


# Multi-party semi-quantum private comparison protocol of size relation based on two-dimensional Bell states

Bing Wang(王冰), Li-Hua Gong(龚黎华), and San-Qiu Liu(刘三秋)

**Citation:**Chin. Phys. B, 2024, 33 (**11**): 110303. DOI: 10.1088/1674-1056/ad73ae
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

---

## Measurement-device-independent quantum secret sharing with hyper-encoding

Xing-Xing Ju(居星星), Wei Zhong(钟伟), Yu-Bo Sheng(盛宇波), and Lan Zhou(周澜)
Chin. Phys. B, 2022, 31 (**10**): 100302. DOI: 10.1088/1674-1056/ac70bb

## Semi-quantum private comparison protocol of size relation with *d*-dimensional GHZ states

Bing Wang(王冰), San-Qiu Liu(刘三秋), and Li-Hua Gong(龚黎华)
Chin. Phys. B, 2022, 31 (**1**): 010302. DOI: 10.1088/1674-1056/ac1413

## Measurement-device-independent quantum cryptographic conferencing with an untrusted source

Rui-Ke Chen(陈瑞柯), Wan-Su Bao(鲍皖苏), Yang Wang(汪洋), Hai-Ze Bao(包海泽), Chun Zhou(周淳), Mu-Sheng Jiang(江木生), Hong-Wei Li(李宏伟)
Chin. Phys. B, 2017, 26 (**1**): 010302. DOI: 10.1088/1674-1056/26/1/010302

## Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad

Zhi-Hao Liu(刘志昊), Han-Wu Chen(陈汉武)
Chin. Phys. B, 2016, 25 (**8**): 080308. DOI: 10.1088/1674-1056/25/8/080308

## Quantum dual signature scheme based on coherent states with entanglement swapping

Jia-Li Liu(刘佳丽), Rong-Hua Shi(施荣华), Jin-Jing Shi(石金晶), Ge-Li Lv(吕格莉), Ying Guo(郭迎)
Chin. Phys. B, 2016, 25 (**8**): 080306. DOI: 10.1088/1674-1056/25/8/080306

---

# Multi-party semi-quantum private comparison protocol of size relation based on two-dimensional Bell states

Bing Wang(王冰)[1,2], Li-Hua Gong(龚黎华)[1,3], and San-Qiu Liu(刘三秋)[1,2,†]

[1] *Jiangxi Province Key Laboratory of Fusion and Information Control, Department of Physics, Nanchang University, Nanchang* 330031, *China*
[2] *School of Physics and Materials, Nanchang University, Nanchang* 330031, *China*
[3] *Department of Electronic Information Engineering, Nanchang University, Nanchang* 330031, *China*

(Received 27 March 2024; revised manuscript received 15 August 2024; accepted manuscript online 27 August 2024)

Currently, all quantum private comparison protocols based on two-dimensional quantum states can only compare equality, via using high-dimensional quantum states that it is possible to compare the size relation in existing work. In addition, it is difficult to manipulate high-dimensional quantum states under the existing conditions of quantum information processing, leading to low practicality and engineering feasibility of protocols for comparing size relation. Considering this situation, we propose an innovative protocol. The proposed protocol can make size comparison by exploiting more manageable two-dimensional Bell states, which significantly enhances its feasibility with current quantum technologies. Simultaneously, the proposed protocol enables multiple participants to compare their privacies with the semi-quantum model. The communication process of the protocol is simulated on the IBM Quantum Experience platform to verify its effectiveness. Security analysis shows that the proposed protocol can withstand common attacks while preserving the privacies of all participants. Thus, the devised protocol may provide an important reference for implementation of quantum private size comparison protocols.

**Keywords:** two-dimensional Bell state, size relation, multi-party, semi-quantum private comparison

**PACS:** 03.67.Dd, 03.67.Hk, 03.67.–a, 03.67.Ac **DOI:** 10.1088/1674-1056/ad73ae

## 1. Introduction

Quantum private comparison (QPC) refers to the fact that two or more participants holding privacies can confirm the size relation of their privacies by executing a quantum cryptographic protocol without disclosing their own privacies. It is a special case of quantum secure multiparty computation, which originates from Yao's millionaire problem.[1] To address Yao's millionaire problem, Boudot *et al.* designed a protocol to determine whether or not two millionaires are equally rich.[2] However, the introduction of a third-party in the QPC protocol became necessary after Mayers,[3] Lo[4] and Colbeck[5] demonstrated independently that it is impossible to construct a secure two-party protocol with comparison function. In the existing protocols, the third party, often involving to help the participants achieve private comparison, may be completely honest,[6] malicious dishonest,[7,8] or semi-honest.[9–11] Therein, the semi-honest third party (STP) does not conspire with others despite having curiosity about participants' privacies but attempts to deduce them from available information. QPC protocols have been found for many applications in quantum auction,[12,13] quantum multi-party summation,[14] anonymous voting.[15,16] Generally, the QPC protocols can be broadly categorized into two cases, one is to compare the equality of the participants' privacies (QPCE),[17–19] and the other is to compare the size relation (QPCS). The latter is more versatile and has led to the proposal of various QPCS protocols based on the high-dimensional quantum states over the past decade, where high dimension means that the quantum state has a dimension greater than two.

Jia *et al.* introduced the first QPCS protocol,[11] where the participants' privacies were encrypted into the phases of the $d$-dimensional entangled states by local operations and an STP performed collective measurement on each $d$-dimensional entangled state. Based on these measurements, STP can be used to determine the size relation between two participants' privacies. In 2013, Lin *et al.* presented a new QPCS protocol based on the $d$-dimensional Bell states.[20] Several other QPCS protocols were put forth by using the high-dimensional quantum states in the same year.[21–23] However, the QPCS protocols mentioned above can only make private comparison between two participants. Fortunately, Luo *et al.* designed the first multi-party QPCS protocol,[24] in which STP prepares and sends the $d$-dimensional maximally entangled states, while each participant needs to measure the $d$-dimensional quantum states. In 2018, Ye *et al.* also put forward two novel multi-party QPCS protocols with the $d$-dimensional single-particles.[25] Henceforth, the multi-party QPCS protocols attracted increasing attention.[26–28]

Boyer *et al.* proved that cryptographic protocol can be unconditional security with quantum resources or operators as few as possible. Based on this, they put forward a semi-quantum theorical model.[29,30] In the semi-quantum model, quantum party is generally thought to have powerful quantum

[†]Corresponding author. E-mail: sqlgroup@ncu.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd 

ability to prepare and control the quantum states with quantum devices, while classical party has a limited or no quantum ability to perform only some restricted quantum or classical operations.[31] Due to its high practicability, the QPC protocols based on the semi-quantum model (SQPC) have been widely investigated in recent years. In 2021, Zhou *et al.* came up with the first two-party SQPC protocol to compare the size relation (SQPCS) by considering the $d$-dimensional Bell states as information carriers.[32] Luo *et al.* also proposed a novel two-party SQPCS protocol based on the $d$-dimensional Bell states in 2022.[33] Later, several SQPCS protocols have been designed all depending on the high-dimensional quantum states.[34–36]

As we can see, all size comparison protocols rely on the high-dimensional quantum states. However, it is quite difficult to prepare, send, and especially measure the high-dimensional quantum state during experiments now.[37] Therefore, there are serious constraints on the practical applications of such protocols. Furthermore, we found that all the protocols based on the two-dimensional quantum states can only compare the equality.[38–40] Considering this, we propose a brand-new multi-party SQPCS protocol with the following advantages: (1) The designed protocol can determine the size relation just only with more manageable two-dimensional Bell state. (2) Our protocol enables multiple participants to compare their privacies based on the semi-quantum model. (3) The communication processes of the proposed protocol are simulated on the IBM Quantum Experience[41] to further demonstrate its feasibility.

The rest is organized as follows: In Section 2, the preliminaries are introduced. In Sections 3 and 4, the multi-party SQPCS protocol with the analysis of correctness is described in detail. In Section 5, the proposed protocol is simulated on the IBM Quantum Experience platform. In Section 6 the security is analyzed. Finally, the discussion and conclusion are given in Section 7.

## 2. Preliminaries

Before presenting the protocol, some basic knowledge and preparations are introduced.

### 2.1. Two-dimensional Bell state

Two-dimensional Bell state, the most common quantum entangled state, is used to describe the four maximal entangled states in a two-qubit system

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

In the proposed protocol, we do not consider the robustness of the two qubits in the correlated quantum channel and default to using various methods[42] to keep them at ideal values.

### 2.2. Semi-quantum model

In the proposed protocol, STP can prepare the two-dimensional Bell states, send them to the classical participants via the quantum channel, measure these Bell states and perform the binary logic operations, while the classical participants are limited to perform the addition operations with carry and the following specific operations: (I) Return the particle without any disturbance. (Ⅱ) Perform a Pauli gate operation on the particle and distribute it back.

### 2.3. Pauli gate operations

There are four Pauli gate operations $I, X, Y, Z$:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

When $P_n$ performs a Pauli gate operation on particle $A$, the Bell state would be changed as follows:

$$|\varphi^{+}\rangle_{AB} \xrightarrow{X_A} |\psi^{+}\rangle_{AB}, \ |\varphi^{+}\rangle_{AB} \xrightarrow{Y_A} |\psi^{-}\rangle_{AB},$$
$$|\varphi^{+}\rangle_{AB} \xrightarrow{Z_A} |\varphi^{-}\rangle_{AB}, \tag{2}$$
$$|\varphi^{-}\rangle_{AB} \xrightarrow{X_A} |\psi^{-}\rangle_{AB}, \ |\varphi^{-}\rangle_{AB} \xrightarrow{Y_A} |\psi^{+}\rangle_{AB},$$
$$|\varphi^{-}\rangle_{AB} \xrightarrow{Z_A} |\varphi^{+}\rangle_{AB}, \tag{3}$$
$$|\psi^{+}\rangle_{AB} \xrightarrow{X_A} |\varphi^{+}\rangle_{AB}, \ |\psi^{+}\rangle_{AB} \xrightarrow{Y_A} |\varphi^{-}\rangle_{AB},$$
$$|\psi^{+}\rangle_{AB} \xrightarrow{Z_A} |\psi^{-}\rangle_{AB}, \tag{4}$$
$$|\psi^{-}\rangle_{AB} \xrightarrow{X_A} |\varphi^{-}\rangle_{AB}, \ |\psi^{-}\rangle_{AB} \xrightarrow{Y_A} |\varphi^{+}\rangle_{AB},$$
$$|\psi^{-}\rangle_{AB} \xrightarrow{Z_A} |\psi^{+}\rangle_{AB}. \tag{5}$$

### 2.4. Preparation

Assume that there are $N$ classical participants $(P_1, P_2, \ldots, P_N)$ and each of them has a privacy expressed as $p_n = p_n^L \cdots p_n^2 p_n^1$, where $p_n^l \in \{0,1\}$, $n \in \{1,2,\ldots,N\}$ and $l \in \{1,2,\ldots,L,L+1\}$. When the length of $p_n$ is less than $L$, $P_n$ would add sufficient zeros to the highest bit. There is a secure key $K = k^L \cdots k^2 k^1$ shared among the classical participants in advance through a secure multi-party secret sharing protocol, where $k^l \in \{0,1\}$. In addition, a secure key $d_n = d_n^{L+1} d_n^L \cdots d_n^2 d_n^1$ is pre-shared between STP and $P_n$ in advance through a secure two-party secret sharing protocol, where $d_n^l \in \{0,1\}$.

## 3. Multi-party SQPCS protocol

These participants are all curious about the size relation of their privacies. With STP's help, they can carry out the protocol as follows (also see Fig. 1).

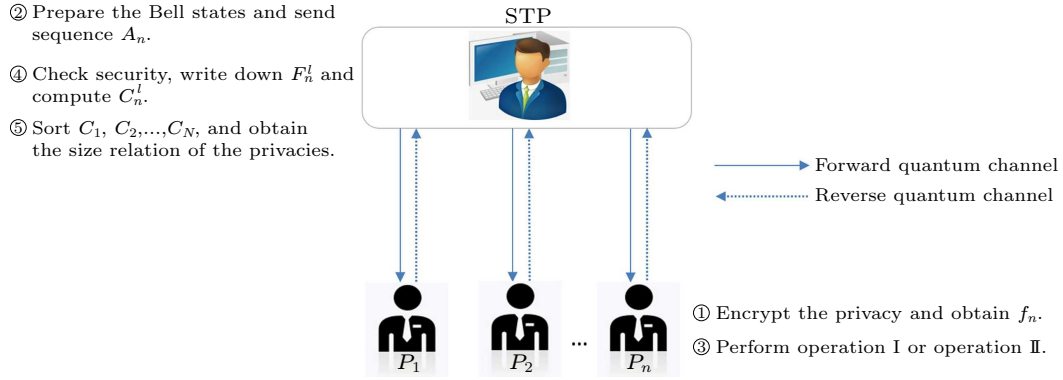



**Fig. 1.** The proposed protocol. STP would implement steps ②, ④ and ⑤, while each classical participant would implement steps ① and ③.

**Step 1** Each participant would encrypt his privacy before communication. Firstly, $P_n$ can obtain a string of data $c_n = c_n^L \cdots c_n^2 c_n^1$ or $c_n = c_n^{L+1} c_n^L \cdots c_n^2 c_n^1$ according to the following equation:

$$c_n^l = p_n^l + k^l, \tag{6}$$

where $+$ represents the addition operation with carry. Hence, if $c_n \geq c_{n'}$, one can obtain $p_n \geq p_{n'}$, with $n' \in \{1,2,\ldots,N\}$ and $n \neq n'$. Additionally, if $c_n$ only has $L$ bits, one could add one zero to the highest bit. Consequently, $c_n$ can be expressed as $c_n^{L+1} c_n^L \cdots c_n^2 c_n^1$. Secondly, $P_n$ would perform the logical operation with Eq. (7) and obtain a string of data $f_n = f_n^{L+1} f_n^L \cdots f_n^2 f_n^1$,

$$f_n^l = c_n^l \oplus d_n^l, \tag{7}$$

where $\oplus$ represents the logical xor operation.

**Step 2** STP randomly prepares $N(L+1)$ two-dimensional Bell states as follows:

$$\begin{aligned}
&|A_1^1 B_1^1\rangle, |A_2^1 B_2^1\rangle, \ldots, |A_N^1 B_N^1\rangle,\\
&|A_1^2 B_1^2\rangle, |A_2^2 B_2^2\rangle, \ldots, |A_N^2 B_N^2\rangle,\\
&\cdots\\
&|A_1^L B_1^L\rangle, |A_2^L B_2^L\rangle, \ldots, |A_N^L B_N^L\rangle,\\
&|A_1^{L+1} B_1^{L+1}\rangle, |A_2^{L+1} B_2^{L+1}\rangle, \ldots, |A_N^{L+1} B_N^{L+1}\rangle,
\end{aligned} \tag{8}$$

where $A$ represents the second particle and $B$ represents the first particle of the Bell state. With these Bell states, one can prepare $2N$ quantum sequences in which the sequences $A = [A_1, A_2, \ldots, A_N]$ and $B = [B_1, B_2, \ldots, B_N]$ contain all the second and the first particles, respectively, where $A_n = [A_n^1, A_n^2, \ldots, A_n^L, A_n^{L+1}]$ and $B_n = [B_n^1, B_n^2, \ldots, B_n^L, B_n^{L+1}]$. Then, STP sends the sequence $A_n$ to the $P_n$ and puts the sequence $B_n$ on reserve.

**Step 3** When $P_n$ has received the particle $A_n^l$, $P_n$ would select operation I or operation Ⅱ according to the value of $f_n^l$. As shown in Table 1, if $f_n^l$ is 0, $P_n$ would return the particle $A_n^l$ directly without any disturbance, in the other case, one would perform a Pauli gate operation on the particle and distribute it back.

**Table 1.** $P_n$'s operation.

| $f_n^l$ | Operation on the particle $A_n^l$ |
|---|---|
| 0 | Operation I: return the particle via the reverse quantum channel without any disturbance |
| 1 | Operation Ⅱ: perform a Pauli gate operation on the particle and distribute it back via the reverse quantum channel |

**Step 4** When STP confirms that the particle $A_n^l$ has been received, $P_n$ would announce the operation on it. Here, $P_n$'s announcement is sent through an open channel and is directly exposed to all. When $P_n$ performs operation I on particle $A_n^l$, STP would make Bell measurement on particles $A_n^l$ and $B_n^l$. According to the measurement, $P_n$ could know whether there exists the eavesdropping or not in the quantum channel. If the eavesdropping does not exist, STP would write down $F_n^l = 0$, or they will abort the protocol. When $P_n$ performs operation Ⅱ on the particle, STP would make the Bell measurement on particles $A_n^l$ and $B_n^l$ too. According to the measurement, STP could also know whether the eavesdropping exists or not in the quantum channel. If there is not the eavesdropping, STP would write down $F_n^l = 1$, or they would abort the protocol. When all particles in sequence $A_n$ have been done, STP would obtain a bunch of data $F_n = F_n^{L+1} F_n^L \cdots F_n^2 F_n^1$. Then, STP would compute $C_n^l$,

$$C_n^l = F_n^l \oplus d_n^l. \tag{9}$$

**Step 5** After STP has done with all particles from all participants, STP would obtain $N$ bunches of data $C_1, C_2, \ldots, C_N$. Next, STP would take out the same digits (the $l$-th digit) from $C_1, C_2, \ldots, C_N$ to compute $R_{nn'}^l$,

$$R_{nn'}^l = C_n^l \oplus C_{n'}^l. \tag{10}$$

Based on Eq. (10), STP would obtain

$$\begin{aligned}
&C_n^l = C_{n'}^l, \ \text{if} \ R_{nn'}^l = 0;\\
&C_n^l \neq C_{n'}^l, \ \text{if} \ R_{nn'}^l = 1.
\end{aligned} \tag{11}$$

When $R_{nn'}^l = 1$, $C_n^l$ is not equal to $C_{n'}^l$, and one of them is 0 (the small number), the other is 1 (the large number). STP can tell if $C_n^l$ is 0 or 1 by $r_n^l$,

$$r_n^l = C_n^l \oplus 1; \tag{12}$$

$$C_n^l = 1 \text{ and } C_n^l > C_{n'}^l, \text{ if } r_n^l = 0;$$
$$C_n^l = 0 \text{ and } C_n^l < C_{n'}^l, \text{ if } r_n^l = 1. \quad (13)$$

To sum up, the size relation between $C_n^l$ and $C_{n'}^l$ can be determined as follows:

$$\text{if } R_{nn'}^l = 0 \Rightarrow C_n^l = C_{n'}^l;$$
$$\text{if } R_{nn'}^l = 1 \text{ and } r_n^l = 0 \Rightarrow C_n^l > C_{n'}^l;$$
$$\text{if } R_{nn'}^l = 1 \text{ and } r_n^l = 1 \Rightarrow C_n^l < C_{n'}^l. \quad (14)$$

Thus, STP can sort $C_1, C_2, \ldots, C_N$ according to the above compared results.

## 4. Correctness

### 4.1. Output correctness

From Table 1 and step 4, one can see

$$F_n = f_n. \quad (15)$$

With Eqs. (7) and (15), one can obtain

$$C_n^l = F_n^l \oplus d_n^l = f_n^l \oplus d_n^l = c_n^l \oplus d_n^l \oplus d_n^l = c_n^l. \quad (16)$$

Therefore, the size relation between $c_n$ and $c_{n'}$ $(n \neq n')$ can be obtained from Eq. (14). According to Eq. (6), it must follow that when $c_n$ is greater than or equal to $c_{n'}$, $p_n$ must be greater than or equal to $p_{n'}$. That is to say, the size relation among the privacies $p_1, p_2, \ldots, p_N$ can be obtained with Eq. (14).

### 4.2. Examples

Assume that there are three participants ($P_1$, $P_2$, $P_3$) and each of them has a privacy ($p_1 = 101$, $p_2 = 010$, $p_3 = 110$). The key $K$ is 100. In addition, the keys $d_1$, $d_2$, and $d_3$ are 1011, 0011, and 0101, respectively. With the help of STP, they can carry out the following steps.

**Step S1** The participants would encrypt their privacies, and obtain some data with Eq. (6),

$$c_1 = 1001, \ c_2 = 110, \ c_3 = 1010. \quad (17)$$

Since $c_2$ has fewer than 4 digits, $P_2$ adds a zero to the highest digit, resulting in $c_2 = 0110$. Then, the participants proceed to encrypt their private information by Eq. (7), yielding

$$f_1 = 0010, \ f_2 = 0101, \ f_3 = 1111. \quad (18)$$

**Step S2** STP would randomly prepare $3 \times 4$ two-dimensional Bell states,

$$|A_1^1 B_1^1\rangle, |A_2^1 B_2^1\rangle, |A_3^1 B_3^1\rangle,$$
$$|A_1^2 B_1^2\rangle, |A_2^2 B_2^2\rangle, |A_3^2 B_3^2\rangle,$$
$$|A_1^3 B_1^3\rangle, |A_2^3 B_2^3\rangle, |A_3^3 B_3^3\rangle,$$
$$|A_1^4 B_1^4\rangle, |A_2^4 B_2^4\rangle, |A_3^4 B_3^4\rangle. \quad (19)$$

Then, STP would prepare the particle sequences according to step 2, and send the particle sequence $A_1$ to $P_1$, $A_2$ to $P_2$, and $A_3$ to $P_3$.

**Step S3** When the participants received the particle sequence, they would perform the corresponding action based on the value of $f_n^l$. The detailed actions are shown in Table 2.

**Table 2.** $P_n$'s detailed actions. R: return, P: Pauli gate operation.

| Participant | $P_1$ | | | | $P_2$ | | | | $P_3$ | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Particle | $A_1^1$ | $A_1^2$ | $A_1^3$ | $A_1^4$ | $A_2^1$ | $A_2^2$ | $A_2^3$ | $A_2^4$ | $A_3^1$ | $A_3^2$ | $A_3^3$ | $A_3^4$ |
| $f_n^l$ | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| Action | R | R | P | R | R | P | R | P | P | P | P | P |

**Step S4** After STP received all the particles, the participants would announce their actions on each particle. According to step 3, STP can obtain $F_1 = 0010$, $F_2 = 0101$, $F_3 = 1111$. From Eq. (18), we have

$$F_1 = f_1, \ F_2 = f_2, \ F_3 = f_3. \quad (20)$$

Then based on Eq. (10), STP can obtain

$$C_1 = 1001, \ C_2 = 0110, \ C_3 = 1010. \quad (21)$$

Form Eq. (17), it can be seen that

$$C_1 = c_1, \ C_2 = c_2, \ C_3 = c_3. \quad (22)$$

**Step S5** STP would take the same bits from $C_n$ ($n = 1, 2, 3$) to compare them. With Eqs. (10) and (12), we can obtain

$$R_{12}^1 = C_1^1 \oplus C_2^1 = 1, \ r_1^1 = C_1^1 \oplus 1 = 0; \ R_{12}^2 = 1, \ r_1^2 = 1;$$
$$R_{12}^3 = 1, \ r_1^3 = 1; \ R_{12}^4 = 1, \ r_1^4 = 0;$$
$$R_{13}^1 = C_1^1 \oplus C_3^1 = 1, \ r_1^1 = C_1^1 \oplus 1 = 0; \ R_{13}^2 = 1, \ r_1^2 = 1;$$
$$R_{13}^3 = 0; \ R_{13}^4 = 0; \ R_{23}^1 = C_2^1 \oplus C_3^1 = 0; \ R_{23}^2 = 0;$$
$$R_{23}^3 = 1, \ r_2^3 = 0; \ R_{23}^4 = 1, \ r_2^4 = 1. \quad (23)$$

According to Eq. (16), STP can obtain

$$C_1^1 > C_2^1 = C_3^1, \ C_1^2 < C_2^2 = C_3^2,$$
$$C_1^3 = C_3^3 < C_2^3, \ C_1^4 = C_3^4 > C_2^4. \quad (24)$$

Therefore, STP can obtain the size relation among $C_1$, $C_2$ and $C_3$ as follows:

$$C_3 > C_1 > C_2. \quad (25)$$

Following Eqs. (6) and (22), STP can obtain the size relation

of the participants' privacies,

$$p_3 > p_1 > p_2. \tag{26}$$

Compared with their actual privacies ($p_1 = 101$, $p_2 = 010$, $p_3 = 110$), it can be seen that the comparison results in Eq. (26) are correct. More examples are given in Table 3 to further prove the correctness of the proposed protocol.

**Table 3.** Proof of the correctness. It can be seen that all the comparison results are turned out to be correct compared with the participants' privacies. Thus, the proposed protocol can compare the size relation among multiple participants' privacies.

| $K$ | $P_n$ | $p_n$ | $c_n$ | $d_n$ | $f_n = F_n$ | $C_n$ | $R^l_{nn'}$ |
|---|---|---|---|---|---|---|---|
| 11 | $P_1$ | 11 | 110 | 001 | 111 | 110 | $R^3_{12}=0$ |
| | $P_2$ | 10 | 101 | 011 | 110 | 101 | $R^2_{12}=1$ |
| | | | | | | | $R^1_{12}=1$ |
| 001 | $P_1$ | 100 | 0101 | 0110 | 0011 | 0101 | $R^4_{12}=1, R^4_{13}=R^4_{23}=1$ |
| | $P_2$ | 111 | 1000 | 0011 | 1011 | 1000 | $R^3_{12}=1, R^3_{13}=1, R^3_{23}=0$ |
| | $P_3$ | 001 | 0010 | 1100 | 1110 | 0010 | $R^2_{12}=0, R^2_{13}=1, R^2_{23}=1$ |
| | | | | | | | $R^1_{12}=1, R^1_{13}=1, R^1_{23}=0$ |
| 1010 | $P_1$ | 1011 | 10101 | 01010 | 11111 | 10101 | $R^5_{12}=0, R^5_{13}=0, R^5_{14}=1, R^5_{23}=0, R^5_{24}=1, R^5_{34}=1$ |
| | $P_2$ | 0110 | 10000 | 11111 | 01111 | 10000 | $R^4_{12}=0, R^4_{13}=1, R^4_{14}=1, R^4_{23}=1, R^4_{24}=1, R^4_{34}=0$ |
| | $P_3$ | 1110 | 11000 | 00011 | 11011 | 11000 | $R^3_{12}=1, R^3_{13}=1, R^3_{14}=1, R^3_{23}=0, R^3_{24}=0, R^3_{34}=0$ |
| | $P_4$ | 0001 | 01011 | 11100 | 10111 | 01011 | $R^2_{12}=0, R^2_{13}=0, R^2_{14}=1, R^2_{23}=0, R^2_{24}=1, R^2_{34}=1$ |
| | | | | | | | $R^1_{12}=1, R^1_{13}=1, R^1_{14}=0, R^1_{23}=0, R^1_{24}=1, R^1_{34}=1$ |

| $K$ | $r^l_{nn'}$ | The size relation between $C^l_n$ and $C^l_{n'}$ | The size relation of $C_n(p_n)$ |
|---|---|---|---|
| 11 | $r^2_1=0$ | $C^3_1=C^3_2$ | $C_1>C_2$ |
| | $r^1_1=1$ | $C^2_1>C^2_2$ | $(p_1>p_2)$ |
| | | $C^1_1<C^1_2$ | |
| 001 | $r^4_1=1, r^4_2=0$ | $C^4_1<C^4_2, C^4_1=C^4_3, C^4_2>C^4_3$ | $C_2>C_1>C_3$ |
| | $r^3_1=0$ | $C^3_1>C^3_2, C^3_1>C^3_3, C^3_2=C^3_3$ | $(p_2>p_1>p_3)$ |
| | $r^2_1=1, r^2_2=1$ | $C^2_1=C^2_2, C^2_1<C^2_3, C^2_2<C^2_3$ | |
| | $r^1_1=0$ | $C^1_1>C^1_2, C^1_1>C^1_3, C^1_2=C^1_3$ | |
| 1010 | $r^5_1=0, r^5_2=0, r^5_3=0$ | $C^5_1=C^5_2, C^5_1=C^5_3, C^5_1>C^5_4, C^5_2=C^5_3, C^5_2>C^5_4, C^5_3>C^5_4$ | $C_3>C_1>C_2>C_4$ |
| | $r^4_1=1, r^4_2=1$ | $C^4_1=C^4_2, C^4_1<C^4_3, C^4_1<C^4_4, C^4_2<C^4_3, C^4_2<C^4_4, C^4_3=C^4_4$ | $(p_3>p_1>p_2>p_4)$ |
| | $r^3_1=0$ | $C^3_1>C^3_2, C^3_1>C^3_3, C^3_1>C^3_4, C^3_2=C^3_3, C^3_2=C^3_4, C^3_3=C^3_4$ | |
| | $r^2_1=1, r^2_2=1, r^2_3=1$ | $C^2_1=C^2_2, C^2_1=C^2_3, C^2_1<C^2_4, C^2_2=C^2_3, C^2_2<C^2_4, C^2_3<C^2_4$ | |
| | $r^1_1=0, r^1_2=1, r^1_3=1$ | $C^1_1>C^1_2, C^1_1>C^1_3, C^1_1=C^1_4, C^1_2=C^1_3, C^1_2<C^1_4, C^1_3<C^1_4$ | |

## 5. Simulations

Next, two types of quantum communication processes are simulated on the IBM Quantum Experience platform according to the operation $P_n$ performed on the particle. Before simulations, the basic knowledge is introduced.

On the IBM Quantum Experience platform, the Bell state can be prepared by the Hadamard and the CNOT gate operations in quantum circuit.

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ \mathrm{CNOT} = \begin{bmatrix}I & 0\\ 0 & X\end{bmatrix}; \tag{27}$$

$$\begin{aligned}
&|00\rangle_{AB} \xrightarrow{H_AI_B} \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)_{AB}\\
&\xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB} = |\varphi^+\rangle_{AB},
\end{aligned} \tag{28}$$

$$\begin{aligned}
&|10\rangle_{AB} \xrightarrow{H_AI_B} \frac{1}{\sqrt{2}}(|00\rangle-|10\rangle)_{AB}\\
&\xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{AB} = |\varphi^-\rangle_{AB},
\end{aligned} \tag{29}$$

$$\begin{aligned}
&|01\rangle_{AB} \xrightarrow{H_AI_B} \frac{1}{\sqrt{2}}(|01\rangle+|11\rangle)_{AB}\\
&\xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB} = |\psi^+\rangle_{AB},
\end{aligned} \tag{30}$$

$$\begin{aligned}
&|11\rangle_{AB} \xrightarrow{H_AI_B} \frac{1}{\sqrt{2}}(|01\rangle-|11\rangle)_{AB}\\
&\xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{AB} = |\psi^-\rangle_{AB}.
\end{aligned} \tag{31}$$

Correspondingly, the Bell measurement can be performed by the CNOT and the Hadamard gate operations in quantum circuit.

$$\begin{aligned}
|\varphi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB} \xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)_{AB}\\
&\xrightarrow{H_AI_B} |00\rangle_{AB},
\end{aligned} \tag{32}$$

$$\begin{aligned}
|\varphi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{AB} \xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|00\rangle-|10\rangle)_{AB}\\
&\xrightarrow{H_AI_B} |10\rangle_{AB},
\end{aligned} \tag{33}$$

$$\begin{aligned}
|\psi^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB} \xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|01\rangle+|11\rangle)_{AB}\\
&\xrightarrow{H_AI_B} |01\rangle_{AB},
\end{aligned} \tag{34}$$

$$\begin{aligned}
|\psi^-\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle-|11\rangle)_{AB} \xrightarrow{\mathrm{CNOT}_{AB}} \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{AB}\\
&\xrightarrow{H_AI_B} |11\rangle_{AB}.
\end{aligned} \tag{35}$$

### 5.1. Simulation for $P_n$ performing operation I

When $P_n$ performs operation I on the particle $A_n^l$ and the Bell state STP prepared is $|\varphi^+\rangle_{AB}$, the quantum circuit is shown in Fig. 2(a). If there is no attack in the quantum channel, STP's measurement result must be 00 according to Eq. (32), as shown in Fig. 2(b). When the output is not 00, there must exist eavesdropping. For example, Eve, an external attacker, intercepts and measures the particle $A_n^l$, then returns a new particle with the same measurement as the measurement of the particle $A_n^l$ (the intercept-measure-resend attack). When her measurement result is 1, the particle $B_n^l$ would collapse into $|1\rangle$ according to Eq. (1). Eve would resend a new particle with the measurement result of 1. The corresponding quantum circuit and the output are shown in Fig. 3. Obviously, the output is not 00. Therefore, according to the output, STP can tell us if there exists eavesdropping in the quantum channel.

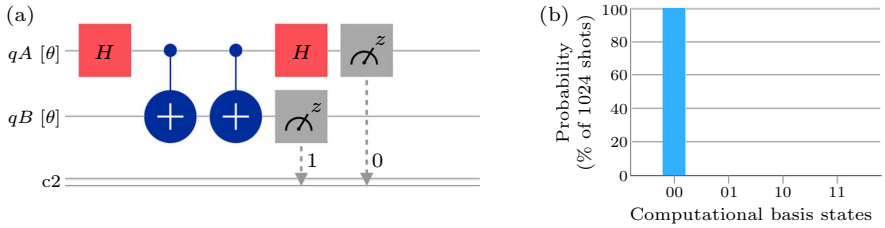



**Fig. 2.** Simulation without eavesdropping: (a) quantum circuit, (b) output.

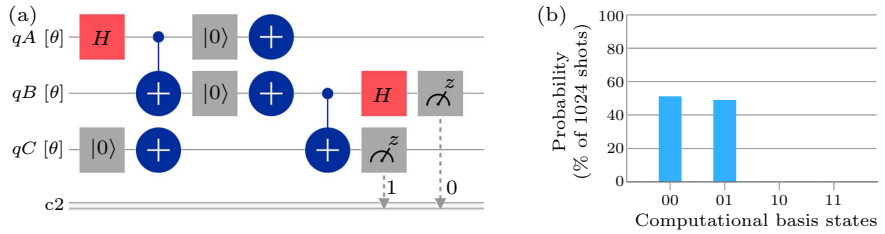



**Fig. 3.** Simulation with the intercept-measure-resend attack: (a) quantum circuit, (b) output.

### 5.2. Simulation for $P_n$ performing operation Ⅱ

When $P_n$ selects operation Ⅱ on particle $A_n^l$, it means that $P_n$ would perform a Pauli gate operation on the particle according to Table 1.

Suppose that the Bell state STP prepared is $|\varphi^-\rangle_{AB}$ and $P_n$ performs the Pauli-$X$ gate operation, the quantum circuit is shown in Fig. 4(a). If there is no attack in the quantum channel, the output must be 11 according to Eqs. (3) and (35), as shown in Fig. 4(b). When the output is not 11, there must exist eavesdropping in the quantum channel. For example, Eve intercepts the particle $A_n^l$ and resends a new particle to STP (the intercept-resend attack). The corresponding simulation shown in Fig. 5 indicates that the outputs are 00, 01, 10, 11 with equal probability (approximately 25%) instead of 11 with 100% probability.

Assume that the Bell state STP prepared is $|\psi^+\rangle_{AB}$ and $P_n$ performs the Pauli-$Y$ gate operation on particle $A_n^l$, the corresponding quantum circuit and output are shown in Fig. 6.

When the Bell state STP prepared is $|\psi^-\rangle_{AB}$ and the Pauli-$Z$ gate operation is performed on particle $A_n^l$, the corresponding quantum circuit and output are shown in Fig. 7.

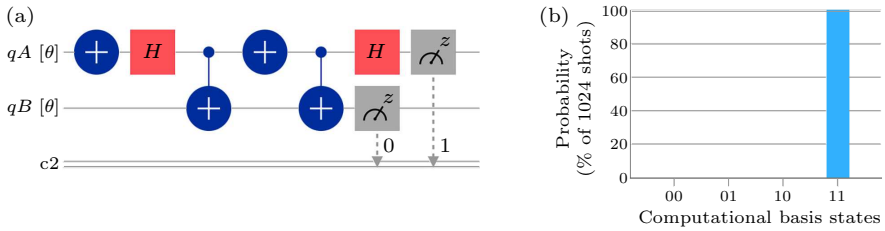



**Fig. 4.** Simulation with the Pauli-$X$ gate operation on particle $A_n^l$: (a) quantum circuit, (b) output.

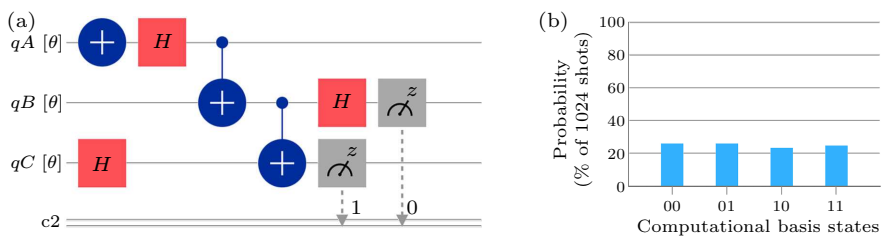



**Fig. 5.** Simulation with the intercept-resend attack: (a) quantum circuit, (b) output.

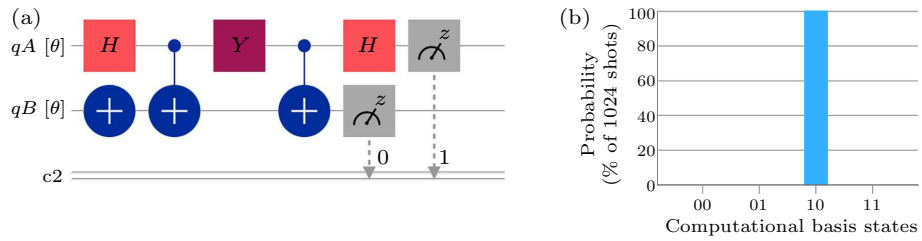



**Fig. 6.** Simulation with the Pauli-$Y$ gate operation on particle $A_n^l$: (a) quantum circuit, (b) output.

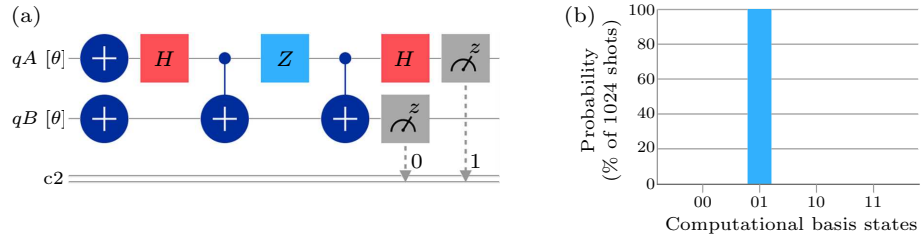



**Fig. 7.** Simulation with the Pauli-$Z$ gate operation on particle $A_n^l$: (a) quantum circuit, (b) output.

## 6. Security

Both the external and the internal attacks on the devised protocol will be analyzed. The quantum channels are assumed to be ideal.

### 6.1. External attacks

Eve, an external attacker, may launch many kinds of common attacks on the quantum channel to obtain some useful information, such as the intercept-resend attack, the intercept-measure-resend attack, and the entanglement attack. From the above simulations, one can see that the intercept-resend attack and the intercept-measure-resend attack to the quantum channel would be detected by the STP. Therefore, both kinds of attacks are invalid to our protocol. Then, a detailed analysis about the entanglement attack will be given.

The entanglement attack occurs when Eve applies operation $U_\phi$ and attaches an auxiliary entanglement state $|\phi\rangle$ to the particles transmitted in the quantum channel,

$$U_\phi|k\rangle|\phi\rangle = \sum_{l=0}^{1} a_{lk}|l\rangle|\varepsilon_{lk}\rangle, \tag{36}$$

where $|\varepsilon_{lk}\rangle$ is the pure auxiliary state determined uniquely by $U_\phi$, and $\sum_{l=0}^{1}|a_{lk}|^2 = 1$. When Eve performs the entanglement attack on particle $A_n^l$, she would obtain

$$U_\phi|0\rangle|\phi\rangle = a_{00}|0\rangle|\varepsilon_{00}\rangle + a_{10}|1\rangle|\varepsilon_{10}\rangle, \tag{37}$$
$$U_\phi|1\rangle|\phi\rangle = a_{01}|0\rangle|\varepsilon_{01}\rangle + a_{11}|1\rangle|\varepsilon_{11}\rangle. \tag{38}$$

The initial Bell state would become

$$\begin{aligned} U_\phi|\varphi^\pm\rangle|\phi\rangle &= \frac{1}{\sqrt{2}}U_\phi(|00\rangle \pm |11\rangle)|\phi\rangle \\ &= \frac{1}{\sqrt{2}}(a_{00}|00\rangle|\varepsilon_{00}\rangle + a_{10}|10\rangle|\varepsilon_{10}\rangle \\ &\quad \pm a_{01}|01\rangle|\varepsilon_{01}\rangle \pm a_{11}|11\rangle|\varepsilon_{11}\rangle), \end{aligned} \tag{39}$$

$$\begin{aligned} U_\phi|\psi^\pm|\phi\rangle &= \frac{1}{\sqrt{2}}U_\phi(|01\rangle \pm |10\rangle)|\phi\rangle \\ &= \frac{1}{\sqrt{2}}(a_{00}|01\rangle|\varepsilon_{00}\rangle + a_{10}|11\rangle|\varepsilon_{10}\rangle \\ &\quad \pm a_{01}|00\rangle|\varepsilon_{01}\rangle \pm a_{11}|10\rangle|\varepsilon 11\rangle). \end{aligned} \tag{40}$$

It is generally known that the Bell measurement result would also be changed, accordingly the initial Bell state would change. Therefore, Eve has to set $a_{10} = a_{01} = 0$ and $a_{00}|\varepsilon_{00}\rangle = a_{11}|\varepsilon_{11}\rangle$ to avoid being detected. Then Eqs. (39) and (40) would turn out to be

$$U_\phi|\varphi^\pm\rangle|\phi\rangle = \frac{1}{\sqrt{2}}a_{00}(|00\rangle \pm |11\rangle)|\varepsilon_{00}\rangle, \tag{41}$$
$$U_\phi|\psi^\pm\rangle|\phi\rangle = \frac{1}{\sqrt{2}}a_{00}(|01\rangle \pm |10\rangle)|\varepsilon_{00}\rangle. \tag{42}$$

Equations (41) and (42) imply that Eve has no effect on the initial Bell state if she attempts to eavesdrop without being detected. One can conclude that the entanglement attack is invalid to the devised protocol.

### 6.2. Internal attacks

The internal attacks from dishonest $P_n$ and STP will be analyzed.

The dishonest $P_n$ may gain some useful information by two ways: (a) $P_n$ launches an attack to the quantum channel; (b) $P_n$ derives other participants' privacies from the available information. In case (a), $P_n$ would be detected as an external attacker who cannot obtain any information just as analyzed in Subsection 5.1. In case (b), since $P_n$ knows nothing about the key shared between $P_{n'}$ $(n \neq n')$ and STP, $P_n$ cannot decrypt the available information and obtain other participant's privacies,

STP, a semi-honest third party, would strictly and faithfully follow the process of the protocol. Hence, STP would neither prepare other quantum states (e.g., GHZ states or single photons) nor collude with other eavesdroppers to steal the

participants' privacies. However, he is curious to know the participants' privacies, and try to extract the privacies from the available information. Since STP does not know the key $K = k^L \cdots k^2 k^1$ pre-shared among the participants, STP cannot derive the privacies from the ciphertext $c_n^l = p_n^l + k^l$. Therefore, this kind of attack to the proposed protocol is invalid.

## 7. Discussion and conclusion

Before presenting the conclusions, we will make comparisons with some existing protocols to highlight the novel contributions of our protocol and to distinguish it from existing protocols. Quantum resource, dimensions of used quantum state, category, requirement for participants, number of participants, simulation, and efficiency $\eta$ are collected in Table 4. Here, $\eta = (q_c/q_t) \times 100\%$, where $q_c$ is the total qubit number to be compared, and $q_t$ is the bit number used in all (inclusive qubit and classical bit in the bits), except for the bits used for key pre-shared among the participants. During the execution of our protocol, the STP requires $2N(L+1)$ qubits to prepare $N(L+1)$ Bell states, and the classical participants do not consume any qubit since they only need to return or perform an operation on the particle. $NL$ is the total number of compared qubits. As a result, the efficiency $\eta$ is $L/2(L+1)$ approaching 50%.

**Table 4.** Comparisons with some existing protocols. QR: quantum resource, DQS: dimensions of used quantum state, RP: requirement for the participants, NP: number of participants.

| Compared aspects | Ref. [43] | Ref. [44] | Ref. [45] | Ref. [46] | Ref. [27] | Ref. [47] | Our protocol |
|---|---|---|---|---|---|---|---|
| QR | Single state | Bell state | Bell state | GHZ-type state | Bell state | GHZ state | Bell state |
| DQS | $d=2$ | $d=2$ | $d=2$ | $d=2$ | $d>2$ | $d>2$ | $d=2$ |
| Category | Equality | Equality | Equality | Equality | Size | Size | Size |
| RP | Quantum | Classical | Classical | Classical | Quantum | Classical | Classical |
| NP | $N=2$ | $N=2$ | $N=2$ | $N\geq 2$ | $N\geq 2$ | $N=2$ | $N\geq 2$ |
| Simulation | NO | Yes | Yes | No | No | No | Yes |
| Efficiency | 50% | 12.5% | 12.5% | 14.3% | 25% | 12.5% | 50% |

From Table 4, we can see that our protocol is able to compare size relation based on the manageable two-dimensional quantum state, whereas the existing protocols can only compare equality. Only when the high-dimensional quantum states are used as the quantum resources, a size comparison protocol becomes possible in existing works. Thus, our protocol can overcome the challenges associated with high-dimensional quantum states by exploiting more manageable two-dimensional states, making it more feasible with current quantum technologies. Moreover, under the semi-quantum model, our protocol can allow multiple classical participants to make private comparison. The correctness of the proposed protocol is proved by several examples, and its effectiveness has been tested via simulation on the IBM Quantum Experience platform. Security analysis shows that the proposed protocol can defend against common attacks. It should be noted that our protocol is only suitable for scenarios such as idealized environments without quantum noise. In the future, we will focus on how to improve the protocol to accommodate more complex environments.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 62161025), the Project of Scientific and Technological Innovation Base of Jiangxi Province (Grant No. 20203CCD46008), and the Jiangxi Provincial Key Laboratory of Fusion and Information Control (Grant No. 20171BCD40005). The authors appreciate the helpful discussion with Dr. Xiao-Song Yang at NanChang University.

## References

[1] Yao A C 1982 *Proceedings of 23rd IEEE Symposium on Foundations of Computer Science* (SFCS'08), November 3–5, 1982, Chicago, IL, USA, pp. 160–164
[2] Boudot F, Schoenmakers B and Traore 2001 *Discrete Appl. Math.* **111** 23
[3] Mayers D 1997 *Phys. Rev. Lett.* **78** 3414
[4] Lo H K 1997 *Phys. Rev. A* **56** 1154
[5] Colbeck R 2007 *Phys. Rev. A* **76** 062308
[6] Wang Q L, Sun H X and Huang W 2014 *Quantum Inf. Process.* **13** 2375
[7] Hung S M, Huang S L, Hwang T and Kao S H 2017 *Quantum Inf. Process.* **16** 36
[8] Huang S L, Hwang T and Gope P 2015 *Quantum Inf. Process.* **14** 4225
[9] Li J, Wang Z, Ye C Q and Che F T 2023 *Int. J. Theor. Phys.* **62** 196
[10] Huang X, Chang Y, Cheng W, Hou M and Zhang S B 2022 *Chin. Phys. B* **31** 040303
[11] Jia H Y, Wen Q Y, Song T T and Gao F 2011 *Opt. Commun.* **284** 545
[12] Naseri M 2009 *Opt. Commun.* **282** 1939
[13] He L B, Huang L S, Yang W, Xu R and Han D Q 2012 *Quantum Inf. Process.* **11** 135969
[14] Chen X B, Xu G, Yang Y X and Wen Q Y 2010 *Int. J. Theor. Phys.* **49** 2793
[15] Hillery M, Ziman M, Buzek V and Bielikova M 2006 *Phys. Lett. A* **349** 75
[16] Bonanome M, Buzek V, Hillery M and Ziman M 2011 *Phys. Rev. A* **84** 022331
[17] Liu W J, Liu C, Chen H W, Li Z Q and Liu Z H 2014 *Commun. Theor. Phys.* **62** 210
[18] Liu W J, Liu C, Wang H B, Liu J F, Wang F and Yuan X M 2014 *Int. J. Theor. Phys.* **53** 1804
[19] Gu J, Ho C Y and Hwang T 2018 *Quantum Inf. Process.* **17** 23
[20] Lin S, Sun Y, Liu X and Yao Z 2013 *Quantum Inf. Process.* **12** 559
[21] Guo F Z, Gao F, Qin S J, Zhang J and Wen Q Y 2013 *Quantum Inf. Process.* **12** 2793
[22] Zhang W W, Li D, Zhang K J and Zuo H J 2013 *Quantum Inf. Process.* **12** 2241

[23] Yu C H, Guo G D and Lin S 2013 *Phys. Scr.* **88** 065013
[24] Luo Q B, Yang G W, She K, Niu W N and Wang Y Q 2014 *Quantum Inf. Process.* **13** 2343
[25] Ye C Q and Ye T Y 2018 *Quantum Inf. Process.* **17** 252
[26] Cao H, Ma W P, Lu L D, He Y F and Liu G 2019 *Quantum Inf. Process.* **18** 287
[27] Wang B, Gong L H and Liu S Q 2022 *Front. Phys.* **10** 981376
[28] Lian J Y, Li X and Ye T Y 2023 *Phys. Scr.* **98** 035011
[29] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[30] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 *Phys. Rev. A* **79** 032341
[31] Ye T Y, Geng M J, Xu T J and C Y 2022 *Quantum Inf. Process.* **21** 123
[32] Zhou N R, Xu Q D, Du N S and Gong L H 2021 *Quantum Inf. Process.* **20** 124
[33] Luo Q B, Li X Y, Yang G W and Lin C 2022 *Quantum Inf. Process.* **21** 257
[34] Lian J Y, Li X and Ye T Y 2023 *EPJ Quantum Technol.* **10** 10
[35] Wang B, Gong L H and Liu S Q 2023 *Laser Phys. Lett.* **20** 105202
[36] Ye T Y and Lian J Y 2023 *Physica A* **611** 128424
[37] Cozzolino D, Da Lio B, Bacco D and Oxenlowe L 2019 *Adv. Quantum Technol.* **2** 1900038
[38] Xu Q D, Chen H Y, Gong L H and Zhou N R 2020 *Int. J. Theor. Phys.* **59** 1798
[39] He Z B and Lou X P 2023 *Quantum Inf. Process.* **22** 150
[40] Gong L H, Chen Z Y, Qin L G and Huang J H 2023 *Adv. Quantum Technol.* **6** 2300097
[41] IBM Quantum Experience
[42] Wang Z Y, Wu F L, Peng Z Y and Liu S Y 2022 *Chin. Phys. B* **31** 070302
[43] Kou T Y, Che B C, Dou Z, Chen X B, Lai Y P and Li J 2022 *Chin. Phys. B* **31** 060307
[44] Gong L H, Ye Z J, Liu C and Zhou S 2024 *Laser Phys. Lett.* **21** 035207
[45] Gong L H, Li M L, Cao H and Wang B 2024 *Laser Phys. Lett.* **21** 055209
[46] Wu W Q, Guo L N and Xie M Z 2022 *Front. Phys.* **10** 1048325
[47] Wang B, Liu S Q and Gong L H 2022 *Chin. Phys. B* **31** 010302