Quantum Information Processing (2023) 22:255
https://doi.org/10.1007/s11128-023-03999-y

Quantum private comparison protocol based on 4D GHZ-like states

Chao Liu[1] · Shun Zhou[2] · Li-Hua Gong[2] · Hua-Ying Chen[3]

Received: 31 December 2022 / Accepted: 17 May 2023 / Published online: 24 June 2023

Abstract
This paper proposes a new private comparison protocol based on four-dimensional three-particle GHZ-like states. The QPC protocol allows two participants with limited quantum abilities to compare their private information whether they are equal or not with the help of a semi-honest third party. The semi-honest third party means that it may be unfaithful on his own behavior, though it will execute the protocol loyally. The presented QPC protocol not only reduces the requirement on quantum operations without involving the unitary operation, but it also requires only the single-particle measurement. The quantum circuit of the six-qubit state and the measurement results are presented under the IBM Quantum Experimental platform. The correctness and the effectiveness of the suggested protocol are illustrated with some examples. In addition, detailed security analysis demonstrates that the proposed two-party QPC protocol is secure against the internal and external attacks.

Keywords Quantum private comparison protocol · Single-particle measurement · GHZ-like state · Semi-honest third party · Quantum cryptography

1 Introduction

The security problem of information transmission has resulted in wide attention. However, to guarantee the security of information transmission, quantum cryptography, not underlying the computational hardness problems, has been conceived by Wiesner [1]. In 1984, Bennett et al. invented the first quantum key distribution (QKD)

✉ Hua-Ying Chen
chenhuaying@ncu.edu.cn

1 Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

2 School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Songjiang, Shanghai 201620, China

3 Department of Physics, Nanchang University, Nanchang 330031, China

protocol, which can achieve theoretically unconditional security [2]. Except QKD protocols [2–4], many quantum cryptography protocols have been invented to solve various security communication issues, such as quantum secure direct communication (QSDC) [5, 6], quantum secret sharing (QSS) [7–9], quantum key agreement (QKA) [10, 11].

In 1982, Andrew Yao introduced the concept of the millionaire problem [12], addressing whether two or more participants have the same secret information as each other without leaking their own secret information. After performing related research on the classical communication problems, multiparty secure computation, as a branch of cryptography, was born. Quantum private comparison (QPC) protocols were an important family member of multiparty secure computation. In 2009, Yang et al. designed the first QPC protocol based on Bell states, allowing two participants to compare the equality of their secrets with the assistance of a semi-honest third party (TP) and decoy photons [13]. Chen et al. invented an efficient QPC protocol with the triplet GHZ states by carrying out the simpler single-particle measurement [14]. Subsequently, different QPC protocols were designed based on different quantum entangled states, such as EPR pair [15], W state and Bell state [16], Bell state and five-qubit genuinely entangled state [17], cluster state and extended Bell state [18], GHZ state [19]. A two-party QPC protocol was put forward with the four-particle GHZ states, and greatly compared the equality of three information bits in each round of comparison to ensure relatively high efficiency [20]. Huang et al. utilized the entanglement swapping and GHZ-basis measurement to compare two parties' secrets practically [21]. A new QPC protocol was raised with the hyperentangled GHZ state to compare secret inputs securely and efficiently [22]. Huang et al. constructed a QPC protocol with arbitrary single-qubit states, which is easy to implement [23]. In addition, Xiao et al. designed a fault-tolerant QPC protocol to fulfill higher encoding efficiency by applying the classical linear block code [24].

These above-mentioned two-party QPC protocols were based on the low-dimensional single-particle states or low-dimensional entanglement states. Each particle can encode only one bit, thereby restricting the transmission efficiency of secret information. With the constantly increase of the number of dimensions, high-dimensional single-particle states or high-dimensional entangled states enables to encode much more information. From then on, many scholars started paying more attention on how to employ high-dimensional entanglement states to solve the two-party QPC protocols' problems. In 2011, Jia et al. first introduced the d-level GHZ states to compare two participants' privacies, which was able to solve the millionaire problem [25]. To improve the security of the protocol, the secret information can be coded into the phases of the d-level GHZ states by local operations and retrieved by the collective measurements of TP. In 2013, Yu et al. came up with a QPC protocol based on the d-level single-particle states and unitary operation, which can compare the size relationship of two parties' secrets [26]. Guo et al. proposed a QPC protocol with d-dimensional Bell states and bit-shifting operation, which is efficient and economic due to the property of entanglement swapping [27]. Subsequently, Li et al. applied the quantum Fourier transform and CNOT operation to provide higher communication efficiency by fulfilling the secret-by-secret comparison [28]. In 2021, Wu et al. designed a QPC protocol based on the d-level Bell states with a semi-honest

TP, which can determine the size relation of two participants' private data [29]. Wang et al. designed a multi-party QPC protocol to compare the size relation of secret information with the d-dimensional Bell states without involving the unitary operation [30]. To reduce the consumption of quantum devices, various semi-quantum private comparison (SQPC) protocols have been extensively studied recently. Zhou et al. designed a novel SQPC protocol with employing the entanglement correlation of the d-dimensional Bell states [31]. Wang et al. put forward a SQPC protocol with the d-dimensional GHZ states to compare the size of two clients' privacies [32]. In 2022, Luo et al. came up with a mediated semi-quantum QPC protocol based on the high-dimensional Bell states to solve the millionaires' problem [33]. Ye et al. designed a multi-party SQPC protocol based on the d-dimensional single-particle states, which can compare the size of multiple clients' secret inputs [34].

However, these above-mentioned high-dimensional entanglement states were conflicted to implement in physical experiments. In 2016, the first multi-photon (3, 3, 2) entangled state with particle numbers and dimensions greater than two was generated experimentally [35]. Xiang et al. put forward a QSS protocol with the 4D GHZ-like state, where each party needs to perform single-particle measurement [7]. In 2018, Erhard et al. created a three-particle GHZ state entangled in three levels for every particle to carry more information [36]. In 2020, Hu et al. applied the path mode of photons to prepare a real multi-particle (4, 4, 2) entangled state experimentally, which can construct more complicated high-dimensional quantum networks [37]. The tripartite layered quantum key distribution protocol with the (4, 4, 4) entangled state was presented to effectively ensure the fairness among the communication parties [38].

Enlightened by the work in [7], we come up with a new two-party QPC protocol based on the 4D GHZ-like entangled states, which can compare one classical bit in each comparison. Furthermore, with the help of decoy photons and QKD protocol, it can better check whether there exists the eavesdropper Eve.

The remaining parts of this paper are organized as follows. In Sect. 2, the quantum circuit and the measurement results are presented. In Sect. 3, the protocol is described in detail. In Sect. 4, the security and the correctness of our proposed protocol are analyzed. In Sect. 5, the proposed protocol is compared with the existing protocols, and a brief conclusion is given in Sect. 6.

2 Preliminaries

A four-dimensional three-particle entangled state, 4D GHZ-like state, is expressed as

$$|\zeta\rangle_{TAB} = \frac{1}{2}(|000\rangle + |111\rangle + |222\rangle + |333\rangle)_{TAB}. \quad (1)$$

To show online preparation and verification of 4D GHZ-like state better by applying the IBM Quantum Experimental platform [39], high-dimensional quantum entangled state is transformed into the two-dimensional quantum entangled state,

$$|0\rangle \rightarrow |00\rangle, |1\rangle \rightarrow |01\rangle, |2\rangle \rightarrow |10\rangle, |3\rangle \rightarrow |11\rangle. \tag{2}$$

The six-qubit entangled state is written as

$$|\zeta\rangle'_{TAB} = \frac{1}{2}(|000000\rangle + |010101\rangle + |101010\rangle + |111111\rangle)'_{TAB}. \tag{3}$$

It is clearly seen that the measurement results of the odd particles and the even particles are equal. Taking advantage of this property, the gate operations for preparing a six-qubit entangled state are shown in Fig. 1a, which consists of Hadamard operations and CNOT gate operations. To make the experiment more realistic, the simulation of the six-qubit state is performed by 5000 counts. The measurement results are described in Fig. 1b. In summary, it is verified that the scheme of preparing the six-qubit state is correct and feasible.

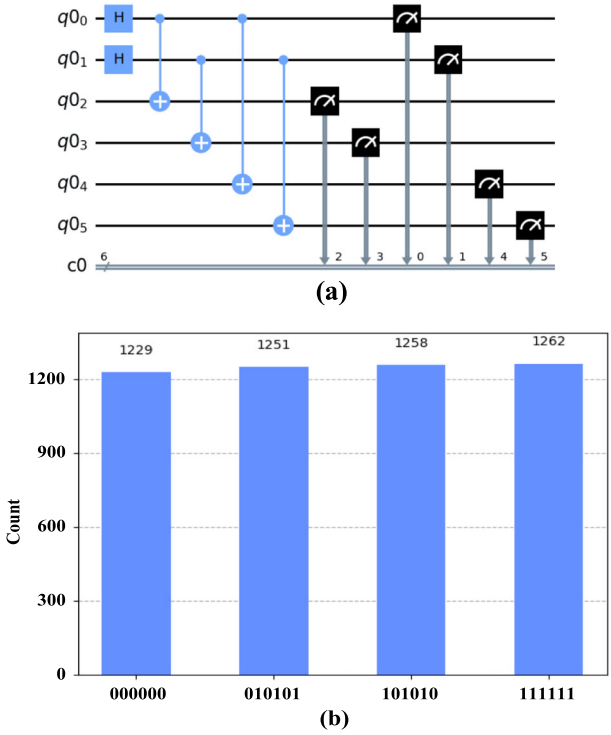

Fig. 1 Quantum circuit **a** and statistical diagram of measurement results **b** with the protocol

In the suggested protocol, two sets of orthogonal bases are Z-basis and X-basis, respectively. $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ belongs to Z-basis. $\{|e\rangle,|f\rangle,|g\rangle,|h\rangle\}$ is described as

$$|e\rangle=\frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle), \tag{4}$$

$$|f\rangle=\frac{1}{2}(|0\rangle - \mathrm{i}|1\rangle - |2\rangle + \mathrm{i}|3\rangle), \tag{5}$$

$$|g\rangle=\frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle), \tag{6}$$

$$|h\rangle=\frac{1}{2}(|0\rangle + \mathrm{i}|1\rangle - |2\rangle - \mathrm{i}|3\rangle). \tag{7}$$

where i is an imaginary number and $\mathrm{i}^2=-1$. If TP performs the single-qubit measurement on particle T in the state $|\zeta\rangle_{TAB}$ with X-basis, $|\zeta\rangle_{TAB}$ on particles A and B will collapse into one of the following results,

$$\langle e|\zeta\rangle_{TAB}=\frac{1}{2}(\langle 0|+\langle 1|+\langle 2|+\langle 3|) \times \frac{1}{2}(|000\rangle+|111\rangle+|222\rangle+|333\rangle)_{TAB} = \frac{1}{2}|\zeta\rangle_{AB}^{00}, \tag{8}$$

$$\begin{aligned}\langle f|\zeta\rangle_{TAB} =& \frac{1}{2}(\langle 0| - \mathrm{i}\langle 1| - \langle 2| + \mathrm{i}\langle 3|) \\ &\times \frac{1}{2}(|000\rangle + |111\rangle + |222\rangle + |333\rangle)_{TAB} = \frac{1}{2}|\zeta\rangle_{AB}^{01},\end{aligned} \tag{9}$$

$$\langle g|\zeta\rangle_{TAB}=\frac{1}{2}(\langle 0| - \langle 1|+\langle 2| - \langle 3|) \times \frac{1}{2}(|000\rangle+|111\rangle+|222\rangle+|333\rangle)_{TAB} = \frac{1}{2}|\zeta\rangle_{AB}^{10}, \tag{10}$$

$$\begin{aligned}\langle h|\zeta\rangle_{TAB} =& \frac{1}{2}(\langle 0| + \mathrm{i}\langle 1| - \langle 2| - \mathrm{i}\langle 3|) \\ &\times \frac{1}{2}(|000\rangle + |111\rangle + |222\rangle + |333\rangle)_{TAB} = \frac{1}{2}|\zeta\rangle_{AB}^{11}.\end{aligned} \tag{11}$$

Therefore, the quantum state $|\zeta\rangle_{TAB}$ is written as

$$|\zeta\rangle_{TAB} = \frac{1}{2}\Big(|e\rangle_T|\zeta\rangle_{AB}^{00} + |f\rangle_T|\zeta\rangle_{AB}^{01} + |g\rangle_T|\zeta\rangle_{AB}^{10} + |h\rangle_T|\zeta\rangle_{AB}^{11}\Big). \tag{12}$$

If TP performs the single-qubit measurement on particle A in the state $|\zeta\rangle_{AB}^{00}$ with X-basis, the quantum state $|\zeta\rangle_{AB}^{00}$ on particles B will collapse into one of the following four results:

$$\langle e|\zeta\rangle_{AB}^{00}=\frac{1}{2}(\langle 0|+\langle 1|+\langle 2|+\langle 3|) \times \frac{1}{2}(|00\rangle+|11\rangle+|22\rangle+|33\rangle)_{AB} = \frac{1}{2}|e\rangle_B, \tag{13}$$

$$\langle f|\zeta\rangle_{AB}^{00}=\frac{1}{2}(\langle 0|-\mathrm{i}\langle 1|-\langle 2|+\mathrm{i}\langle 3|)\times\frac{1}{2}(|00\rangle+|11\rangle+|22\rangle+|33\rangle)_{AB}=\frac{1}{2}|h\rangle_B, \quad (14)$$

$$\langle g|\zeta\rangle_{AB}^{00}=\frac{1}{2}(\langle 0|-\langle 1|+\langle 2|-\langle 3|)\times\frac{1}{2}(|00\rangle+|11\rangle+|22\rangle+|33\rangle)_{AB}=\frac{1}{2}|g\rangle_B, \quad (15)$$

$$\langle h|\zeta\rangle_{AB}^{00}=\frac{1}{2}(\langle 0|+\mathrm{i}\langle 1|-\langle 2|-\mathrm{i}\langle 3|)\times\frac{1}{2}(|00\rangle+|11\rangle+|22\rangle+|33\rangle)_{AB}=\frac{1}{2}|f\rangle_B. \quad (16)$$

Therefore, $|\zeta\rangle_{AB}^{00}$ is transformed as

$$|\zeta\rangle_{AB}^{00}=\frac{1}{2}(|e\rangle|e\rangle+|f\rangle|h\rangle+|g\rangle|g\rangle+|h\rangle|f\rangle)_{AB}. \quad (17)$$

According to Eqs. (8)–(11), the other states are denoted as

$$|\zeta\rangle_{AB}^{01}=\frac{1}{2}(|e\rangle|h\rangle+|f\rangle|g\rangle+|g\rangle|f\rangle+|h\rangle|e\rangle)_{AB}, \quad (18)$$

$$|\zeta\rangle_{AB}^{10}=\frac{1}{2}(|e\rangle|g\rangle+|f\rangle|f\rangle+|g\rangle|e\rangle+|h\rangle|h\rangle)_{AB}, \quad (19)$$

$$|\zeta\rangle_{AB}^{11}=\frac{1}{2}(|e\rangle|f\rangle+|f\rangle|e\rangle+|g\rangle|h\rangle+|h\rangle|g\rangle)_{AB}. \quad (20)$$

According to Eqs. (12), (17)–(20), $|\zeta\rangle_{TAB}$ is rewritten as

$$\begin{aligned}|\zeta\rangle_{TAB}=&\frac{1}{4}(|eee\rangle+|efh\rangle+|egg\rangle+|ehf\rangle)_{TAB}+\frac{1}{4}(|feh\rangle+|ffg\rangle+|fgf\rangle+|fhe\rangle)_{TAB}\\&+\frac{1}{4}(|geg\rangle+|gff\rangle+|gge\rangle+|ghh\rangle)_{TAB}+\frac{1}{4}(|hef\rangle+|hfe\rangle+|hgh\rangle+|hhg\rangle)_{TAB}.\end{aligned} \quad (21)$$

Consequently, TP, Alice and Bob perform the single-qubit measurement in the quantum state $|\zeta\rangle_{TAB}$ with X basis. In every measurement outcomes, the value of TP, Alice and Bob denote M_T^i, M_A^i and M_B^i, respectively, where $i=0,\ 1,\ \ldots,\ L-1$. For TP, Alice and Bob, $|e\rangle$, $|f\rangle$, $|g\rangle$, $|h\rangle$ represent 0, 1, 0, 1, respectively. Apparently, in the measurement outcomes, the value of TP, Alice and Bob satisfy

$$M_T^i\oplus M_A^i\oplus M_B^i=0. \quad (22)$$

3 Two-party QPC protocol based on the 4D GHZ-like states

Suppose there are two participants Alice and Bob, Alice has the secret information H, while Bob has the secret information J, where the binary representations of H and J in F_{2^L} are $(x_0,\ x_1,\ \ldots,\ x_{L-1})$ and $(y_0,\ y_1,\ \ldots,\ y_{L-1})$, respectively, where $x_i,\ y_i\in\{0,\ 1\}$, $H=\sum_{i=0}^{L-1}x_i2^i$ and $J=\sum_{i=0}^{L-1}x_i2^i$.

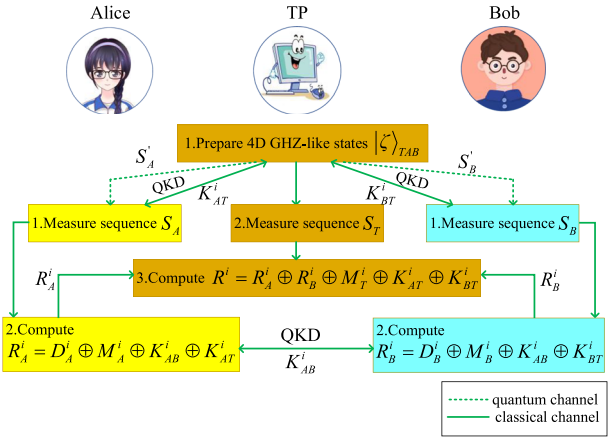

Fig. 2 The proposed QPC protocol based on the 4D GHZ-like states

In the meantime, Alice and TP, Bob and TP, Alice and Bob share a common key sequence K_{AT}, K_{BT} and K_{AB} by a secure QKD protocol as

$$K_{AT} = K_{AT}^0 K_{AT}^1 K_{AT}^2 \ldots K_{AT}^{L-1} \tag{23}$$

$$K_{BT} = K_{BT}^0 K_{BT}^1 K_{BT}^2 \ldots K_{BT}^{L-1} \tag{24}$$

$$K_{AB} = K_{AB}^0 K_{AB}^1 K_{AB}^2 \ldots K_{AB}^{L-1} \tag{25}$$

where K_{AT}^i, K_{BT}^i, $K_{AB}^i \in \{0, 1\}$. The process of the protocol is clearly depicted in Fig. 2.

Step 1 Alice (Bob) divides her (his) binary representation $H(J)$ into L groups $D_A^0, D_A^1, \ldots, D_A^{L-1}$ $\left(D_B^0, D_B^1, \ldots, D_B^{L-1}\right)$, where each group contains one binary bit.

Step 2 According to Eq. (1), TP generates L 4D three-particle quantum entanglement states to construct a quantum state sequence $\mathrm{P_T^0 P_A^0 P_B^0 P_T^1 P_A^1 P_B^1} \ldots \mathrm{P_T^{L-1} P_A^{L-1} P_B^{L-1}}$, where T, A, B denote three particles in one three-particle entanglement state and the superscripts denote the orders of three-particle entanglement state in this quantum state sequence. TP divides these three-particle quantum states to form three ordered Sequences S_T, S_A and S_B,

$$S_A = P_A^0 P_A^1 \ldots P_A^{L-1}, \tag{26}$$

$$S_B = P_B^0 P_B^1 \ldots P_B^{L-1}, \tag{27}$$

$$S_T = P_T^0 P_T^1 \ldots P_T^{L-1}. \tag{28}$$

Step 3 TP prepares two sets of decoy photons C_1 and C_2. Each decoy photon is randomly selected from the state set $\{|0\rangle,|1\rangle,|2\rangle,|3\rangle,|e\rangle,|f\rangle,|g\rangle,|h\rangle\}$. Then, TP randomly inserts C_1 (C_2) into Sequence S_A (S_B) to construct a new Sequence $S_A^{'}$ $\left(S_B^{'}\right)$. Finally, TP sends Sequences $S_A^{'}$ and $S_B^{'}$ to Alice and Bob, respectively, and retains Sequence S_T in his own hand.

Step 4 After confirming Alice (Bob) has received Sequence $S_A^{'}$ $\left(S_B^{'}\right)$, TP informs Alice (Bob) of the positions and the bases of every decoy photon in $S_A^{'}$ $\left(S_B^{'}\right)$. Then, Alice (Bob) performs the corresponding measurement on all decoy photons and notifies TP of the measurement results. TP judges whether there exists an eavesdropper. If the error rate is higher than expected, Alice (Bob) will abort the protocol and restart from Step 1; Otherwise, Alice (Bob) will discard all decoy photons in $S_A^{'}$ $\left(S_B^{'}\right)$ to restore original Sequence S_A (S_B) and continue the next step.

Step 5 Alice (Bob) measures the particle P_A^i $\left(P_B^i\right)$ in X basis and obtains M_A^i $\left(M_B^i\right)$. If the particle P_A^i (P_B^i) is $|e\rangle$ ($|f\rangle$), the value of M_A^i $\left(M_B^i\right)$ will be replaced by 0 (1). If the particle P_A^i(P_B^i) is $|g\rangle$ ($|h\rangle$), the value of M_A^i $\left(M_B^i\right)$ will be replaced by 0 (1). Subsequently, Alice (Bob) encrypts the private information such that $R_A^i = D_A^i \oplus M_A^i \oplus K_{AT}^i \oplus K_{AB}^i$ $\left(R_B^i = D_B^i \oplus M_B^i \oplus K_{BT}^i \oplus K_{AB}^i\right)$. In the end, Alice (Bob) delivers R_A (R_B) to TP via the classical channel, where $R_A=\left[R_A^0,\ R_A^1,\ldots,\ R_A^{L-1}\right]$ $\left(R_B=\left[R_B^0,\ R_B^1,\ldots,\ R_B^{L-1}\right]\right)$.

Step 6 TP measures the particle P_T^i in X basis and obtains M_T^i according to the measurement outcomes, where the measurement outcomes of P_T^i are shown in Table 1. Afterwards, TP calculates R^i, where $R^i \in \{0,\ 1\}$. If R^i is 0, TP will conclude that their privacies are equal; Otherwise, TP will consider that their privacies are different. Eventually, TP announces the comparison results to Alice (Bob) via a classical channel.

Table 1 The measurement outcomes of TP, Alice and Bob

TP	Alice	Bob	TP	Alice	Bob
$\|e\rangle$: 0	$\|e\rangle$: 0	$\|e\rangle$: 0	$\|f\rangle$: 1	$\|e\rangle$: 0	$\|h\rangle$: 1
	$\|f\rangle$: 1	$\|h\rangle$: 1		$\|f\rangle$: 1	$\|g\rangle$: 0
	$\|g\rangle$: 0	$\|g\rangle$: 0		$\|g\rangle$: 0	$\|f\rangle$: 1
	$\|h\rangle$: 1	$\|f\rangle$: 1		$\|h\rangle$: 1	$\|e\rangle$: 0
$\|g\rangle$: 0	$\|e\rangle$: 0	$\|g\rangle$: 0	$\|h\rangle$: 1	$\|e\rangle$: 0	$\|f\rangle$: 1
	$\|f\rangle$: 1	$\|f\rangle$: 1		$\|f\rangle$: 1	$\|e\rangle$: 0
	$\|g\rangle$: 0	$\|e\rangle$: 0		$\|g\rangle$: 0	$\|h\rangle$: 1
	$\|h\rangle$: 1	$\|h\rangle$: 1		$\|h\rangle$: 1	$\|g\rangle$: 0

4 Correctness and security

4.1 Correctness

According to Eq. (22), one can obtain

$$\begin{aligned} R^i =& R_A^i \oplus R_B^i \oplus M_T^i \oplus K_{AT}^i \oplus K_{BT}^i \\ =& \left(D_A^i \oplus M_A^i \oplus K_{AT}^i \oplus K_{AB}^i\right) \\ & \oplus \left(D_B^i \oplus M_B^i \oplus K_{BT}^i \oplus K_{AB}^i\right) \oplus M_T^i \oplus K_{AT}^i \oplus K_{BT}^i \\ =& \left(D_A^i \oplus D_B^i\right) \oplus \left(M_A^i \oplus M_B^i \oplus M_T^i\right) \\ =& D_A^i \oplus D_B^i. \end{aligned} \tag{29}$$

Therefore, the protocol is correct. If R^i is equal to 0, then D_A^i will be equal to D_B^i; Otherwise, $D_A^i \neq D_B^i$.

4.2 Security

Both participant attack and outside attack on the proposed protocol will be analyzed.

4.2.1 Participant attack

In the proposed protocol, we consider two cases of participant attacks. First of all, we analyze the security of the proposed protocol against the attacks of dishonest participants. Afterwards, the attack of semi-honest TP is also analyzed.

Case 1 Dishonest Alice (Bob) attempts to obtain Bob's (Alice's) privacies As an internal attacker, Alice (Bob) attempts to obtain Bob (Alice)'s privacies. In the protocol, Alice (Bob) does not transmit any information to Bob (Alice) except the pre-shared key K_{AB}. Alice (Bob) only knows $D_A^i, K_{AT}^i, K_{AB}^i, M_A^i$ $\left(D_B^i, K_{BT}^i, K_{AB}^i, M_B^i\right)$. If Alice (Bob) obtains P_B^i $\left(P_A^i\right)$ and R_B^i $\left(R_A^i\right)$, she (he) will be regarded as an outside attacker. Furthermore, Alice (Bob) cannot obtain K_{BT}^i $\left(K_{AT}^i\right)$ and D_B^i $\left(D_A^i\right)$. In addition, if Alice (Bob) achieves P_B^i $\left(P_A^i\right)$ and R_B^i $\left(R_A^i\right)$ without being discovered, Alice (Bob) will not access other participant's private information, since Alice (Bob) cannot obtain K_{BT}^i $\left(K_{AT}^i\right)$. Therefore, the privacies D_A^i $\left(D_B^i\right)$ are not eavesdropped in theory.

Case 2 Semi-honest TP tries to obtain (Alice's) Bob's privacies In the suggested protocol, TP obtains the shared secret keys K_{AT}^i, K_{BT}^i and knows R_A^i, R_B^i in Step 5. As a semi-honest third party, TP may acquire the secret information of Alice (Bob) through a quantum channel in Step 4. In a word, if TP attacks the transmitted information between TP and participants with evading detection, it will be also secure even with the assistance of these information $K_{AT}^i, K_{BT}^i, R_A^i, R_B^i$ in Case 2, since TP does not know

the pre-shared sequence K_{AB}. Therefore, TP cannot obtain any private information of participants. The protocol is secure against participant attacks.

4.2.2 Outsider attack

Suppose Eve is a malicious attacker, she attempts to steal the private information of participants. For this situation, we consider four cases of outside attacks.

Intercept-resend attack Eve intercepts Sequence $S_A^{'}\left(S_B^{'}\right)$ in Step 3 and then replaces Sequence $S_A^{'}\left(S_B^{'}\right)$ with a fake sequence. Afterwards, she sends the fake sequence to Alice (Bob). Unfortunately, Eve does not know the position and the preparation basis of every decoy photon in Sequence $S_A^{'}\left(S_B^{'}\right)$. Suppose Eve measures the decoy photon in Z-basis with Z-basis. It is known that she cannot be found in the eavesdropping detection. However, if she chooses X-basis to measure these decoy photons in Z-basis, there is a 25% probability for each photon to be eavesdropped. Therefore, based on the above two cases, the probability of avoiding Alice's (Bob's) detection is $\frac{5}{8}$. If there are v decoy photons, the probability of being detected will be $1-\left(\frac{5}{8}\right)^{v}$. If v is big enough, the probability is going to be close to 1. Therefore, the intercept-resend attack in the QPC protocol does not work.

Measure-resend attack The measure-resend attack is that the eavesdropper Eve intercepts the new Sequence $S_A^{'}\left(S_B^{'}\right)$ transmitted from TP to participants and then directly measures the particle $P_A^i\left(P_B^i\right)$. The new sequence $S_A^{'}\left(S_B^{'}\right)$ is randomly inserted with decoy particles. Subsequently, Eve still sends the measured sequence to participants. In this case, Eve is easily detected by the participants who perform the eavesdropping detection. Eve cannot distinguish the positions of decoy photons from Sequence $S_A^{'}\left(S_B^{'}\right)$, so it cannot acquire any useful information.

Entangle-measure attack Suppose Eve is a dishonest user. When the particle $P_A^i\left(P_B^i\right)$ is transmitted between TP and participants one by one, Eve may intercept the particle $P_A^i\left(P_B^i\right)$ in Step 3. Then, Eve prepares an auxiliary particle in $|\zeta\rangle_E$ and entangles it with the particle $P_A^i\left(P_B^i\right)$ sent between TP and participants via unitary operation U_E. This attack can be denoted as

$$U_E|l\rangle|\zeta\rangle_E=\sum_{\mu=0}^{3}\lambda_{l\mu}|\mu\rangle\left|\eta_{l\mu}\right\rangle_E. \tag{30}$$

According to Eq. (30), when $l,\ \mu\in\{0,\ 1,\ 2,\ 3\}$, one can analyze the effect of Eve's eavesdropping on the decoy photons $\{|0\rangle,\ |1\rangle,\ |2\rangle,\ |3\rangle\}$,

$$U_E|0\rangle|\zeta\rangle_{\mathrm{E}} = \lambda_{00}|0\rangle|\eta_{00}\rangle + \lambda_{01}|1\rangle|\eta_{01}\rangle + \lambda_{02}|2\rangle|\eta_{02}\rangle + \lambda_{03}|3\rangle|\eta_{03}\rangle, \quad (31)$$

$$U_E|1\rangle|\zeta\rangle_{\mathrm{E}} = \lambda_{10}|0\rangle|\eta_{10}\rangle + \lambda_{11}|1\rangle|\eta_{11}\rangle + \lambda_{12}|2\rangle|\eta_{12}\rangle + \lambda_{13}|3\rangle|\eta_{13}\rangle, \quad (32)$$

$$U_E|2\rangle|\zeta\rangle_{\mathrm{E}} = \lambda_{20}|0\rangle|\eta_{20}\rangle + \lambda_{21}|1\rangle|\eta_{21}\rangle + \lambda_{22}|2\rangle|\eta_{22}\rangle + \lambda_{23}|3\rangle|\eta_{23}\rangle, \quad (33)$$

$$U_E|3\rangle|\zeta\rangle_{\mathrm{E}} = \lambda_{30}|0\rangle|\eta_{30}\rangle + \lambda_{31}|1\rangle|\eta_{31}\rangle + \lambda_{32}|2\rangle|\eta_{32}\rangle + \lambda_{33}|3\rangle|\eta_{33}\rangle, \quad (34)$$

where $|\zeta\rangle_E$ is the initial state of ancillary particles. $\left|\eta_{l\mu}\right\rangle$ is a pure state uniquely determined by unitary operation. In addition, $\sum_{\mu=0}^{3}\left|\lambda_{l\mu}\right|^2 = 1$.

If Eve attempts to eavesdrop without being detected, $\lambda_{l\mu}$ must be 0 for the case that $l \neq \mu$. The decoy photons are in one of the eight states $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |e\rangle, |f\rangle, |g\rangle, |h\rangle\}$. Hence, if U_E acts on the decoy photons $|e\rangle$, $|f\rangle$, $|g\rangle$ and $|h\rangle$, one will obtain

$$\begin{aligned}
U_E|e\rangle|\zeta\rangle =& \frac{1}{2}(\lambda_{00}|0\rangle|\eta_{00}\rangle + \lambda_{11}|1\rangle|\eta_{11}\rangle + \lambda_{22}|2\rangle|\eta_{22}\rangle + \lambda_{33}|3\rangle|\eta_{33}\rangle)\\
=&\frac{1}{4}|e\rangle(\lambda_{00}|\eta_{00}\rangle + \lambda_{11}|\eta_{11}\rangle + \lambda_{22}|\eta_{22}\rangle + \lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|f\rangle(\lambda_{00}|\eta_{00}\rangle - \mathrm{i}\lambda_{11}|\eta_{11}\rangle - \lambda_{22}|\eta_{22}\rangle + \mathrm{i}\lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|g\rangle(\lambda_{00}|\eta_{00}\rangle - \lambda_{11}|\eta_{11}\rangle + \lambda_{22}|\eta_{22}\rangle - \lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|h\rangle(\lambda_{00}|\eta_{00}\rangle + \mathrm{i}\lambda_{11}|\eta_{11}\rangle - \lambda_{22}|\eta_{22}\rangle - \mathrm{i}\lambda_{33}|\eta_{33}\rangle), \quad (35)
\end{aligned}$$

$$\begin{aligned}
U_E|f\rangle|\zeta\rangle =& \frac{1}{2}(\lambda_{00}|0\rangle|\eta_{00}\rangle + \mathrm{i}\lambda_{11}|1\rangle|\eta_{11}\rangle - \lambda_{22}|2\rangle|\eta_{22}\rangle - \mathrm{i}\lambda_{33}|3\rangle|\eta_{33}\rangle)\\
=&\frac{1}{4}|e\rangle(\lambda_{00}|\eta_{00}\rangle + \mathrm{i}\lambda_{11}|\eta_{11}\rangle - \lambda_{22}|\eta_{22}\rangle - \mathrm{i}\lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|f\rangle(\lambda_{00}|\eta_{00}\rangle + \lambda_{11}|\eta_{11}\rangle + \lambda_{22}|\eta_{22}\rangle + \lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|g\rangle(\lambda_{00}|\eta_{00}\rangle - \mathrm{i}\lambda_{11}|\eta_{11}\rangle - \lambda_{22}|\eta_{22}\rangle + \mathrm{i}\lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|h\rangle(\lambda_{00}|\eta_{00}\rangle - \lambda_{11}|\eta_{11}\rangle + \lambda_{22}|\eta_{22}\rangle - \lambda_{33}|\eta_{33}\rangle), \quad (36)
\end{aligned}$$

$$\begin{aligned}
U_E|g\rangle|\zeta\rangle =& \frac{1}{2}(\lambda_{00}|0\rangle|\eta_{00}\rangle - \lambda_{11}|1\rangle|\eta_{11}\rangle + \lambda_{22}|2\rangle|\eta_{22}\rangle - \lambda_{33}|3\rangle|\eta_{33}\rangle)\\
=&\frac{1}{4}|e\rangle(\lambda_{00}|\eta_{00}\rangle - \lambda_{11}|\eta_{11}\rangle + \lambda_{22}|\eta_{22}\rangle - \lambda_{33}|\eta_{33}\rangle)\\
&+\frac{1}{4}|f\rangle(\lambda_{00}|\eta_{00}\rangle + \mathrm{i}\lambda_{11}|\eta_{11}\rangle - \lambda_{22}|\eta_{22}\rangle - \mathrm{i}\lambda_{33}|\eta_{33}\rangle)
\end{aligned}$$

$$+\frac{1}{4}|g\rangle(\lambda_{00}|\eta_{00}\rangle+\lambda_{11}|\eta_{11}\rangle+\lambda_{22}|\eta_{22}\rangle+\lambda_{33}|\eta_{33}\rangle)$$
$$+\frac{1}{4}|h\rangle(\lambda_{00}|\eta_{00}\rangle-\mathrm{i}\lambda_{11}|\eta_{11}\rangle-\lambda_{22}|\eta_{22}\rangle+\mathrm{i}\lambda_{33}|\eta_{33}\rangle), \quad (37)$$

$$\begin{aligned}U_E|h\rangle|\zeta\rangle &= \frac{1}{2}(\lambda_{00}|0\rangle|\eta_{00}\rangle-\mathrm{i}\lambda_{11}|1\rangle|\eta_{11}\rangle-\lambda_{22}|2\rangle|\eta_{22}\rangle+\lambda_{33}|3\rangle|\eta_{33}\rangle)\\ &=\frac{1}{4}|e\rangle(\lambda_{00}|\eta_{00}\rangle-\mathrm{i}\lambda_{11}|\eta_{11}\rangle-\lambda_{22}|\eta_{22}\rangle+\mathrm{i}\lambda_{33}|\eta_{33}\rangle)\\ &\quad+\frac{1}{4}|f\rangle(\lambda_{00}|\eta_{00}\rangle-\lambda_{11}|\eta_{11}\rangle+\lambda_{22}|\eta_{22}\rangle-\lambda_{33}|\eta_{33}\rangle)\\ &\quad+\frac{1}{4}|g\rangle(\lambda_{00}|\eta_{00}\rangle+\mathrm{i}\lambda_{11}|\eta_{11}\rangle-\lambda_{22}|\eta_{22}\rangle-\mathrm{i}\lambda_{33}|\eta_{33}\rangle)\\ &\quad+\frac{1}{4}|h\rangle(\lambda_{00}|\eta_{00}\rangle+\lambda_{11}|\eta_{11}\rangle+\lambda_{22}|\eta_{22}\rangle+\lambda_{33}|\eta_{33}\rangle). \quad (38)\end{aligned}$$

If Eve is not being detected, the following equations will hold

$$\begin{cases}\lambda_{00}|\eta_{00}\rangle-\mathrm{i}\lambda_{11}|\eta_{11}\rangle-\lambda_{22}|\eta_{22}\rangle+\mathrm{i}\lambda_{33}|\eta_{33}\rangle=0\\ \lambda_{00}|\eta_{00}\rangle-\lambda_{11}|\eta_{11}\rangle+\lambda_{22}|\eta_{22}\rangle-\lambda_{33}|\eta_{33}\rangle=0\\ \lambda_{00}|\eta_{00}\rangle+\mathrm{i}\lambda_{11}|\eta_{11}\rangle-\lambda_{22}|\eta_{22}\rangle-\mathrm{i}\lambda_{33}|\eta_{33}\rangle=0\end{cases}. \quad (39)$$

According to Eq. (39), one can conclude

$$\lambda_{00}|\eta_{00}\rangle=\lambda_{11}|\eta_{11}\rangle=\lambda_{22}|\eta_{22}\rangle=\lambda_{33}|\eta_{33}\rangle. \quad (40)$$

It can be seen that Eve cannot distinguish $\lambda_{00}|\eta_{00}\rangle$, $\lambda_{11}|\eta_{11}\rangle$, $\lambda_{22}|\eta_{22}\rangle$ and $\lambda_{33}|\eta_{33}\rangle$ by only measuring her ancillary particles. In a word, if Eve attempts to obtain any private information, it is apparent that she will inevitably introduce errors and her entangle-measure attack will also easily be found during the eavesdropping detection. Therefore, the protocol can resist the entangle-measure attack.

Trojan horse attack In this proposed one-way communication protocol, qubits are only transmitted from TP to participants. Therefore, it is immune to Trojan horse attacks. Although the attacker can inject some spy photons into the original qubits, they have no opportunity to extract Sequence S_A (S_B), since the spy photons cannot be retrieved. Thus, this protocol naturally avoids the Trojan horse attack. Therefore, Alice (Bob) does not require to install expensive devices (such as filter and photon number splitters) in the front of its quantum signal receiver. To sum up, Eve cannot obtain (Alice's) Bob's private information from the Trojan horse attack.

5 Comparison

The qubit efficiency is defined as $\theta = \tau_u/\tau_a$, where τ_u is the number of compared bits in each round of comparison while τ_a is the total number of prepared particles

and consumed decoy photons in each round of comparison. As shown in Table 2, the number of prepared particles is same as that the number of the consumed decoy photons in each comparison time. The suggested protocol fulfills the comparison of two parties' secret information via the QKD protocol. Though QKD protocol consumes some resources, our protocol is more secure than those in [15, 16]. Unlike [21, 32–34], in our protocol, the existence of eavesdropping is checked with decoy photons. In addition, the proposed protocol is easier to realize than those protocols based on high-dimensional quantum states in [26, 27, 32–34]. In summary, the presented QPC protocol could compare the equality of one bit in each round of comparison, reducing the number of comparison times significantly. Compared with [15, 19], the qubit efficiency up to 10% is the lowest in [16], since the protocol needs to prepare ν W states, ν Bell states and 4ν decoy photons. In [20, 21], these two protocols can compare the equality of three information bits. In [20], the protocol only prepares 5ν particles and 5ν decoy photons, and the qubit efficiency is the highest in [15, 16, 19, 21]. In [27], the number of d-level Bell states used is $4\nu - 1$, where there is $2\nu - 2$ d-level Bell states as the eavesdropped detection. In [32], TP needs to prepare 4ν d-dimensional GHZ states, and Alice (Bob) needs to prepare 2ν single particles in the measure mode. In [33], TP needs to prepare 4ν d-dimensional Bell states, and Alice (Bob) needs to prepare 2ν single particles in the detect and encode mode. Therefore, the number of the consumed qudits is 12ν. In [34], the number of qudits used is $32\nu N$, where there are $16\nu N$ qudits used in the measure mode and N represents the number of participants. Therefore, the qubit efficiency is the lowest among the other ten protocols. However, in [26], the protocol only prepares ν d-level single particles and 2ν decoy photons, and the qubit efficiency is the highest among the other ten protocols. In our protocol, TP needs to prepare ν 4D GHZ-like states and 2ν decoy photons. Therefore, the number of the consumed qubits is 5ν to compare ν bits of classical information. As a result, the qubit efficiency of our protocol is only up to 20%, not the highest in these protocols, but it is not necessary for our protocol to involve unitary operation or entanglement swapping operation, which could save more resources than those protocols in [16, 21, 26, 27].

6 Conclusion

A two-party QPC protocol is proposed by considering the 4D GHZ-like states as quantum resources. The decoy photons can greatly enhance the security and reliability of the suggested protocol. Furthermore, in terms of quantum operations, it only involves not unitary operation but single particle measurement and decoy photons, which makes our protocol more secure. However, the presented protocol only can compare the privacies of equality, where the participants in the protocol can only determine whether their secret information is same or different. In the future, we will dedicate to studying a two-party QPC protocol of size relation.

Table 2 Comparison among some typical QPC protocols

	QM	QR	Need for decoy photon	QKD	ES	UO	Secure	Bit compared each time (bit)	QE
[15]	SPM	EPR pair	Yes	No	No	No	Yes	1	25%
[16]	SPM	W state and Bell state	Yes	No	Yes	No	Yes	1	10%
[19]	SPM	$(n+1)$-qubit GHZ state	Yes	Yes	No	No	Yes	1	[16.7% 25%]
[20]	SPM, BM	four-particle GHZ state	Yes	Yes	No	No	Yes	3	30%
[21]	GM	Bell state	No	Yes	Yes	No	Yes	3	25%
[26]	d-level SPM	d-level single-particle state	Yes	Yes	No	Yes	Yes	1	33.3%
[27]	d-level BM	d-level Bell state	Yes	Yes	Yes	Yes	Yes	1	16.67%
[32]	d-dimensional BM	d-dimensional GHZ state	No	Yes	No	No	Yes	1	6.25%
[33]	d-dimensional BM	d-dimensional Bell state	No	Yes	No	No	Yes	1	8.3%
[34]	d-dimensional SPM	d-dimensional single-particle state	No	Yes	No	No	Yes	1	$\frac{1}{32N}$
Our protocol	SPM	4D GHZ-like state	Yes	Yes	No	No	Yes	1	20%

QM quantum measurement, *QR* quantum resource, *NQO* necessary quantum operation, *QE* qubit efficiency, *SPUO* single-particle unitary operation, *SPM* single-particle measurement, *FPOM* four-particle orthogonal measurement, *BM* Bell measurement, *ES* entanglement swapping, *EBM* extended Bell measurement, *GM* GHZ-basis measurement

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No. 62161025), the Top Double 1000 Talent Programme of Jiangxi Province (Grant No. JXSQ2019201055), and the Innovation Special Foundation of Graduate Student of Jiangxi Province (Grant No. YC2022-S122).

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Wiesner, S.: Conjugate coding. ACM SIGACT News **15**(1), 78–88 (1983)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp 175–179 (1984)
3. Zhang, H.G., Ji, Z.X., Wang, H.Z., Wu, W.Q.: Survey on quantum information security. China Commun. **16**(10), 1–36 (2019)
4. Wang, F., Zeng, P., Zhao, J., et al.: High-dimensional quantum key distribution based on mutually partially unbiased bases. Phys. Rev. A **101**(3), 032340 (2020)
5. Li, T., Long, G.L.: Quantum secure direct communication based on single-photon Bell-state measurement. New J. Phys. **22**(6), 063017 (2020)
6. Yang, L., Wu, J.W., Lin, Z.S., et al.: Quantum secure direct communication with entanglement source and single-photon measurement. Sci. China Phys. Mech. Astron. **63**(11), 110311 (2020)
7. Xiang, Y., Mo, Z.W.: Quantum secret sharing protocol based on four-dimensional three-particle entangled states. Mod. Phys. Lett. B **30**(02), 1550267 (2016)
8. Gu, J., Cao, X.Y., Yin, H.L., et al.: Differential phase shift quantum secret sharing using a twin field. Opt. Express **29**(6), 9165–9173 (2021)
9. Zhou, Y., Yu, J., Yan, Z., et al.: Quantum secret sharing among four players using multipartite bound entanglement of an optical field. Phys. Rev. Lett. **121**(15), 150502 (2018)
10. Zhao, S.M., Shen, Z.G., Xiao, H., et al.: Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding. Sci. China Phys. Mech. Astron. **61**(9), 090323 (2018)
11. Liu, C., Cheng, S., Li, H.H., et al.: New semi-quantum key agreement protocol based on the -type entanglement states. Int. J. Theor. Phys. **61**(3), 60 (2022)
12. Yao, A.C.: Protocols for secure computations. In Proceedings of 23rd IEEE Symposium on Foundations of Computer Science, Washington, DC, pp 160–164 (1982)
13. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. **42**(5), 055305 (2009)
14. Chen, X.B., Xu, G., Niu, X.X., et al.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**(7), 1561–1565 (2010)
15. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
16. Li, J., Zhou, H.F., Jia, L., et al.: An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping. Int. J. Theor. Phys. **53**(7), 2167–2176 (2014)
17. Ji, Z.X., Zhang, H.G., Wang, H.Z.: Quantum private comparison protocols with a number of multi-particle entangled states. IEEE Access **7**, 44613–44621 (2019)
18. Li, C.Y., Chen, X.B., Li, H.J., et al.: Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state. Quantum Inf. Process. **18**(5), 158 (2019)
19. Ji, Z.X., Fan, P.R., Zhang, H.G., et al.: Greenberger-Horne-Zeilinger-based quantum private comparison protocol with bit-flipping. Phys. Scr. **96**(1), 015103 (2020)
20. Xu, Q.D., Chen, H.Y., Gong, L.H., et al.: Quantum private comparison protocol based on four-particle GHZ States. Int. J. Theor. Phys. **59**(6), 1798–1806 (2020)

21. Huang, X., Zhang, S.B., Chang, Y., et al.: Efficient quantum private comparison based on entanglement swapping of Bell states. Int. J. Theor. Phys. **60**(10), 3783–3796 (2021)
22. Gianni, J., Qu, Z.: New Quantum private comparison using hyperentangled GHZ state. J. Quantum Comput. **3**(2), 45–54 (2021)
23. Huang, X., Chang, Y., Cheng, W., et al.: Quantum private comparison of arbitrary single qubit states based on swap test. Chin. Phys. B **31**(4), 040303 (2022)
24. Xiao, M., Ma, C.A.: Fault-tolerant quantum private comparison protocol. Int. J. Theor. Phys. **61**(2), 41 (2022)
25. Jia, H.Y., Wen, Q.Y., Song, T.T., et al.: Quantum protocol for millionaire problem. Opt. Commun. **284**(1), 545–549 (2011)
26. Yu, C.H., Guo, G.D., Lin, S.: Quantum private comparison with -level single-particle states. Phys. Scr. **88**(6), 065013 (2013)
27. Guo, F.Z., Gao, F., Qin, S.J., et al.: Quantum private comparison protocol based on entanglement swapping of -level Bell states. Quantum Inf. Process. **12**(8), 2793–2802 (2013)
28. Li, L., Shi, R.: A novel and efficient quantum private comparison scheme. J. Korean Phys. Soc. **75**(1), 15–21 (2019)
29. Wu, W.Q., Zhao, Y.X.: Quantum private comparison of size using -level Bell states with a semi-honest third party. Quantum Inf. Process. **20**(4), 155 (2021)
30. Wang, B., Gong, L.H., Liu, S.Q.: Multi-party quantum private size comparison protocol with -dimensional Bell states. Front. Phys. **10**, 981376 (2022)
31. Zhou, N.R., Xu, Q.D., Du, N.S., et al.: Semi-quantum private comparison protocol of size relation with -dimensional Bell states. Quantum Inf. Process. **20**(3), 124 (2021)
32. Wang, B., Liu, S.Q., Gong, L.H.: Semi-quantum private comparison protocol of size relation with -dimensional GHZ states. Chin. Phys. B **31**(1), 010302 (2022)
33. Luo, Q.B., Li, X.Y., Yang, G.W., et al.: A mediated semi-quantum protocol for millionaire problem based on high-dimensional Bell states. Quantum Inf. Process. **21**(7), 257 (2022)
34. Ye, T.Y., Lian, J.Y.: A novel multi-party semiquantum private comparison protocol of size relationship with -dimensional single-particle states. Phys. A **611**, 128424 (2023)
35. Malik, M., Erhard, M., Huber, M., et al.: Multi-photon entanglement in high dimensions. Nat. Photonics **10**(4), 248–252 (2016)
36. Pivoluska, M., Huber, M., Malik, M.: Layered quantum key distribution. Phys. Rev. A **97**(3), 032312 (2018)
37. Hu, X.M., Xing, W.B., Zhang, C., et al.: Experimental creation of multi-photon high-dimensional layered quantum states. NPJ Quantum Inf. **6**(1), 88 (2020)
38. Zhang, X.H., Yan, X.Y., Wang, Y.Q., et al.: Tripartite layered quantum key distribution scheme with a symmetrical key structure. Int. J. Theor. Phys. **59**(2), 562–573 (2020)
39. IBM Quantum Experience. https://quantum-computing.ibm.com/composer/