Lian et al. *EPJ Quantum Technology* (2023) 10:10
https://doi.org/10.1140/epjqt/s40507-023-00167-0

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Multi-party semiquantum private comparison of size relationship with *d*-dimensional Bell states

Jiang-Yuan Lian[1], Xia Li[1] and Tian-Yu Ye[1*]

*Correspondence:
happyyty@aliyun.com
[1]College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P.R. China

Abstract

In this paper, we utilize *d*-dimensional Bell states to construct a multi-party semiquantum private comparison (MSQPC) protocol with two supervisors, which can determine the size relationship of more than two classical users' private inputs under the control of two supervisors within one round implementation. The two supervisors, i.e., one quantum third party (TP) and one classical TP, are both semi-honest, which means that they can misbehave at their own wishes but are not permitted to conspire with anyone else. Neither quantum entanglement swapping nor unitary operations are required in the proposed MSQPC protocol. The security analysis certifies that the proposed MSQPC protocol can overcome both the outside attacks and the participant attacks.

Keywords: Multi-party semiquantum private comparison; *d*-dimensional Bell states; Semi-honest third party; Size relationship

1 Introduction

Classical secure multiparty computation (SMC) is one of the most important branches of classical cryptography whose security relies on the computational complexity of mathematical problems. As an important branch of SMC, the classical private comparison (CPC) aims to compare the size relationship of private inputs from different users. The first CPC protocol, which is usually named as "the millionaire problem", was put forward by Yao [1] in 1982. However, the security of this protocol is determined by the computation complexity of solving mathematical problems, which implies that this protocol may be threatened to a great extent once the computing ability of computer is tremendously improved. To get over this problem, a completely novel kind of private comparison, i.e., quantum private comparison (QPC), was invented by Yang and Wen [2] in 2009 by introducing quantum cryptography [3] into CPC. Since then, a series of QPC protocols [4–21] have been proposed in turn. These QPC protocols can be divided into two categories: QPC of equality [2, 4–13] and QPC of size relationship [14–21]. Different from QPC of equality, QPC of size relationship can judge whether the private input of one user is greater than, smaller

Springer

than or equal to that of another user. Generally speaking, QPC of size relationship is of more use than QPC of equality in practice.

In reality, not everyone is capable of affording expensive quantum devices. In order to overcome this issue, Boyer *et al.* [22] put forward the novel concept of semiquantumness in 2007. Within a semiquantum cryptography protocol, a classical participant, who only possesses limited quantum capabilities, is free of preparation and measurement of quantum superposition states and quantum entangled states. By absorbing semiquantumness into QPC, Chou *et al.* [23] constructed the first semiquantum private comparison (SQPC) protocol through utilizing entanglement swapping of Bell states. Hereafter, scholars put forward lots of SQPC protocols [24–34]. SQPC can be also divided into two kinds: SQPC of equality and SQPC of size relationship. The SQPC protocols of Refs. [23–29] belong to the former kind while the ones of Refs. [30–34] belong to the latter kind. However, each of the SQPC protocols of Refs. [30–34] only can determine the size relationship of private inputs from two users within one execution of protocol. There is few SQPC protocol of size relationship which is suitable for more than two users up to now.

Based on the above analysis, in this paper, we concentrate on considering the situation that N classical users aim to compare the size relationship of their private integer sequences under the control of two supervisors within one execution of protocol. In order to accomplish this goal, we put forward a novel multi-party semiquantum private comparison (MSQPC) protocol with two semi-honest third parties (TPs) by using d-dimensional Bell states. Here, two semi-honest TPs, i.e., a quantum TP and a classical TP, are the supervisors, each of whom is permitted to misbehave on her own but cannot conspire with anyone else [5]. Neither quantum entanglement swapping nor unitary operations are employed in the proposed MSQPC protocol.

2 Protocol description

In a d-dimensional quantum system, the Bell state can be denoted as

$$|\phi_{u,v}\rangle = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}} |t\rangle |t \oplus v\rangle, \tag{1}$$

where $u, v \in \{0, 1, \ldots, d-1\}$, and $\oplus$ represents the addition modulo d. In addition, the Z-basis in the d-dimensional quantum system can be represented by

$$T_1 = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{2}$$

Suppose that the classical user P_n owns a secret integer string $p_n = \{p_n^1, p_n^2, \ldots, p_n^L\}$, where $p_n^i \in \{0, 1, \ldots, h\}$, $h = \frac{d-1}{2}$, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. Here, since h needs to be greater than or equal to 1, d is an odd integer greater than or equal to 3. In addition, N classical users share a private key sequence $K = \{k_1, k_2, \ldots, k_L\}$ beforehand by virtue of the d-dimensional quantum system version of the secure mediated semiquantum key distribution (SQKD) protocol in Ref. [35], where $k_i \in \{0, 1, \ldots, d-1\}$ and $i = 1, 2, \ldots, L$. Note that the d-dimensional quantum system version of the mediated SQKD protocol in Ref. [35] can be derived after quantum TP generates the qudits randomly in the T_1 basis and then sends them out in Step *i*. Furthermore, there are two TPs, i.e., the quantum TP TP_1 and the classical TP TP_2, where TP_1 and TP_2 are allowed to impose any attack but cannot conspire

with others. The proposed MSQPC protocol with two supervisors is composed of the following steps. Here, the quantum channels used in the proposed protocol are assumed to be ideal.

Step 1: TP_1 generates N groups of $8L$ d-dimensional Bell states, where $\{|\phi_{u_n^1,v_n^1}\rangle, |\phi_{u_n^2,v_n^2}\rangle, \ldots, |\phi_{u_n^{8L},v_n^{8L}}\rangle\}$ denotes the nth group Bell states and $n = 1,2,\ldots,N$. TP_1 records the value of V_n, where $V_n = \{v_n^1, v_n^2, \ldots, v_n^{8L}\}$. Here, v_n^l is the second label of the lth Bell state in the nth group, $n = 1,2,\ldots,N$ and $l = 1,2,\ldots,8L$. Then, TP_1 makes the first particles of the nth group Bell states to form sequence S_n and the second particles of the nth group Bell states to form sequence M_n. Here, $S_n = \{S_n^1, S_n^2, \ldots, S_n^{8L}\}$, $M_n = \{M_n^1, M_n^2, \ldots, M_n^{8L}\}$, S_n^l is the first particle of the lth Bell state in the nth group, M_n^l is the second particle of the lth Bell state in the nth group, $n = 1,2,\ldots,N$ and $l = 1,2,\ldots,8L$. Afterward, TP_1 transmits S_n to P_n and keeps M_n on her hand, where $n = 1,2,\ldots,N$. Except the first particle, the next particle of S_n is sent out by TP_1 only after she obtains the previous one from TP_2.

Step 2: When receiving the lth particle of S_n, P_n randomly chooses one mode between the REFLECT mode and the MEASURE mode, where $l = 1,2,\ldots,8L$. Here, the REFLECT mode means that the receiver returns the received particle directly to the sender, while the MEASURE mode means that the receiver uses the T_1 basis to measure the received particle, generates a fresh particle in the same state as the received particle and sends the fresh particle back to the sender. P_n writes down her measurement results when choosing the MEASURE mode. Let $S_n' = \{S_n^{1'}, S_n^{2'}, \ldots, S_n^{8L'}\}$ denote the new sequence derived from P_n's operations on S_n, where $n = 1,2,\ldots,N$. Then, P_n transmits S_n' to TP_2.

Step 3: TP_2 also randomly chooses one mode between the REFLECT mode and the MEASURE mode for the lth particle of S_n', where $l = 1,2,\ldots,8L$. TP_2 also writes down her measurement results when selecting the MEASURE mode. Let $S_n'' = \{S_n^{1''}, S_n^{2''}, \ldots, S_n^{8L''}\}$ denote the new sequence derived from TP_2's operations on S_n', where $n = 1,2,\ldots,N$. Afterward, TP_2 transmits S_n'' to TP_1.

Step 4: After TP_1 receives all particles of S_n'' from TP_2, P_n and TP_2 announce their operation modes, respectively, where $n = 1,2,\ldots,N$. Then, TP_1, TP_2 and P_n take the corresponding actions according to Table 1.

Case 1: both P_n and TP_2 have entered into the REFLECT mode. TP_1 imposes the d-dimensional Bell basis measurement on particles $S_n^{l''}$ and M_n^l, where $l \in \{1,2,\ldots,8L\}$. Through the comparison of her measurement results and the corresponding initial prepared Bell states, TP_1 can know whether an eavesdropper is on line or not. If an eavesdropper is on line, the communication will be aborted;

Case 2: P_n and TP_2 have entered into the REFLECT mode and the MEASURE mode, respectively. TP_2 publishes the state of particle $S_n^{l''}$ to TP_1, while TP_1 adopts the T_1 basis

Table 1 Operations of TP_1, TP_2 and P_n under different Cases

Case	The mode of P_n	The mode of TP_2	The operations of P_n, TP_1 and TP_2
Case 1	The REFLECT mode	The REFLECT mode	TP_1 measures $S_n^{l''}$ and M_n^l with the d-dimensional Bell basis
Case 2	The REFLECT mode	The MEASURE mode	TP_2 publishes the state of $S_n^{l''}$; TP_1 measures $S_n^{l''}$ and M_n^l with the T_1 basis
Case 3	The MEASURE mode	The REFLECT mode	P_n publishes the state of $S_n^{l'}$; TP_1 measures $S_n^{l''}$ and M_n^l with the T_1 basis
Case 4	The MEASURE mode	The MEASURE mode	P_n publishes the state of $S_n^{l'}$; TP_2 publishes the state of $S_n^{l''}$; TP_1 measures $S_n^{l''}$ and M_n^l with the T_1 basis

to measure particle $S_n^{l''}$ and particle M_n^l, where $l \in \{1, 2, \ldots, 8L\}$. Through comparing her measurement results on the received particles of S_n'' in this Case, her measurement results on the corresponding particles in M_n and TP_2's publishments, TP_1 can know whether an eavesdropper is on line or not. If an eavesdropper is on line, the communication will be aborted;

Case 3: P_n and TP_2 have entered into the MEASURE mode and the REFLECT mode, respectively. P_n publishes the state of particle $S_n^{l'}$ to TP_1, while TP_1 adopts the T_1 basis to measure particle $S_n^{l''}$ and particle M_n^l, where $l \in \{1, 2, \ldots, 8L\}$. Through comparing her measurement results on the received particles of S_n'' in this Case, her measurement results on the corresponding particles in M_n and P_n's publishments, TP_1 can know whether an eavesdropper is on line or not. If an eavesdropper is on line, the communication will be aborted;

Case 4: both P_n and TP_2 have entered into the MEASURE mode. TP_1 randomly picks out half particles of S_n'' from the ones belonging to Case 4, and informs P_n and TP_2 of the chosen positions. For each chosen position, P_n and TP_2 publishes the states of particles $S_n^{l'}$ and $S_n^{l''}$, respectively, while TP_1 measures particle $S_n^{l''}$ and particle M_n^l with the T_1 basis, where $l \in \{1, 2, \ldots, 8L\}$. TP_1 can know whether an eavesdropper is on line or not by comparing her measurement results on these chosen particles of S_n'', her measurement results on the corresponding particles of M_n and the publishments from P_n and TP_2. If an eavesdropper is on line, the communication will be aborted.

Step 5: TP_1 counts the number of the remaining particles of S_n'' belonging to Case 4. If this number is less than L, the communication will be halted and restarted from Step 1.

P_n, TP_1 and TP_2 select the first L particles from the remaining ones of S_n'' belonging to Case 4 to accomplish private comparison. Let $s_n = \{s_n^1, s_n^2, \ldots, s_n^L\}$ denote the measurement results of S_n from P_n on these L chosen positions, where $s_n^i \in \{0, 1, \ldots, d-1\}$, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. Note that TP_1 and TP_2 can naturally know s_n. Then, P_n computes

$$f_n^i = p_n^i \oplus s_n^i \oplus k_i. \tag{3}$$

Finally, P_n sends f_n^i to TP_1 via an authenticated classical channel.

Step 6: TP_1 uses the T_1 basis to measure the L particles of M_n corresponding to the first L particles from the remaining ones of S_n'' belonging to Case 4 in Step 5, where $n = 1, 2, \ldots, N$. Let $m_n = \{m_n^1, m_n^2, \ldots, m_n^L\}$ represent TP_1's measurement results on these L particles of M_n, where $m_n^i \in \{0, 1, \ldots, d-1\}$ and $i = 1, 2, \ldots, L$. Then, TP_1 calculates

$$g_n^i = f_n^i \ominus m_n^i \oplus v_n^i. \tag{4}$$

Afterward, TP_1 computes

$$c_{nn'}^i = g_n^i \ominus g_{n'}^i, \tag{5}$$

where $n' = 1, 2, \ldots, N$ and $n' \neq n$. After that, TP_1 makes

$$y\left(c_{nn'}^i\right) = \begin{cases} -1, & \text{if } h < c_{nn'}^i \leq 2h; \\ 0, & \text{if } c_{nn'}^i = 0; \\ 1, & \text{if } 0 < c_{nn'}^i \leq h. \end{cases} \tag{6}$$

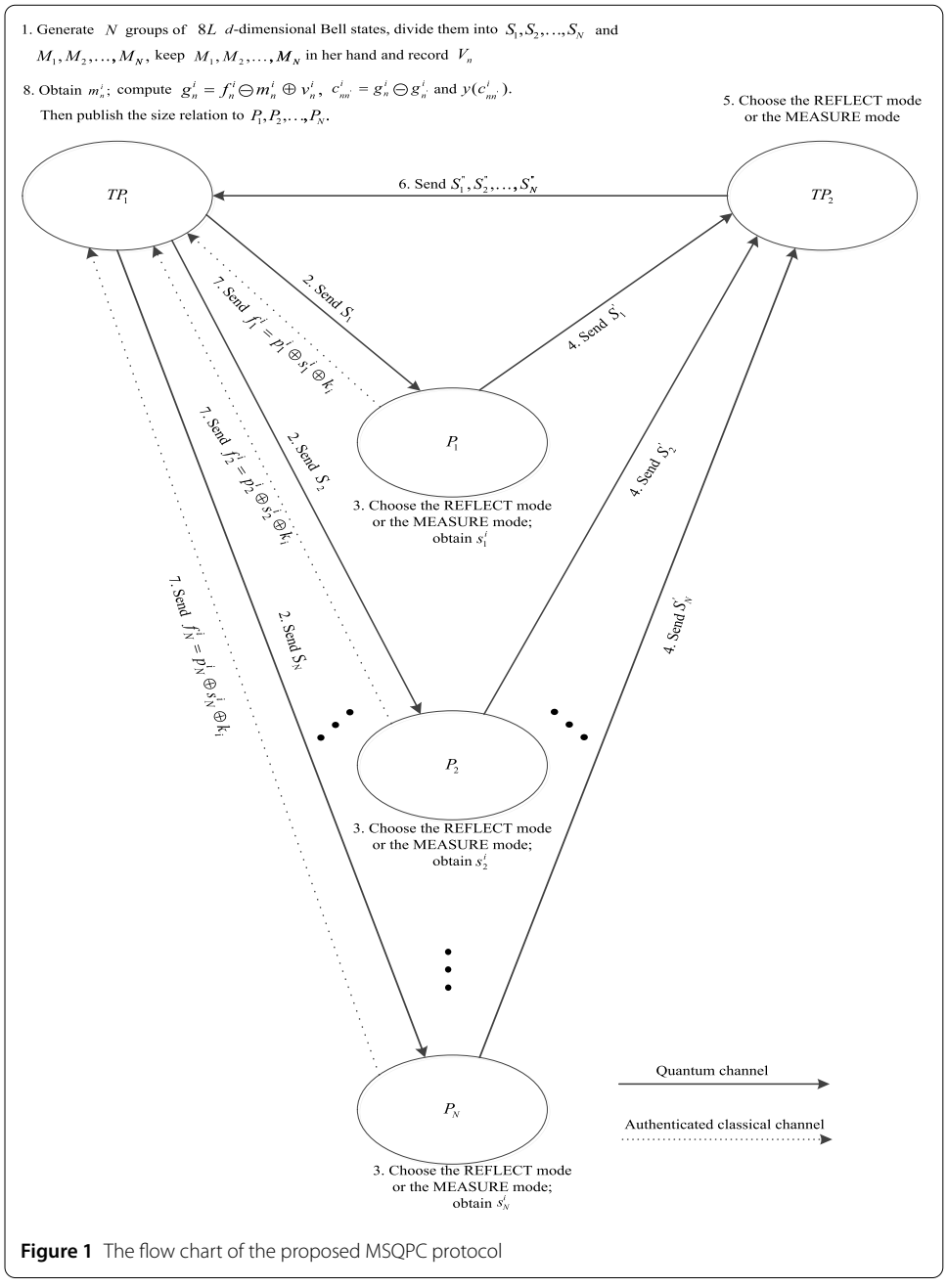

Figure 1 The flow chart of the proposed MSQPC protocol

Here, $y(c_{nn'}^i) = -1$ implies $p_n^i < p_{n'}^i$; $y(c_{nn'}^i) = 0$ implies $p_n^i = p_{n'}^i$; $y(c_{nn'}^i) = 1$ implies $p_n^i > p_{n'}^i$. Finally, TP_1 informs $P_1, P_2, \ldots, P_N$ of the final comparison results.

Now we finish the description of the procedure of the proposed MSQPC protocol. For clarity, we show its procedure in Fig. 1 after the processes of eavesdropping detection are neglected.

3 Correctness analysis

3.1 Output correctness

According to Eq. (1), a d-dimensional Bell state is collapsed into $|t\rangle|t \oplus v\rangle$ after its two particles are measured with the T_1 basis, where $t, v \in \{0, 1, \ldots, d-1\}$. Based on this, we

can infer

$$s_n^i \ominus m_n^i \oplus v_n^i = 0. \tag{7}$$

After inserting Eq. (3) into Eq. (4), we have

$$\begin{aligned} g_n^i &= f_n^i \ominus m_n^i \oplus v_n^i \\ &= \left(p_n^i \oplus s_n^i \oplus k_i\right) \ominus m_n^i \oplus v_n^i \\ &= s_n^i \ominus m_n^i \oplus v_n^i \oplus p_n^i \oplus k_i. \end{aligned} \tag{8}$$

According to Eq. (7) and Eq. (8), we can obtain

$$g_n^i = p_n^i \oplus k_i. \tag{9}$$

In the light of Eq. (5) and Eq. (9), we can calculate

$$\begin{aligned} c_{nn'}^i &= g_n^i \ominus g_{n'}^i \\ &= \left(p_n^i \oplus k_i\right) \ominus \left(p_{n'}^i \oplus k_i\right) \\ &= p_n^i \ominus p_{n'}^i. \end{aligned} \tag{10}$$

Here, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. In accordance with $p_n^i \in \{0, 1, \ldots, h\}$ and $h = \frac{d-1}{2}$, we can conclude from Eq. (6) and Eq. (10) that when $h < p_n^i \ominus p_{n'}^i \leq 2h$, i.e., $y(c_{nn'}^i) = -1$, it has $p_n^i < p_{n'}^i$; when $p_n^i \ominus p_{n'}^i = 0$, i.e., $y(c_{nn'}^i) = 0$, it has $p_n^i = p_{n'}^i$; when $0 < p_n^i \ominus p_{n'}^i \leq h$, i.e., $y(c_{nn'}^i) = 1$, it has $p_n^i > p_{n'}^i$. It can be concluded now that the comparison results of this protocol are accurate.

3.2 Examples

In order to further prove the output correctness of this protocol, a concrete example is given in detail. Suppose that $d = 13$, which implies $h = 6$; P_1, P_2, P_3, P_4 are four classical users; $p_1^1 = 4$, $p_2^1 = 5$, $p_3^1 = 0$, $p_4^1 = 4$; $k_1 = 10$; $v_1^1 = 4$, $v_2^1 = 7$, $v_3^1 = 6$, $v_4^1 = 2$ and $s_1^1 = 3$, $s_2^1 = 8$, $s_3^1 = 11$, $s_4^1 = 6$, which implies $m_1^1 = 7$, $m_2^1 = 2$, $m_3^1 = 4$, $m_4^1 = 8$. In accordance with Eq. (3), P_1, P_2, P_3, P_4 calculate $f_1^1 = 4 \oplus 3 \oplus 10 = 4$, $f_2^1 = 5 \oplus 8 \oplus 10 = 10$, $f_3^1 = 0 \oplus 11 \oplus 10 = 8$ and $f_4^1 = 4 \oplus 6 \oplus 10 = 7$, respectively. After receiving $f_1^1, f_2^1, f_3^1, f_4^1$, by virtue of Eq. (4), TP_1 obtains $g_1^1 = 4 \ominus 7 \oplus 4 = 1$, $g_2^1 = 10 \ominus 2 \oplus 7 = 2$, $g_3^1 = 8 \ominus 4 \oplus 6 = 10$ and $g_4^1 = 7 \ominus 8 \oplus 2 = 1$. Then, by using Eq. (5), TP_1 gets $c_{12}^1 = 1 \ominus 2 = 12$, $c_{13}^1 = 1 \ominus 10 = 4$, $c_{14}^1 = 1 \ominus 1 = 0$, $c_{23}^1 = 2 \ominus 10 = 5$, $c_{24}^1 = 2 \ominus 1 = 1$ and $c_{34}^1 = 10 \ominus 1 = 9$. Furthermore, based on Eq. (6), TP_1 can acquire $y(c_{12}^1) = -1$, $y(c_{13}^1) = 1$, $y(c_{14}^1) = 0$, $y(c_{23}^1) = 1$, $y(c_{24}^1) = 1$ and $y(c_{34}^1) = -1$, which means $p_1^1 < p_2^1$, $p_1^1 > p_3^1$, $p_1^1 = p_4^1$, $p_2^1 > p_3^1$, $p_2^1 > p_4^1$ and $p_3^1 < p_4^1$. In conclusion, it can be obtained that $p_3^1 < p_1^1 = p_4^1 < p_2^1$. We can draw the conclusion now that the comparison results of this example are right.

4 Security analysis

4.1 Outside attacks

In the following, we analyze three famous kinds of attack launched by an outside eavesdropper, Eve, who aims to obtain p_n, where $n = 1, 2, \ldots, N$.

(1) The intercept-resend attack

There are three kinds of intercept-resend attack need to be discussed.

Firstly, in Step 1, Eve intercepts the particle of S_n sent out from TP_1 and transmits P_n the fake one produced in the T_1 basis; then, in Step 2, Eve intercepts the particle of S'_n sent out from P_n and transmits TP_2 the intercepted original genuine particle of S_n. When both P_n and TP_2 choose the REFLECT mode, Eve leaves no trace for her attack and cannot be discovered in Step 4; when P_n and TP_2 choose the REFLECT mode and the MEASURE mode, respectively, the presence of Eve cannot be found in Step 4 either; when P_n and TP_2 choose the MEASURE mode and the REFLECT mode, respectively, the eavesdropping behavior of Eve can be discovered with the probability of $\frac{d-1}{d}$ in Step 4; when both P_n and TP_2 choose the MEASURE mode, the probability that P_n's measurement result on the fake particle from Eve is not same to TP_2's measurement result on the particle of S_n is $\frac{d-1}{d}$, and the probability that this particle position is chosen for security check is $\frac{1}{2}$, so the probability that Eve can be detected is $\frac{d-1}{2d}$ in Step 4.

Secondly, in Step 1, Eve intercepts the particle of S_n sent out from TP_1 and transmits P_n the fake one generated in the T_1 basis; then, in Step 3, Eve intercepts the particle of S''_n sent out from TP_2 and transmits TP_1 the intercepted original genuine particle of S_n. Considering that P_n chooses the REFLECT mode, when TP_2 chooses the REFLECT mode, Eve leaves no trace for her attack and cannot be discovered in Step 4; when TP_2 chooses the MEASURE mode, the eavesdropping behavior of Eve can be discovered with the probability of $\frac{d-1}{d}$ in Step 4. Considering that P_n chooses the MEASURE mode, when TP_2 chooses the REFLECT mode, the probability that Eve can be discovered is $\frac{d-1}{d}$ in Step 4; when TP_2 chooses the MEASURE mode, the probability that P_n's measurement result on the fake particle from Eve is not identical to TP_1's measurement result on the particle of S_n is $\frac{d-1}{d}$, and the probability that this particle position is chosen for security check is $\frac{1}{2}$, so the presence of Eve can be detected with the probability of $\frac{d-1}{2d}$ in Step 4.

Thirdly, in Step 2, Eve intercepts the particle of S'_n sent out from P_n and transmits TP_2 the fake one produced in the T_1 basis; then, in Step 3, Eve intercepts the particle of S''_n sent out from TP_2 and transmits TP_1 the intercepted original genuine particle of S'_n. Considering that TP_2 chooses the REFLECT mode, no matter what mode P_n chooses, the eavesdropping behavior of Eve cannot be discovered in Step 4. Considering that TP_2 chooses the MEASURE mode, when P_n chooses the REFLECT mode, the presence of Eve can be detected with the probability of $\frac{d-1}{d}$ in Step 4; when P_n chooses the MEASURE mode, the probability that P_n's measurement result on the particle of S_n is not identical to TP_2's measurement result on the fake particle from Eve is $\frac{d-1}{d}$, and the probability that this particle position is chosen for security check is $\frac{1}{2}$, so the probability that Eve can be discovered is $\frac{d-1}{2d}$ in Step 4.

In short, Eve cannot acquire any useful information without being detected by launching the intercept-resend attack.

(2) The measure-resend attack

Eve intercepts the particle of $S_n/S'_n/S''_n$ sent out from $TP_1/P_n/TP_2$, employs the T_1 basis to measure it and transmits $P_n/TP_2/TP_1$ the resulted state. If at least one of P_n and TP_2 chooses the MEASURE mode, the eavesdropping behavior of Eve cannot be detected. Considering that both P_n and TP_2 choose the REFLECT mode, the measurement of Eve destroys the entanglement of two qudits within a d-dimensional Bell state, which makes her presence be discovered with the probability of $\frac{d-1}{d}$.

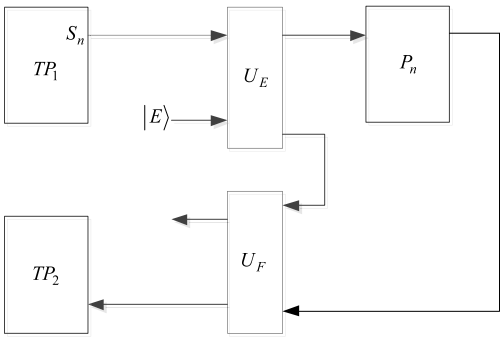

Figure 2 Eve's entangle-measure attack with U_E and U_F

To sum up, when Eve performs the measure-resend attack on the transmitted particle, she cannot get any useful information without being discovered.

(3) The entangle-measure attack

Eve may launch her entangle-measure attack shown in Fig. 2: she performs the unitary operation U_E on the particle of S_n sent out from TP_1 in Step 1 and imposes the unitary operation U_F on the particle of S'_n sent out from P_n in Step 2, where a common probe space is shared by U_E and U_F with the initial state $|E\rangle$. As illustrated in Ref. [22], the shared probe permits Eve to launch the attack on the particle of S'_n in accordance with the knowledge gained from U_E.

Theorem 1 *Suppose that Eve performs U_E on the particle of S_n sent out from TP_1 in Step* 1 *and imposes U_F on the particle of S'_n sent out from P_n in Step* 2*. In order to incur no error in Step* 4*, the final state of Eve's probe should be independent of not only the operation of P_n, TP_2 and TP_1 but also their measurement results. Consequently, Eve has no knowledge about s_n.*

Proof According to Ref. [31], the effect of U_E on the particle prepared in the T_1 basis and Eve's probe can be described as

$$U_E\big(|t\rangle|E\rangle\big) = \sum_{t'=0}^{d-1} \alpha_{tt'} \big|t'\big\rangle|\varepsilon_{tt'}\rangle. \tag{11}$$

Here, the probe $|\varepsilon_{tt'}\rangle$ are decided by U_E, $\sum_{t'=0}^{d-1} |\alpha_{tt'}|^2 = 1$ and $t = 0, 1, \ldots, d-1$. When Eve performs U_E on the particle of S_n sent out from TP_1 in Step 1, we have

$$U_E\big(|\phi_{u,v}\rangle|E\rangle\big) = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}} U_E\big(|t\rangle|E\rangle\big)|t \oplus v\rangle. \tag{12}$$

After inserting Eq. (11) into Eq. (12), we have

$$\begin{aligned} U_E\big(|\phi_{u,v}\rangle|E\rangle\big) &= \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}} \left(\sum_{t'=0}^{d-1} \alpha_{tt'} \big|t'\big\rangle|\varepsilon_{tt'}\rangle \right)|t \oplus v\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{t'=0}^{d-1} \big|t'\big\rangle \left(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}} \alpha_{tt'} |t \oplus v\rangle|\varepsilon_{tt'}\rangle \right). \end{aligned} \tag{13}$$

Firstly, consider the situation that P_n chooses the MEASURE mode for the particle of S_n sent out from TP_1. Consequently, in accordance with Eq. (13), the whole quantum system is collapsed into $|t'\rangle(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}}\alpha_{tt'}|t\oplus v\rangle|\varepsilon_{tt'}\rangle)$ when the measurement result of P_n is $|t'\rangle$, where $t' = 0, 1, \ldots, d-1$.

Eve imposes U_F on the particle of S'_n sent out from P_n. In order that Eve's attacks cannot be detected in Step 4, no matter what mode TP_2 chooses for the particle of S'_n sent out from P_n, the whole quantum system should be

$$U_F\left[|t'\rangle\left(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}}\alpha_{tt'}|t\oplus v\rangle|\varepsilon_{tt'}\rangle\right)\right] = e^{\frac{2\pi it'u}{d}}|t'\rangle|t'\oplus v\rangle|\varepsilon_{t'}\rangle, \tag{14}$$

when the measurement result of P_n is $|t'\rangle$.

Secondly, consider the situation that P_n chooses the REFLECT mode for the particle of S_n sent out from TP_1. As a result, the whole quantum system after the operation of P_n is $\frac{1}{\sqrt{d}}\sum_{t'=0}^{d-1}|t'\rangle(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}}\alpha_{tt'}|t\oplus v\rangle|\varepsilon_{tt'}\rangle)$.

Eve imposes U_F on the particle of S'_n sent out from P_n. Assume that TP_2 also chooses the REFLECT mode for the particle of S'_n sent out from P_n. As a result, the whole quantum system after the operation of TP_2 is

$$\begin{aligned} U_F\left[U_E\left(|\phi_{u,v}\rangle|E\rangle\right)\right] &= U_F\left[\frac{1}{\sqrt{d}}\sum_{t'=0}^{d-1}|t'\rangle\left(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}}\alpha_{tt'}|t\oplus v\rangle|\varepsilon_{tt'}\rangle\right)\right] \\ &= \frac{1}{\sqrt{d}}\sum_{t'=0}^{d-1} U_F\left[|t'\rangle\left(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}}\alpha_{tt'}|t\oplus v\rangle|\varepsilon_{tt'}\rangle\right)\right]. \end{aligned} \tag{15}$$

Inserting Eq. (14) into Eq. (15) produces

$$U_F\left[U_E\left(|\phi_{u,v}\rangle|E\rangle\right)\right] = \frac{1}{\sqrt{d}}\sum_{t'=0}^{d-1} e^{\frac{2\pi it'u}{d}}|t'\rangle|t'\oplus v\rangle|\varepsilon_{t'}\rangle. \tag{16}$$

For Eve's attacks not being discovered in Step 4, the probability that the measurement result of TP_1 is $|\phi_{u,v}\rangle$ should be 1. Thus, it can be derived from Eq. (1) and Eq. (16) that

$$|\varepsilon_0\rangle = |\varepsilon_1\rangle = \cdots = |\varepsilon_{d-1}\rangle = |\varepsilon\rangle. \tag{17}$$

Inserting Eq. (17) into Eq. (14) generates

$$U_F\left[|t'\rangle\left(\sum_{t=0}^{d-1} e^{\frac{2\pi itu}{d}}\alpha_{tt'}|t\oplus v\rangle|\varepsilon_{tt'}\rangle\right)\right] = e^{\frac{2\pi it'u}{d}}|t'\rangle|t'\oplus v\rangle|\varepsilon\rangle. \tag{18}$$

Inserting Eq. (17) into Eq. (16) generates

$$U_F\left[U_E\left(|\phi_{u,v}\rangle|E\rangle\right)\right] = |\phi_{u,v}\rangle|\varepsilon\rangle. \tag{19}$$

Thirdly, consider the situation that P_n chooses the REFLECT mode for the particle of S_n sent out from TP_1, while TP_2 chooses the MEASURE mode for the particle of S'_n sent

out from P_n. It is easy to find that as long as Eq. (19) stands, Eve naturally leaves no trace in this situation and cannot be detected in Step 4.

It can be concluded from Eq. (18) and Eq. (19) that, when Eve performs U_E on the particle of S_n sent out from TP_1 in Step 1 and imposes U_F on the particle of S'_n sent out from P_n in Step 2, in order to incur no error in Step 4, the final state of Eve's probe should be independent of not only the operation of P_n, TP_2 and TP_1 but also their measurement results. Consequently, Eve has no knowledge about s_n.

On the other hand, Eve may launch other two entangle-measure attacks: (1) Eve imposes U_E on the particle sent out from P_n and imposes U_F on the particle sent out from TP_2; (2) Eve performs U_E on the particle sent out from TP_1 and performs U_F on the particle sent out from TP_2. We can prove in a similar way to the above deduction and conclude that Eve still has no way to acquire any useful information about s_n under these two circumstances. □

4.2 Participant attacks

In the following, we analyze the security of this protocol towards the participant attack, which was first discovered by Gao *et al.* [36] in 2007.

(1) The participant attack from one dishonest user

In this protocol, $P_1, P_2, \ldots, P_N$ act equally. Here, we suppose that P_1 is the only dishonest user aiming to get P_a's secret integer string p_a, where $a = 2, 3, \ldots, N$. In order to achieve this goal, P_1 may launch her different attacks on $S_a/S'_a/S''_a$ sent out from $TP_1/P_a/TP_2$. However, P_1 is independent from TP_1, TP_2 and P_a, which makes her actually act as an outside eavesdropper. According to Sect. 4.1, P_1 has no chance to acquire p_a without being discovered.

In addition, P_1 may get f_a^i sent out from P_a in Step 5, but she has no way to infer out p_a^i, because she cannot acquire s_a^i. Furthermore, although TP_1 informs P_1 of the final comparison results in Step 6, P_1 still has no opportunity to acquire p_a^i. Here, $a = 2, 3, \ldots, N$ and $i = 1, 2, \ldots, L$.

(2) The participant attack from more than one dishonest user

The worst case is that the number of dishonest users is $N - 1$. Assume that the $N - 1$ dishonest users are $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$, colluding together to extract p_b, where $b = 2, 3, \ldots, N - 1$. It is obvious that the union of $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ is independent from TP_1, TP_2 and P_b. $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may implement their attacks on $S_b/S'_b/S''_b$ sent out from $TP_1/P_b/TP_2$. However, they essentially play the role of an outside eavesdropper and are undoubtedly detected according to Sect. 4.1.

Besides, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may get f_b^i sent out from P_b in Step 5. But they have no knowledge about s_b^i so that they have no way to infer out p_b^i. Furthermore, although TP_1 informs $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ of the final comparison results in Step 6, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ still has no opportunity to acquire p_b^i. Here, $b = 2, 3, \ldots, N - 1$ and $i = 1, 2, \ldots, L$.

(3) The participant attack from TP_1

TP_1 is assumed to be semi-honest in this protocol. On one hand, TP_1 obtains f_n^i from P_n in Step 5, where $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. However, due to lack of k_i, TP_1 cannot extract p_n^i based on f_n^i and s_n^i. On the other hand, TP_1 obtains the final comparison results in Step 6. Unfortunately, it is useless for her to acquire p_n^i.

(4) The participant attack from TP_2

TP_2 is assumed to be semi-honest in this protocol. TP_2 may receive f_n^i from P_n in Step 5, but she has no way to acquire p_n^i based on f_n^i and s_n^i, being short of k_i. In addition, although the final comparison results may be received by TP_2 from TP_1 in Step 6, she still has no opportunity to acquire p_n^i. Here, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$.

5 Discussions and conclusions

As this protocol is achieved in the d-dimensional quantum system, here we adopt the qudit efficiency defined in Eq. (20) [31] to evaluate its efficiency:

$$\eta = \frac{x}{y + z}, \tag{20}$$

where x, y and z are the length of compared private integer string, the number of consumed qudits and the length of required classical information, respectively. Note that we do not consider the classical resources required for eavesdropping detections.

In this protocol, the length of p_n is L, which implies $x = L$. TP_1 produces N groups of $8L$ d-dimensional Bell states, lets the first particles of the nth group Bell states make up S_n and the second particles of the nth group Bell states make up M_n, and transmits S_n to P_n; after receiving S_n from TP_1, when P_n chooses the MEASURE mode, she produces $4L$ fresh qudits; after receiving S_n' from P_n, TP_2 produces $4L$ fresh qudits when she chooses the MEASURE mode; here, $n = 1, 2, \ldots, N$; $P_1, P_2, \ldots, P_N$ share K in advance through the d-dimensional quantum system version of the secure mediated SQKD protocol in Ref. [35], which consumes $4L(2^N + \delta) + 2L(2^N + \delta) \times N$ qudits; so it has $y = (16L + 4L + 4L) \times N + 4L(2^N + \delta) + 2L(2^N + \delta) \times N = 24NL + 2L(N + 2)(2^N + \delta)$. Furthermore, P_n transmit f_n^i to TP_1, where $i = 1, 2, \ldots, L$, so it has $z = L \times N = NL$. Hence, this protocol's qudit efficiency is $\eta = \frac{L}{24NL+2L(N+2)(2^N+\delta)+NL} = \frac{1}{25N+2(N+2)(2^N+\delta)}$.

This protocol is further compared with the SQPC protocols of size relationship in Refs. [30–34], as listed in Table 2. By virtue of Table 2, we can conclude that this protocol takes advantage over the protocol of Ref. [34] in quantum resource, as the preparation of d-dimensional Bell state is easier than d-dimensional GHZ state; as for the usage of unitary operation, this protocol exceeds the second protocol of Ref. [32]; this protocol defeats the protocol of Ref. [34] in TP's quantum measurement, due to no use of d-dimensional GHZ state measurements; and this protocol is the only one which can obtain the size relationship of more than two classical users' secret integer strings within one round execution.

In addition, if we make all Bell states generated by TP_1 in Step 1 be $|\phi_{00}\rangle$, which implies to eliminate the need for V_n, the modified protocol will be much simpler. However, we do not intend to do this, because the corresponding protocol with all Bell states generated by TP_1 in the state of $|\phi_{00}\rangle$ is just the special version of the proposed protocol with $u_n^l = 0$ and $v_n^l = 0$ for $n = 1, 2, \ldots, N$ and $l = 1, 2, \ldots, 8L$.

Furthermore, in the proposed protocol, P_n, TP_1 and TP_2 share s_n through quantum technology first; and then, P_n and TP_1 conduct private comparison by using the classical method. P_n obtains s_n under the control of both TP_1 and TP_2. The generation of s_n can be regarded as the SQKD process where TP_1 and TP_2 cooperate to distribute s_n to P_n. If we make P_n and TP_1 directly share the key s_n using SQKD technology, and then implement the private comparison, the same correct private comparison results also can be derived. However, this alternative protocol doesn't need the presence of TP_2, which

Table 2 Comparison results between this protocol and previous SQPC protocols of size relationship

	Quantum resource	Number of users	Number of TP	Type of TP	Usage of unitary operation	Usage of quantum entanglement swapping	Usage of pre-shared key	Classical users' quantum measurement	TP's knowledge about the comparison result	TP's quantum measurement
The protocol of Ref. [30]	d-dimensional Bell states	2	1	Semi-honest	No	No	Yes	d-dimensional single-particle measurements	Yes	d-dimensional Bell state measurements and d-dimensional single-particle measurements
The protocol of Ref. [31]	d-dimensional single-particle states	2	1	Semi-honest	No	No	Yes	d-dimensional single-particle measurements	No	d-dimensional single-particle measurements
The first protocol of Ref. [32]	d-dimensional single-particle states	2	1	Semi-honest	No	No	Yes	d-dimensional single-particle measurements	Yes	d-dimensional single-particle measurements
The second protocol of Ref. [32]	d-dimensional single-particle states	2	1	Semi-honest	Yes	No	Yes	d-dimensional single-particle measurements	Yes	d-dimensional single-particle measurements
The protocol of Ref. [33]	d-dimensional Bell states	2	1	Semi-honest	No	No	Yes	No	Yes	d-dimensional Bell state measurements and d-dimensional single-particle measurements
The protocol of Ref. [34]	d-dimensional GHZ states	2	1	Semi-honest	No	No	Yes	d-dimensional single-particle measurements	Yes	d-dimensional GHZ state measurements, d-dimensional Bell state measurements and d-dimensional single-particle measurements
This protocol	d-dimensional Bell states	N	2	Semi-honest	No	No	Yes	d-dimensional single-particle measurements	Yes	d-dimensional Bell state measurements and d-dimensional single-particle measurements

violates the aim of the proposed protocol, i.e., only under the permissions of both TP_1 and TP_2 can $P_1, P_2, \ldots, P_N$ determine the size relationship of their private integer strings within one round execution.

To sum up, we construct a novel MSQPC protocol with two supervisors in this paper with d-dimensional Bell states, which aims to determine the size relationship of more than two classical users' private integer strings under the control of two supervisors within one round execution. In other words, only under the permissions of both supervisors can the goal of this protocol be achieved. The two supervisors, i.e., one quantum TP and one classical TP, are both allowed to perform arbitrary attacks but cannot cooperate with anyone else. Both outside attacks and the participant attacks can be resisted by this protocol. Neither quantum entanglement swapping nor unitary operations are needed.

As far as the current technology is concerned, errors are possible in quantum communication with a certain probability, due to the presence of noise. In the paper, we are devoted to designing a theoretically feasible MSQPC protocol with two supervisors. The quantum channels of the proposed protocol are assumed to be ideal, so the possibility of introducing errors in quantum communication is not considered here. Because how to evaluate the influence of noise in quantum communication is very complicated, we will study this point in future.

In addition, how to apply SQKD with two degrees of freedom [37, 38] into SQPC [39, 40] is also worth of studying. How to convert SQPC into semiquantum summation [41, 42] and Semiquantum secret sharing [43] is also valuable to study.

Acknowledgements
The authors would like to thank the anonymous reviewers for their valuable comments that help enhancing the quality of this paper.

Funding
The National Natural Science Foundation of China (Grant No.62071430 and No.61871347) and the Fundamental Research Funds for the Provincial Universities of Zhejiang (Grant No.JRK21002).

Availability of data and materials
The datasets used during the current study are available from the corresponding author on reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable

Consent for publication
Not applicable

Competing interests
The authors declare no competing interests.

Author contributions
Jiang-Yuan Lian designed the protocol, conducted partial security analysis and wrote the manuscript; Xia Li conducted partial security analysis; and Tian-Yu Ye checked the protocol and the whole security analysis and reviewed the paper

Received: 11 December 2022 Accepted: 10 April 2023 Published online: 19 April 2023

References

1. Yao AC. Protocols for secure computations. In: Proc. of the 23rd annual IEEE symposium on foundations of computer science. 1982. p. 160–4.
2. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A, Math Theor. 2009;42(5):055305.
3. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE international conference on computers, systems and signal processing. Bangalore. 1984. p. 175–9.

4. Tseng HY, Lin J, Hwang T. New quantum private comparison protocol using EPR pairs. Quantum Inf Process. 2012;11:373–84.
5. Yang YG, Xia J, Jia X, Zhang H. Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf Process. 2013;12:877–85.
6. Ji ZX, Ye TY. Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun Theor Phys. 2016;65(6):711–5.
7. Ye TY. Multi-party quantum private comparison protocol based on entanglement swapping of Bell entangled states. Commun Theor Phys. 2016;66(3):280–90.
8. Ye TY. Quantum private comparison via cavity QED. Commun Theor Phys. 2017;67(2):147–56.
9. Ye TY, Ji ZX. Two-party quantum private comparison with five-qubit entangled states. Int J Theor Phys. 2017;56(5):1517–29.
10. Ye TY, Ji ZX. Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. Sci China, Phys Mech Astron. 2017;60(9):090312.
11. Ji ZX, Ye TY. Multi-party quantum private comparison based on the entanglement swapping of *d*-level Cat states and *d*-level Bell states. Quantum Inf Process. 2017;16(7):177.
12. Ye CQ, Ye TY. Circular multi-party quantum private comparison with *n*-level single-particle states. Int J Theor Phys. 2019;58:1282–94.
13. Ye TY, Hu JL. Multi-party quantum private comparison based on entanglement swapping of Bell entangled states within *d*-level quantum system. Int J Theor Phys. 2021;60(4):1471–80.
14. Lin S, Sun Y, Liu XF, Yao ZQ. Quantum private comparison protocol with *d*-dimensional Bell states. Quantum Inf Process. 2013;12:559–68.
15. Guo FZ, Gao F, Qin SJ, Zhang J, Wen QY. Quantum private comparison protocol based on entanglement swapping of *d*-level Bell states. Quantum Inf Process. 2013;12(8):2793–802.
16. Luo QB, Yang GW, She K, Niu WN, Wang YQ. Multi-party quantum private comparison protocol based on *d*-dimensional entangled states. Quantum Inf Process. 2014;13:2343–52.
17. Ye CQ, Ye TY. Multi-party quantum private comparison of size relation with *d*-level single-particle states. Quantum Inf Process. 2018;17(10):252.
18. Song X, Wen A, Gou R. Multiparty quantum private comparison of size relation based on single-particle states. IEEE Access. 2019;99:1–7.
19. Cao H, Ma WP, Lü LD, He YF, Liu G. Multi-party quantum comparison of size based on *d*-level GHZ states. Quantum Inf Process. 2019;18:287.
20. Chen FL, Zhang H, Chen SG, Cheng WT. Novel two-party quantum private comparison via quantum walks on circle. Quantum Inf Process. 2021;20(5):1–19.
21. Wang B, Gong LH, Liu SQ. Multi-party quantum private size comparison protocol with *d*-dimensional Bell states. Front Phys. 2022;10:981376.
22. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett. 2007;99(14):140501.
23. Chou WH, Hwang T, Gu J. Semi-quantum private comparison protocol under an almost-dishonest third party. 2016. https://arxiv.org/abs/1607.07961.
24. Ye TY, Ye CQ. Measure-resend semi-quantum private comparison without entanglement. Int J Theor Phys. 2018;57(12):3819–34.
25. Thapliyal K, Sharma RD, Pathak A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Int J Quantum Inf. 2018;16(5):1850047.
26. Lang YF. Semi-quantum private comparison using single photons. Int J Theor Phys. 2018;57:3048–55.
27. Lin PH, Hwang T, Tsai CW. Efficient semi-quantum private comparison using single photons. Quantum Inf Process. 2019;18:207.
28. Jiang LZ. Semi-quantum private comparison based on Bell states. Quantum Inf Process. 2020;19:180.
29. Ye CQ, Li J, Chen XB, Yuan T. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. Quantum Inf Process. 2021;20:262.
30. Zhou NR, Xu QD, Du NS, Gong LH. Semi-quantum private comparison protocol of size relation with *d*-dimensional Bell states. Quantum Inf Process. 2021;20:124.
31. Geng MJ, Xu TJ, Chen Y, Ye TY. Semiquantum private comparison of size relationship based *d*-level single-particle states. Sci China, Ser G, Phys Mech Astron. 2022;52(9):290311.
32. Li YC, Chen ZY, Xu QD, Gong LH. Two semi-quantum private comparison protocols of size relation based on single particles. Int J Theor Phys. 2022;61:157.
33. Luo QB, Li XY, Yang GW, Lin C. A mediated semi-quantum protocol for millionaire problem based on high-dimensional Bell states. Quantum Inf Process. 2022;21:257.
34. Wang B, Liu SQ, Gong LH. Semi-quantum private comparison protocol of size relation with *d*-dimensional GHZ states. Chin Phys B. 2022;31:010302.
35. Zhang XZ, Gong WG, Tan YG, Ren ZZ, Guo XT. Quantum key distribution series network protocol with *M*-classical Bobs. Chin Phys B. 2009;18(6):2143.
36. Gao F, Qin SJ, Wen QY, Zhu FC. A simple participant attack on the Bradler-Dusek protocol. Quantum Inf Comput. 2007;7:329.
37. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. Quantum Inf Process. 2022;21(4):123.
38. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. Int J Theor Phys. 2020;59(9):2807.
39. Ye TY, Lian JY. A novel multi-party semiquantum private comparison protocol of size relationship with *d*-dimensional single-particle states. Physica A. 2023;611:128424.
40. Geng MJ, Chen Y, Xu TJ, Ye TY. Single-state semiquantum private comparison based on Bell states. EPJ Quantum Technol. 2022;9:36.
41. Ye TY, Xu TJ, Geng MJ, Ying C. Two-party secure semiquantum summation against the collective-dephasing noise. Quantum Inf Process. 2022;21:118.

42. Hu JL, Ye TY. Three-party secure semiquantum summation without entanglement among quantum user and classical users. Int J Theor Phys. 2022;61(6):170.
43. Chen Y, Ye TY. Semiquantum secret sharing by using χ-type states. Eur Phys J Plus. 2022;137(12):1331.

Publisher's Note