[1] Shamir A 1979 *Commun. ACM* **22** 612
[2] Benaloh J and Leichter J 1988 *Conference on the Theory and Application of Cryptography*, 1988, Springer, New York, p. 27
[3] Brickell E F 1989 *Workshop on the Theory and Application of of Cryptographic Techniques*, 1989, Springer, Berlin, Heidelberg, p. 468
[4] Krawczyk H 1993 *Annual international cryptology conference*, 1993, Springer, Berlin, Heidelberg, p. 136
[5] Wang X W, Xia L X, Wang Z Y and Zhang D Y 2010 *Opt. Commun.* **283** 1196
[6] Wang X W, Zhang D Y, Tang S Q, Zhan X G and You K M 2010 *Int. J. Theor. Phys.* **49** 2691
[7] Wang X W, Zhang D Y, Tang S Q and Xie L J 2011 *J. Phys. B: At., Mol. Opt. Phys.* **44** 035505
[8] Peng J Y, Bai M Q and Mo Z W 2014 *Chin. Phys. B* **23** 010304
[9] Guo W M and Qin L R 2018 *Chin. Phys. B* **27** 110302
[10] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[11] Steane A M 1996 *Phys. Rev. A* **54** 4741
[12] Li Y, Zhang K and Peng K 2004 *Phys. Lett. A* **324** 420
[13] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
[14] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev. A* **72** 022338
[15] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev. A* **72** 044301
[16] Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys. B: At., Mol. Opt. Phys.* **39** 1975
[17] Liu Y L, Man Z X and Xia Y J 2008 *Acta Phys Sin.* **57** 2680 (in Chinese)
[18] Zhang J X, Jing J T, Xie C D and Peng K C 2005 *Chin. Phys. Lett.* **22** 2751
[19] Muralidharan S and Panigrahi P K 2008 *Phys. Rev. A* **77** 032321

[20] Brown I D, Stepney S, Sudbery A and Braunstein S L 2005 *J. Phys. A: Math. Gen.* **38** 1119
[21] Nie Y Y, Sang M H, Li Y H and Liu J C 2011 *Int. J. Theor. Phys.* **50** 1367
[22] Muralidharan S, Jain S and Panigrahi P K 2011 *Opt. Commun.* **284** 1082
[23] Paul N, Menon J V, Karumanchi S, Muralidharan S and Panigrahi P K 2011 *Quantum Inf. Process.* **10** 619
[24] Han L F and Xu H F 2012 *Int. J. Theor. Phys.* **51** 2540
[25] Sun X M, Zha X W, Qi J X and Lan Q 2013 *Acta Phys Sin.* **62** 230302 (in Chinese)
[26] Jiang M and Dong D 2013 *Quantum Inf. Process.* **12** 237
[27] Wang M M, Wang W, Chen J G and Farouk A 2015 *Quantum Inf. Process.* **14** 4211
[28] Cao H and Ma W 2017 *IEEE Photon. J.* **9** 1
[29] Cao H and Ma W 2018 *IEEE Access* **6** 10453
[30] Song X, Liu Y, Xiao M, Deng H and Yang S 2020 *Quantum Inf. Process.* **19** 1
[31] Halpern J and Teague V 2004 *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, 2004, p. 623
[32] Kol G and Naor M 2008 *Proceedings of the fortieth annual ACM symposium on theory of computing*, 2008, p. 423
[33] Asharov G and Lindell Y 2009 *Annual International Cryptology Conference*, 2009, Springer, Berlin, Heidelberg, p. 559
[34] De S J and Ruj S 2016 *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, p. 925
[35] Vakilinia I and Sengupta S 2019 *IET Inf Secur.* **13** 530
[36] Chen Z, Tian Y and Peng C 2021 *Sci. China Life Sci.* **64** 1
[37] Maitra A, De S J, Paul G and Pal A K 2015 *Phys. Rev. A* **92** 022305
[38] Dou Z, Xu G, Chen X B, Liu X and Yang Y X 2018 *Sci. China Life Sci.* **61** 1
[39] Qin H, Tang W K S and Tso R 2018 *Sci. Rep.* **8** 1
[40] Nielsen M A and Chuang I 2002 *Quantum Inf. Comput.* **70** 558
[41] Wen Q Y, Qin S J and Gao F 2014 *J. Cryptol.* **1** 200
[42] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[43] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[44] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561