

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)
Citation: Chin. Phys. B, 2022, 31 (**1**): 010302. DOI: 10.1088/1674-1056/ac1413
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Low-loss belief propagation decoder with Tanner graph in quantum error-correction codes

Dan-Dan Yan(颜丹丹), Xing-Kui Fan(范兴奎), Zhen-Yu Chen(陈祯羽), and Hong-Yang Ma(马鸿洋)†
Chin. Phys. B, 2022, 31 (**1**): 010304. DOI: 10.1088/1674-1056/ac11cf

Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme

Jing-Wen Zhang(张静文), Xiu-Bo Chen(陈秀波), Gang Xu(徐刚), and Yi-Xian Yang(杨义先)
Chin. Phys. B, 2021, 30 (**7**): 070309. DOI: 10.1088/1674-1056/ac003b

Practical decoy-state BB84 quantum key distribution with quantum memory

Xian-Ke Li(李咸柯), Xiao-Qian Song(宋小谦), Qi-Wei Guo(郭其伟), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Chin. Phys. B, 2021, 30 (**6**): 060305. DOI: 10.1088/1674-1056/abda31

Pulse-gated mode of commercial superconducting nanowire single photon detectors

Fan Liu(刘帆), Mu-Sheng Jiang(江木生), Yi-Fei Lu(陆宜飞), Yang Wang(汪洋), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2021, 30 (**4**): 040302. DOI: 10.1088/1674-1056/abc2c2

Deterministic nondestructive state analysis for polarization-spatial-time-bin hyperentanglement with cross-Kerr nonlinearity

Hui-Rong Zhang(张辉荣), Peng Wang(王鹏), Chang-Qi Yu(于长琦), and Bao-Cang Ren(任宝藏)
Chin. Phys. B, 2021, 30 (**3**): 030304. DOI: 10.1088/1674-1056/abd7d5

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

Bing Wang(王冰)[1,2,3], San-Qiu Liu(刘三秋)[1,3], and Li-Hua Gong(龚黎华)[1,4,†]

[1] *Jiangxi Province Key Laboratory of Fusion and Information Control, Department of Physics, Nanchang University, Nanchang* 330031, *China*
[2] *School of Materials Science and Engineering, Nanchang University, Nanchang* 330031, *China*
[3] *NCU-ASIPP Magnetic Confinement Fusion Joint Lab, Institute of Fusion Energy and Plasma Application, Nanchang University, Nanchang* 330031, *China*
[4] *Department of Electronic Information Engineering, Nanchang University, Nanchang* 330031, *China*

(Received 12 June 2021; revised manuscript received 7 July 2021; accepted manuscript online 14 July 2021)

A novel efficient semi-quantum private comparison protocol based on the *d*-dimensional GHZ states is proposed. With the assistance of semi-honest third party, two classical participants can compare the size relation of their secrets without any information leakage. To reduce the consumption of quantum devices, the qubit efficiency of our protocol is improved by introducing the semi-quantum conception via the existing semi-quantum private comparisons. Furthermore, it is unnecessary to prepare the secure classical authentication channel among participants in advance. It is shown that our protocol is not only correct and efficient, but also free from external and internal attacks.

Keywords: semi-quantum private comparison, size relation, dimensional GHZ state, qubit efficiency

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a, 03.67.Ac **DOI:** 10.1088/1674-1056/ac1413

1. Introduction

To date, quantum cryptography has been gained considerable attention worldwide. Many secure quantum cryptographic protocols have been designed, such as quantum key distribution (QKD),[1–5] quantum secret sharing (QSS),[6–8] quantum secure direct communication (QSDC),[2,9–11] and so on. Recently, some new research fields of quantum cryptography have emerged including quantum homomorphic encryption (QHE),[12] quantum information splitting,[13] quantum private comparison (QPC). Since the first QPC protocol was proposed by Yang and Wen in 2009, QPC has become a hot topic.[14] By utilizing Bell state, hash function and decoy photons, their protocol can compare the equality of two parties' secrets. In 2010, Chen *et al.* devised a new QPC protocols which can also compare the equality of privacies.[15] Later, a new type of QPC protocol allowing clients to execute quantum processing on a remote server was presented,[16] with the duality quantum formalism.[17] Although many QPC protocols were proposed, all participants need to be equipped with advanced quantum devices, such as quantum measurement, quantum state generator, or quantum unitary operation.[18–22] To reduce the consumption of quantum devices, an innovative concept of semi-quantum theory has been put forward.[23,24] In the semi-quantum mode, quantum party owns the powerful quantum capability and can prepare quantum state, perform quantum measurement and store qubits in quantum memory, while classical parties only have limited quantum capability and can perform the following classical operations:

(1) Let particle go back without disturbance.

(2) Measure the particle with $\overline{Z}$ basis, prepare a new state in $\overline{Z}$ basis and distribute it back.

(3) Reorder particles with different delay lines.

Not all participants could afford the expensive quantum equipment, semi-quantum theory is very practical and convenient in the near future application, therefore semi-quantum key distribution (SQKD),[25–29] semi-quantum secret sharing (SQSS),[30,31] semi-quantum private comparison (SQPC)[32–35] were investigated widely. Chou *et al.* proposed the first SQPC protocol, allowing two classical participants to compare the equality of their secrets with the help of an almost-dishonest third party.[32] In 2020, Jiang devised two semi-quantum private comparison protocols based on Bell states to compare the equality of two classical participants' secrets.[36] Most previous private comparison protocols based on semi-quantum theory can only compare the equality of privacies between two classical participants. Fortunately, in 2021, Zhou *et al.* presented a semi-quantum private comparison protocol to compare the size relationship of two-participant's secrets under the assistance of a semi–honest third party, and the qubit efficiency is raised to be comparable with the existing semi-quantum private comparison protocols at the cost of preparation of the classical authenticated channel in advance by classical participants.[37]

It is generally known that a quantum two-party secure computation is impossible.[38] However, this goal may be achieved if additional assumptions were made, such as adding a third party. A semi-honest third party (STP) should follow the procedure of the protocol, take a record of all intermediate

†Corresponding author. E-mail: lhgong@ncu.edu.cn
© 2022 Chinese Physical Society and IOP Publishing Ltd

computation and prevent the results from being corrupted by an outside eavesdropper. However, STP may attempt to steal the information from the record.

Motivated by Refs. [36,37,39], we propose a novel efficient private comparison protocol based on the d-dimensional GHZ states. Under the assistance of a semi-honest third party, our protocol can judge the size relationship of the privacies between Alice and Bob. The rest of this paper is organized as follows: In Section 2, we give a detailed description of the proposed protocol. In Section 3, the correctness of the output result is analyzed and some examples are listed for better understanding. In Section 4, the security of the proposed protocol is analyzed. The attacks from external and internal are invalid to our protocol. In Section 5, the comparisons between our SQPC and those previous typical SQPC protocols are given. Finally, a short conclusion is provided in Section 6.

2. Semi-quantum private comparison protocol of size relation

There are two classical participants, Alice and Bob, who own the secrets X and Y, respectively. With the help of STP, they can compare the size relation of X and Y without leaking any information about their secrets. The representations of X and Y are $x_0,x_1,\ldots,x_{N-1}$ and $y_0,y_1,\ldots,y_{N-1}$, where $x_i,y_i \in \{0,1,\ldots,h-1\}$, $i=0,1,\ldots,N-1$, $h=\frac{1}{2}(d+1)$. Meanwhile, Alice and Bob share two common key sequences $K_{\rm AB}$ and $K'_{\rm AB}$ in advance through a secure SQKD protocol, where $K_{\rm AB}=K^0_{\rm AB}K^1_{\rm AB}K^2_{\rm AB},\ldots,K^{N-1}_{\rm AB}$, $K^i_{\rm AB}\in\{0,1,\ldots,h-1\}$. $K'_{\rm AB}$ is a sequence of binary numbers. Then, they divide the binary representation into $n/2$ groups, where $n\geq 8N$. Therefore, $K'_{\rm AB}$ can be expressed as

$$K'_{\rm AB}=K'^0_{\rm AB}K'^1_{\rm AB}K'^2_{\rm AB},\ldots,K'^{n/2}_{\rm AB},$$
$$K'^i_{\rm AB}\in\{00,01,10,11\}.$$

2.1. Preparation for the protocol

The quantum resource used in our SQCP is d-dimensional GHZ state. In a d-dimensional Hilbert space, according to three variables $u_1,u_2,u_3\in\{0,1,\ldots,d-1\}$, a d-dimensional GHZ state can be expressed as[39,40]

$$\left|\phi_{u_1,u_2,u_3}\right\rangle=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}{\rm e}^{{\rm i}\frac{2\pi}{d}u_1k}\left|k,k\oplus u_2,k\oplus u_3\right\rangle, \tag{1}$$

where subscripts u_1, u_2 and u_3 run from 0 to $d-1$, and $\oplus$ denotes module d addition. In addition, we can define d-dimensional Z-basis $\overline{Z}$ and X-basis $\overline{X}$ in a d-dimensional quantum system as follows:[37,41]

$$\overline{Z}=\{\left|0\right\rangle,\left|1\right\rangle,\ldots,\left|d-1\right\rangle\}, \tag{2}$$
$$\overline{X}=\{F\left|0\right\rangle,F\left|1\right\rangle,\ldots,F\left|d-1\right\rangle\}, \tag{3}$$

where F represents quantum Fourier transform. In addition, $F\left|j\right\rangle=\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}{\rm e}^{\frac{2\pi{\rm i}}{d}kj}\left|k\right\rangle$, $j=0,1,\ldots,d-1$. Now, let us give an explicit description of the proposed protocol.

Step 1 STP sends S_A ($S_{\rm B}$) to Alice (Bob). STP prepares $4N(1+\delta)$ d-dimensional GHZ states in the form of Eq. (1). He takes the first quantum particles of these GHZ states to form sequence $S_{\rm A}$, the second quantum particles to form sequence $S_{\rm B}$, and the last particles used to check eavesdropping to form sequence $S_{\rm T}$, which were left in STP's hand. Then STP sends sequence $S_{\rm A}$ to Alice ($S_{\rm B}$ to Bob). We have

$$S_{\rm A}=S^1_{\rm A}S^2_{\rm A}S^3_{\rm A},\ldots,S^{4N(1+\delta)}_{\rm A},$$
$$S_{\rm B}=S^1_{\rm B}S^2_{\rm B}S^3_{\rm B},\ldots,S^{4N(1+\delta)}_{\rm B},$$
$$S_{\rm T}=S^1_{\rm T}S^2_{\rm T}S^3_{\rm T},\ldots,S^{4N(1+\delta)}_{\rm T}.$$

Step 2 After Alice (Bob) has received sequence $S_{\rm A}(S_{\rm B})$, she (he) will select either operation (1) or operation (2) according to the secure shared key in their hands. The detailed information is given in Table 1. If $K'^i_{\rm AB}$ is 00, both Alice and Bob will choose operation (1) on the particles at the same location. If $K'^i_{\rm AB}$ is 01(10), Bob (Alice) will select to measure the particles, record the measurement results $p_{\rm b}(p_{\rm a})$, and produce a new particle with the same state as the measurement result. If $K'^i_{\rm AB}$ is 11, both Alice and Bob will measure the particle, record measurement result $m_{\rm a}(m_{\rm b})$, and generate a new particle with the state as $S^i_{\rm A'}=x_i\oplus m^i_{\rm a}\oplus K^i_{\rm AB}$ ($S^i_{\rm B'}=y_i\oplus m^i_{\rm b}\oplus K^i_{\rm AB}$). After she (he) has finished the above operations, a new sequence $S_{\rm A'}$ ($S_{\rm B'}$) is formed. Finally, Alice (Bob) sends the new sequence $S_{\rm A'}$ ($S_{\rm B'}$) to STP. Here, it is necessary to explain that the two-classical participants do not know the corresponding relationship between the key $K'^i_{\rm AB}$ and the specific operation of their counterpart.

Table 1. Operations of Alice and Bob.

$K'^i_{\rm AB}$	Alice's operation	Bob's operation
00	Operation (1)	Operation (1)
01	Operation (1)	Operation (2): measure and record the measurement result as $p_{\rm b}$, then prepare a new particle in $\overline{Z}$ basis with the same state
10	Operation (2): measure and record the measurement result as $p_{\rm a}$, then prepare a new particle in $\overline{Z}$ basis with the same state	Operation (1)
11	Operation (2): measure and record the measurement result as $m_{\rm a}$ and prepare a new state in $\overline{Z}$ basis with $S^i_{\rm A'}=x_i\oplus m^i_{\rm a}\oplus K^i_{\rm AB}$	Operation (2): measure and record the measurement result as $m_{\rm b}$ and prepare a new state in $\overline{Z}$ basis with $S^i_{\rm B'}=y_i\oplus m^i_{\rm b}\oplus K^i_{\rm AB}$

Step 3 STP informs Alice and Bob of his receipts and stores sequences $S_{\rm A'}$ and $S_{\rm B'}$ in quantum memory. After that, Alice and Bob announce the operations performed on particles to STP. Based on the announced information, STP selects to

execute the corresponding operations demonstrated in Table 2 on these received particles.

Case 1 If both Alice and Bob choose to execute operation (1) on the received particles at the same location (K'^{i}_{AB} is 00), then STP will perform d-dimensional Bell state measurement on the received particles A and B (action 1). It is well known that three-particle GHZ state can be expressed as

$$\begin{aligned}
\phi_{\mathrm{ABT}} &= \frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle_{\mathrm{AB}}\left|x+\right\rangle_{\mathrm{T}}+\left|\phi^{-}\right\rangle_{\mathrm{AB}}\left|x-\right\rangle_{\mathrm{T}}\right),\\
\phi_{\mathrm{ABT}} &= \frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle_{\mathrm{BT}}\left|x+\right\rangle_{\mathrm{A}}+\left|\phi^{-}\right\rangle_{\mathrm{BT}}\left|x-\right\rangle_{\mathrm{A}}\right),\\
\phi_{\mathrm{ABT}} &= \frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle_{\mathrm{AT}}\left|x+\right\rangle_{\mathrm{B}}+\left|\phi^{-}\right\rangle_{\mathrm{AT}}\left|x-\right\rangle_{\mathrm{B}}\right). \qquad (4)
\end{aligned}$$

From Eq. (4), STP could know whether there is an eavesdropper or not by comparing the measurement outcomes with the initial states. If the Bell measurement is $|\phi^{+}\rangle_{\mathrm{AB}}$, then there is no eavesdropping, this protocol will proceed to the next case. Otherwise, they will abort the protocol.

Case 2 If Alice chooses to apply operation (1) and Bob executes operation (2) on the received particles at the same location (K'^{i}_{AB} is 01), then STP will implement action 2 (STP executes d-dimensional Bell state measurement on particles A and T). From Eq. (4), STP could know whether there is an eavesdropper or not by comparing the measurement outcomes with the initial states. If the Bell measurement is $|\phi^{+}\rangle_{\mathrm{AT}}$, then there is no eavesdropping, this protocol will proceed to the next case. Otherwise, they will abort the protocol.

Case 3 If Alice chooses to apply operation (2) and Bob executes operation (1) (K'^{i}_{AB} is 10) on the received particles at the same location, then STP will implement action 3 (STP performs d-dimensional Bell state measurement on particles B and T). From Eq. (4) STP could know whether there exists an eavesdropper or not by comparing the measurement outcomes with the initial states. If the Bell measurement is $|\phi^{+}\rangle_{\mathrm{BT}}$, then there is no eavesdropping, this protocol will proceed to the next case. Otherwise, they will abort the protocol.

Case 4 If both Alice and Bob choose to apply operation (2) on the received particles at the same location, then STP will implement action 4 (STP calculates $T_i = S^{i}_{\mathrm{A}'} \ominus S^{i}_{\mathrm{B}'} \oplus u_2$, where $\ominus$ represents the module d subtraction). STP can obtain the calculated results $\mathrm{sign}[T_i]$,

$$\mathrm{sign}[T_i] = \begin{cases} -1, & h-1 < T_i \le 2h-2;\\ 0, & T_i = 0;\\ 1, & 0 < T_i \le h-1. \end{cases} \qquad (5)$$

Finally, STP tells Alice and Bob $\mathrm{sign}[T_i]$. Based on Eq. (5), Alice and Bob can deduce the size relationship of their privacies between them easily from the values of $\mathrm{sign}[T_i]$,

$$\mathrm{sign}[T_i] = \begin{cases} 1, & x_i > y_i;\\ 0, & x_i = y_i;\\ -1, & x_i < y_i. \end{cases} \qquad (6)$$

Table 2. Actions of STP.

K'^{i}_{AB}	Actions of STP
00	Action 1: STP performs d-dimensional Bell state measurement on the received particles A and B
01	Action 2: STP executes d-dimensional Bell state measurement on particles A and T
10	Action 3: STP performs d-dimensional Bell state measurement on particles B and T
11	Action 4: STP calculates $T_i = S^{i}_{\mathrm{A}'} \ominus S^{i}_{\mathrm{B}'} \oplus u_2$

3. Correctness analyses

3.1. Output correctness

Supposing that both Alice and Bob measure the particles on their received one with $\overline{Z}$ basis separately at the same location, the d-dimensional GHZ state will collapse into $|k\rangle\,|k\oplus u_2\rangle\,|k\oplus u_3\rangle$ according to Eq. (1). Therefore, $m^{i}_{\mathrm{a}} \ominus m^{i}_{\mathrm{b}} \oplus u_2 = 0$ can be easily derived by STP. After he has received the values of $S^{i}_{\mathrm{A}'}$ and $S^{i}_{\mathrm{B}'}$, T_i can be calculated as

$$\begin{aligned}
T_i &= S^{i}_{\mathrm{A}'} \ominus S^{i}_{\mathrm{B}'} \oplus u_2\\
&= \left(x_i \oplus m^{i}_{\mathrm{a}} \oplus K^{i}_{\mathrm{AB}}\right) \ominus \left(y_i \oplus m^{i}_{\mathrm{b}} \oplus K^{i}_{\mathrm{AB}}\right) \oplus u_2\\
&= \left(x_i \ominus y_i\right) \oplus \left(m^{i}_{\mathrm{a}} \ominus m^{i}_{\mathrm{b}}\right) \oplus u_2\\
&= x_i \ominus y_i. \qquad (7)
\end{aligned}$$

From Eqs. (5) and (6), one can see that if the value of T_i is greater than 0 and less than h, then STP could obtain $\mathrm{sign}[T_i] = 1$, so $x_i > y_i$, otherwise $x_i \le y_i$.

3.2. Examples

Some examples are given for better understanding the presented protocol. Suppose that the initial state of d-dimensional GHZ state prepared by TP is $|\phi_{1,2,3}\rangle$ and d is 9. Thus, $u_1 = 1$, $u_2 = 2$, $u_3 = 3$, $h = 5$. Alice and Bob have the secret integers $x_i = 3$ and $y_i = 4$, respectively, which need to be compared. They share a secret key 2 in advance. When both Alice and Bob implement operation (2), they could obtain measurements $m^{i}_{\mathrm{a}} = 2$ and $m^{i}_{\mathrm{b}} = 4$, respectively. Based on the above appointment, STP can calculate the values of $S^{i}_{\mathrm{A}'}$ ($S^{i}_{\mathrm{A}'} = x_i \oplus m^{i}_{\mathrm{a}} \oplus K^{i}_{\mathrm{AB}} = 3 \oplus 2 \oplus 2 = 7$), $S^{i}_{\mathrm{B}'}$ ($S^{i}_{\mathrm{B}'} = y_i \oplus m^{i}_{\mathrm{b}} \oplus K^{i}_{\mathrm{AB}} = 4 \oplus 4 \oplus 2 = 1$) and T_i ($T_i = S^{i}_{\mathrm{A}'} \ominus S^{i}_{\mathrm{B}'} \oplus u_2 = 7 \ominus 1 \oplus 2 = 8$). Thus, STP can obtain $\mathrm{sign}[T_i] = -1$, then he can conclude $x_i < y_i$. In fact, $x_i = 3$ and $y_i = 4$, $3 < 4$, which confirms that STP can give correct calculation result. To further clarify this process, Table 3 shows the relation of essential parameters.

From the examples listed in Table 3, one can see that two participants can achieve a private comparison by the proposed protocol. Meanwhile, it is evident that the correctness and the effectiveness are satisfied.

Table 3. Relation of essential indexes for some examples.

Initial state	$d(h)$	x_i	y_i	K^i_{AB}	m^i_a	m^i_b	$S^i_{A'}$	$S^i_{B'}$	T_i	sign$[T_i]$	Size relationship
		3	1	2	3	5	8	8	2	1	$x_i > y_i$
$\|\phi_{023}\rangle$	9(5)	3	3	2	4	6	0	2	0	0	$x_i = y_i$
		3	4	2	4	6	0	3	8	1	$x_i < y_i$
		4	2	2	3	6	9	10	2	1	$x_i > y_i$
$\|\phi_{034}\rangle$	11(6)	4	4	2	4	7	10	2	0	0	$x_i = y_i$
		4	5	2	5	8	0	4	7	-1	$x_i < y_i$
		5	3	3	4	8	12	1	2	1	$x_i > y_i$
$\|\phi_{045}\rangle$	13(7)	5	5	3	5	9	0	4	0	0	$x_i = y_i$
		5	7	3	6	10	1	7	11	-1	$x_i < y_i$

4. Security analysis

4.1. External attack

Eve, an external attack, wants to steal the information from the participants including STP, Alice and Bob. It is well known that as long as there are particles transmitting in the channel, Eve may use many common attacks to obtain some useful information, such as the intercept-measure-resend attack, the entanglement attack and the Trojan horse attack. Next, the security of the proposed protocol will be analyzed.

4.1.1. Intercept-measure-resend attack

In step 1, there are transmissions of particles. Suppose that Eve implements the intercept-measure-resend attack, she would intercept the particles transmitted from STP to Alice (Bob) and measure them with single measurement. Subsequently, she produces new particles whose states are same as the measurement results and sends them to Alice (Bob). Although Eve could not be perceived in cases 4 and 3 (2), her measurement will destroy the correlation of states in cases 1 and 2 (3). From Eq. (4) and Table 2, one can obtain the following details:

In case 1, Eves' measurement will destroy the correlation of d-dimensional Bell state on particles A and B.

In case 2 (3), Eves' measurement on particle A (B) will destroy the correlation of d-dimensional Bell state on particles A (B) and T.

If Eve implements the intercept-measure-resend attack to each particle from sequence $S_A(S_B)$, the probability that she was not found is 1/2. Thus, the total probability p that he would not be detected is $1/2^{4N}$, where $4N$ is the total number of GHZ states prepared by STP. Via preparing plenty of d-dimensional GHZ states, the probability that STP detects Eve's operation is approximately 1. It can be concluded that Eve cannot obtain any information about the secrets X and Y from Alice and Bob by launching the intercept-measure-resend attack without being discovered in step 1.

In step 2, Alice (Bob) sends sequence $S_{A'}$ ($S_{B'}$) to STP. Although there are transmissions of particles, Eve does not know the choice of Alice (Bob) in advance and cannot do exactly as what Alice (Bob) does. Provided that Eve conducts measurement on these particles in cases 1, 2 and 3, it will cause errors and destroy the correlation of these Bell states. In case 4, though Eve may get the values of $S^i_{A'}$ and $S^i_{B'}$, she does not know m^i_a and m^i_b. Therefore, it can be concluded that Eve cannot obtain any information about secrets X and Y from Alice and Bob by launching the intercept-measure-resend attack in step 2.

In step 3, because there is no particle transmission, the secrets of X and Y will not leak.

4.1.2. Entangle attack

When the particles were transmitted in the quantum channel, Eve may use entanglement attack to obtain more information. First, Eve will apply unitary operation U_E, and then she will attach an auxiliary entanglement state $|E\rangle$ to these particles as follows:[39]

$$U_E|k\rangle|E\rangle = \sum_{l=0}^{d-1} a_{lk}|l\rangle|\varepsilon_{lk}\rangle, \tag{8}$$

$$\begin{aligned} U_E|J_j\rangle|E\rangle &= U_E\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}|k\rangle\right)|E\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}U_E|k\rangle|E\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}\sum_{l=0}^{d-1}a_{lk}|l\rangle|\varepsilon_{lk}\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\omega^{kj}a_{lk}\left(\frac{1}{\sqrt{d}}\sum_{m=0}^{d-1}\omega^{-ml}|J_m\rangle\right)|\varepsilon_{lk}\rangle \\ &= \frac{1}{d}\sum_{k,l,m=0}^{d-1}\omega^{kj-ml}a_{lk}|J_m\rangle|\varepsilon_{lk}\rangle, \end{aligned} \tag{9}$$

where $|\varepsilon_{lk}\rangle$ $(l,k=0,1,\ldots,d-1)$ is the pure auxiliary state determined by the unitary transform U_E, $F|j\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}|k\rangle$ is represented as $|J_j\rangle$ and $\sum_{l=0}^{d-1}|a_{lk}|^2 = 1$. For fear of introducing the error rate for these states, Eve has no choice but to set $a_{lk} = 0$, where $l \neq k$. Thus, Eqs. (8) and (9) can be written as

$$U_E|k\rangle|E\rangle = a_{kk}|k\rangle|\varepsilon_{kk}\rangle, \tag{10}$$

$$U_E|J_j\rangle|E\rangle = \frac{1}{d}\sum_{k,m=0}^{d-1}\omega^{k(j-m)}a_{kk}|J_m\rangle|\varepsilon_{kk}\rangle. \tag{11}$$

Similarly, Eve only obtains $\sum_{k=0}^{d-1}\omega^{k(j-m)}a_{kk}\left|\varepsilon_{kk}\right\rangle=0$, where $m,j\in\{0,1,\ldots,d-1\}$ and $m\neq j$. When Eve performs U_E on the first particle of a d-dimensional GHZ state, the whole system will be obtained from Eqs. (1) and (10),

$$\begin{aligned}&U_E\left|\phi_{0,u_2,u_3}\right\rangle\left|E\right\rangle\\=&\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}U_E\left|k\right\rangle\left|k\oplus u_2\right\rangle\left|k\oplus u_3\right\rangle\left|E\right\rangle\\=&\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}a_{kk}\left|\varepsilon_{kk}\right\rangle\left|k\right\rangle\left|k\oplus u_2\right\rangle\left|k\oplus u_3\right\rangle.\end{aligned}\tag{12}$$

With Eqs. (10)–(12), one can know

$$a_{00}\left|\varepsilon_{00}\right|=\alpha_{11}\left|\varepsilon_{11}\right|=\cdots=\alpha_{(d-1)(d-1)}\left|\varepsilon_{(d-1)(d-1)}\right|.\tag{13}$$

Equation (13) tells us that Eve does not discriminate $|\varepsilon_{00}|$ from others. That is to say, Eve cannot obtain any information from the particles transmitted in quantum channel by launching entanglement attack on our protocol.

4.1.3. Trojan horse attack

Since the particles prepared by STP in the beginning are transmitted in a round trip in our protocol, Trojan horse attack should be considered as an outside eavesdropper, which generally includes invisible photon eavesdropping attack and delay-photon attack.[42,43] To resist these kinds of attacks, every participant should be equipped with photon filter and photon number splitter. For example, the particle receiver inserts a photon filter in the front of her (his) devices to filter out the photon signal with an illegitimate wavelength, which can withstand the invisible photon eavesdropping and the Trojan horse attack.

4.2. Internal attack

Participant attack, an attack from dishonest participant, is more powerful.[44] We will analyze the attacks from two types of participants, i.e., dishonest Alice (Bob) and semi-dishonest TP.

4.2.1. Attack from dishonest Alice (Bob)

Without loss of generality, the role of Alice is similar to Bob's. One only analyzes the chance of Alice stealing Bob's key. Alice (Bob) attempts to obtain some information $S_{\rm B}$ ($S_{\rm A}$) from step 1 and $S_{\rm B'}$ ($S_{\rm A'}$) from step 2.

In steps 1 and 2, although Alice and Bob shared the same key, they do not know the corresponding rules between the keys and the specific operation of the other participant. Therefore, Alice's (Bob's) attack will be detected as an external attack as described in Section 4.11. Hence, one can draw a conclusion that Alice (Bob) could not have the knowledge of secret X (Y).

4.2.2. Attack from semi-dishonest TP

We know that STP can obtain the information from $S_{\rm A}$ ($S_{\rm B}$) and $S_{\rm A'}$ ($S_{\rm B'}$) easily, which provides him more power to attack the protocol. However, since $K_{\rm AB}$ is distributed between Alice and Bob via a secure QKD protocol, STP is unable to learn the value of $K_{\rm AB}$. That is, STP cannot learn any information from the secrets X and Y by launching the internal attack.

5. Discussion

The comparisons among our protocol and those previous typical SQPC protocols in Refs. [35–37] are compiled in Table 4.

Like the protocol in Ref. [37], our protocol could also compare the size relation of two classical participants' input integers, while the SQPC protocol in Refs. [35,36] only could compare the equality of them.

It is well known that the qubit efficiency is expressed as $e=b_{\rm c}/b_{\rm t}$, where $b_{\rm c}$ is the number of compared bits in each comparison and $b_{\rm t}$ is the total number of generated particles in each comparison. Applying our protocol to compare two-party secrets of 2 bits, TP should produce four d-dimensional GHZ states, i.e., twelve particles. Alice (Bob) selects operation (1) or (2) with equal probability, two $\overline{Z}$ basis particles are generated by her (him). Therefore, the qubit efficiency of our protocol is 12.5%. Although most of the protocols mentioned in Table 4 need to share the key in advance, the qubit efficiency of our protocol is the highest, while that in Ref. [35] is the lowest.

Table 4. Comparisons between our SQPC and those previous SQPC protocols.

	Ref. [35]	Ref. [36]	Ref. [37]	Our protocol
Quantum resource	single photon	d-dimensional Bell state	d-dimensional Bell state	d-dimensional GHZ state
Category of QPC	equality	equality	size	size
Qubit efficiency	1/48	2/49	1/12	1/8
Need of classical authentication channel	yes	no	yes	no
Transmission channel of encrypted privacy	classical authentication channel	quantum channel	classical authentication channel	quantum channel
Secure	yes	yes	yes	yes

The classical participants do not need to prepare classical authentication channel in our protocol in advance, which makes the private comparison easier to operate. In addition, the encrypted privacies $S^i_{A'} = x_i \oplus m^i_a \oplus K^i_{AB}$ and $S^i_{B'} = y_i \oplus m^i_b \oplus K^i_{AB}$ are sent to STP via quantum channel, which reduces the probability of information leakage.

In our protocol, all participants hardly disclose any information about particles including the position and values of some particles, which can also greatly reduce the possibility of information leakage.

6. Conclusion

Based on the entangled d-dimensional GHZ states, a new efficient semi-quantum private comparison protocol is presented with the help of a semi-honest TP. Our protocol can compare the size relation of private information between two classical participants. Compared to existing SQPC protocols, our protocol could achieve higher qubit efficiency.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 62161025 and 61871205), the Project of Scientific and Technological Innovation Base of Jiangxi Province, China (Grant No. 20203CCD46008), and the Jiangxi Provincial Key Laboratory of Fusion and Information Control, China (Grant No. 20171BCD40005).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the International Conference on Computers, Systems and Signal Processing*, December 1984, Bangalore, India, pp. 175–179
[2] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[3] Zhang Y and Ni Q 2020 *Quantum Eng.* **2** e31
[4] Yin Z Q, Lu F Y, Teng J, Wang S, Chen W, Guo G C and Han Z F 2021 *Fundam. Res.* **1** 93
[5] Guo H, Li Z Y, Yu S and Zhang Y C 2021 *Fundam. Res.* **1** 96
[6] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[7] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev. A* **69** 052307
[8] Gao Z K, Li T and Li Z H 2020 *Sci. Chin. Phys. Mech. Astron.* **63** 120311
[9] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[10] Chang Y, Xu C X, Zhang S B and Yan L L 2014 *Chin. Sci. Bull.* **59** 2541
[11] Wang C 2021 *Fundam. Res.* **1** 91
[12] Chen X B, Sun Y R, Xu G and Yang Y X 2019 *Inf. Sci.* **501** 172
[13] Xu G, Shan R T, Chen X B, Dong M and Chen Y L 2021 *Comput. Mater. Continua* **69** 339
[14] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[15] Chen X B, Xu G, Niu, X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561
[16] Qiang X G, Zhou X Q, Aungskunsiri K, Cable H and O'Brien J L 2017 *Quantum Sci. Technol.* **2** 045002
[17] Long G L 2006 *Commun. Theor. Phys.* **45** 825
[18] Jia H Y, Wen Q Y, Song T T and Gao F 2011 *Opt. Commun.* **284** 545
[19] Tseng H Y, Lin J and Hwang T 2012 *Quantum Inf. Process* **11** 373
[20] Li J, Zhou H F, Jia L and Zhang T T 2014 *Int. J. Theor. Phys.* **53** 2167
[21] Chang Y, Zhang W B, Zhang S B, Wang H C, Yan L L, Han G H, Sheng Z W, Huang Y Y, Suo W and Xiong J X 2016 *Commun. Theor. Phys.* **66** 621
[22] Xu G, Xiao K, Li Z, Niu X X and Ryan M 2019 *Comput. Mater. Continua* **58** 809
[23] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[24] Boyer M, Gelles R, Kenigsberg D and Mor T 2009 *Phys. Rev. A* **79** 032341
[25] Zou X F, Qiu D W, Li L Z, Wu L H and Li L J 2009 *Phys. Rev. A* **79** 052312
[26] Wang J, Zhang S, Zhang Q and Tang C J 2011 *Chin. Phys. Lett.* **28** 100301
[27] Yu K F, Yang C W, Liao C H and Hwang T 2014 *Quantum Inf. Process* **13** 1457
[28] Krawec W O 2015 *Phys. Rev. A* **91** 032323
[29] Liu Z R and Hwang T 2018 *Ann. Phys.* **530** 1700206
[30] Li Q, Chan W H and Long D Y 2010 *Phys. Rev. A* **82** 022303
[31] Yang C W and Hwang T 2013 *Int. J. Quantum Inf.* **11** 1350052
[32] Chou W H, Hwang T and Gu J 2016 arXiv:1607.07961 [quant-ph]
[33] Thapliyala K, Sharma R D and Pathak A 2018 *Int. J. Quantum Inf.* **16** 1850047
[34] Ye T Y and Ye C Q 2018 *Int. J. Theor. Phys.* **57** 3819
[35] Lin P H, Hwang T and Tsai C W 2019 *Quantum Inf. Process* **18** 207
[36] Jiang L Z 2020 *Quantum Inf. Process* **19** 180
[37] Zhou N R, Xu Q D, Du N S and Gong L H 2021 *Quantum Inf. Process* **20** 124
[38] Lo H K 1997 *Phys. Rev. A* **56** 1154
[39] Bai C M, Li Z H, Xu T T and Li Y M 2017 *Quantum Inf. Process* **16** 59
[40] Rahaman R and Parker M G 2015 *Phys. Rev. A* **91** 022330
[41] Cao H, Ma W P, Lü L D, He Y F and Liu G 2019 *Quantum Inf. Process* **18** 287
[42] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329
[43] Ding Y H, Bacco D, Dalgaard K, Cai X L, Zhou X Q, Rottwitt K and Oxenlowe L K 2017 *NPJ Quantum Inf.* **3** 25
[44] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145