Quantum Information Processing (2022) 21:382
https://doi.org/10.1007/s11128-022-03733-0

Three-party quantum privacy comparison protocol based on classical-quantum authentication channel

WanQing Wu[1] · LingNa Guo[2]

Received: 8 April 2022 / Accepted: 3 November 2022 / Published online: 16 November 2022

Abstract

With the help of semi-honest third party , a new quantum privacy comparison (QPC) protocol is proposed, which can compare the equality of the secrets of three participants without disclosing the secret value. At present, QPC protocols using different quantum states have been proposed. If complex quantum states are used in QPC protocol, more expensive equipment or more complex methods will be required to generate these quantum states, which may reduce efficiency and increase cost. In order to improve the availability of the protocol, a QPC protocol based on classical-quantum authentication channel is proposed in this paper. The protocol takes Bell state as quantum resource and uses single-particle measurement technology to measure particles, so the protocol enables participants to compare quantum privacy without expensive quantum devices. Finally, in order to ensure the security of the protocol, we use decoy photon technology and quantum key distribution technology to encrypt, so that the protocol can resist external attacks and participant attacks.

Keywords Quantum private comparison (QPC) · Bell state · Semi-honest third party

1 Introduction

With the development of computer and the advent of information society, the protection of private information has become particularly important. Cryptography has played a great role in ensuring the integrity, confidentiality and authenticity of information. However, the emergence of quantum parallel computing with strong computing power threatens the security of classical cryptography, which depends on computational

✉ WanQing Wu
wuwanqing8888@126.com

[1] School of Cyber Security and computer, Hebei University, Baoding 071002, People's Republic of China

[2] Key Laboratory on High Trusted Information System in Hebei Province, Hebei University, Baoding 071002, People's Republic of China

complexity. However, quantum cryptography, which depends on the basic principles of quantum mechanics, has unconditional security, so it has attracted extensive attention.

In 1984, Bennett and Brassard [1] combined classical cryptography with quantum mechanics and proposed the first quantum key distribution protocol. After that, quantum mechanics is more and more widely used in cryptography. People have proposed various quantum protocols, such as quantum election [2, 3], quantum secret sharing [4, 5], quantum key distribution [6, 7] and quantum digital signature [8, 9].

In the past decade, quantum privacy comparison (QPC) has become a hot issue in quantum cryptography. The concept of privacy comparison originates from the millionaire problem proposed by Yao [10]. It can compare the equality of two or more parties' privacy information without disclosing them. In 2009, Yang [11] proposed the first quantum privacy comparison protocol, which uses Bell state as quantum resource to compare the equality of two parties' secret values. After that, various QPC protocols for multi-particle entanglement have been proposed, such as W state, eight-qubit entangled state, six-qubit entangled state, cluster states and so on [12–20]. At same time, different quantum technologies such as unitary transformation, quantum shift operation and decoy photon are also gradually applied to QPC protocol. For example, Duan [21] proposes a new quantum privacy comparison protocol based on quantum shift operation. The protocol encodes the private information of participants into quantum states through quantum shift operation, and compares the equality of private information of all participants by executing the protocol once.

On the premise of ensuring security, it is possible to use the easily prepared quantum states as quantum resources and avoid the use of complex quantum technologies, which can improve the availability of the protocol. Based on the above principles, this paper proposes a quantum privacy comparison protocol based on classical-quantum authentication channel. Participants encrypt the secret information according to the entanglement characteristics of Bell state and use decoy photon technology and QKD technology to ensure the security of the protocol. As described in Lo [22], it is impossible to design a safe equality function in the two-party scenario, and some additional assumptions need to be introduced. Therefore, this paper introduces a semi-honest third party, which allows itself to misbehave, but TP does not collude with other participants. Finally, the security analysis shows that our proposed protocol can resist external and internal attacks and is secure.

The structure of this paper is as follows: In Sect. 2, the proposed QPC protocol is described in detail. In Sect. 3 and Sect. 4, the correctness and the security of the proposed protocol are analyzed, respectively. In Sect. 5, we compare our protocol with some existing protocols. Finally, we make a summary in Sect. 6.

2 The proposed scheme

In this section, we offer an explicit description of the presented protocol. Three communicants, Alice, Bob and Charlie, have three private integers, $X = (x_1, x_2, \cdots, x_n)$, $Y = (y_1, y_2, \cdots, y_n)$ and $Z = (z_1, z_2, \cdots, z_n)$, respectively. Here $x_i, y_i, z_i \in \{0, 1\}$ for $i = 1, 2, \cdots, n$. With the help of the semi-honest third party(TP) who is curious but does not collude with communicants, Alice, Bob and Charlie want to judge whether X,

Y and Z are equal or not. The process of the proposed QPC protocol can be described as follow.
Step 1 TP chooses five random number sequence K_{TA}, K_{TB}, K_{TC}, K_1 and K_2, i.e.,

$$\begin{aligned} K_{TA} &= (k_{TA}^1, k_{TA}^2, \cdots, k_{TA}^n), \\ K_{TB} &= (k_{TB}^1, k_{TB}^2, \cdots, k_{TB}^n), \\ K_{TC} &= (k_{TC}^1, k_{TC}^2, \cdots, k_{TC}^n). \end{aligned}$$

where $k_{TA}^i, k_{TB}^i, k_{TC}^i \in \{0, 1\}$ for $i = 1, 2, \cdots, n$.

$$\begin{aligned} K_1 &= (k_{A1}^1 k_{B1}^1 k_{C1}^1, k_{A1}^2 k_{B1}^2 k_{C1}^2, \cdots, k_{A1}^n k_{B1}^n k_{C1}^n), \\ K_2 &= (k_{A2}^1 k_{B2}^1 k_{C2}^1, k_{A2}^2 k_{B2}^2 k_{C2}^2, \cdots, k_{A2}^n k_{B2}^n k_{C2}^n). \end{aligned}$$

where $k_{A1}^i k_{B1}^i k_{C1}^i, k_{A2}^i k_{B2}^i k_{C2}^i \in \{011, 101, 110\}$ for $i = 1, 2, \cdots, n$. It should be noted that $k_{A1}^i k_{B1}^i k_{C1}^i \neq k_{A2}^i k_{B2}^i k_{C2}^i$.

Then, TP divides K_1 into three sequences, K_{A1}, K_{B1} and K_{C1},which are formed by all the first, the second and the third number, respectively.

$$K_{A1} = (k_{A1}^1, k_{A1}^2, \cdots, k_{A1}^n), K_{B1} = (k_{B1}^1, k_{B1}^2, \cdots, k_{B1}^n), K_{C1} = (k_{C1}^1, k_{C1}^2, \cdots, k_{C1}^n).$$

Similarly, TP takes the first number, the second number and the third number in K_2 to form sequences K_{A2}, K_{B2} and K_{C2}

$$K_{A2} = (k_{A2}^1, k_{A2}^2, \cdots, k_{A2}^n), K_{B2} = (k_{B2}^1, k_{B2}^2, \cdots, k_{B2}^n), K_{C2} = (k_{C2}^1, k_{C2}^2, \cdots, k_{C2}^n).$$

Finally, TP sends the sequences K_{TA}, K_{A1}, K_{A2} to Alice, the sequences K_{TB}, K_{B1}, K_{B2} to Bob and the sequences K_{TC}, K_{C1}, K_{C2} to Charlie in advance through the authenticated classical (or quantum) channels, respectively.
Step 2 Alice and Bob use the QKD protocol to generate two shared secret key sequence $K_{AB} = (k_{AB}^1, k_{AB}^2, \cdots, k_{AB}^n)$. Similarly, Bob and Charlie generate two shared key sequence $K_{BC1} = (k_{BC1}^1, k_{BC1}^2, \cdots, k_{BC1}^n)$ and $K_{BC2} = (k_{BC2}^1, k_{BC2}^2, \cdots, k_{BC2}^n)$. Charlie and Alice generate a shared key sequence $K_{AC} = (k_{AC}^1, k_{AC}^2, \cdots, k_{AC}^n)$ Here, $k_{AB}^i, k_{BC1}^i, k_{BC2}^i, k_{AC}^i \in \{0, 1\}$.
Step 3 Alice (Bob and Charlie) prepares quantum states according to the i-th binary representation $k_{TA}^i(k_{TB}^i$ and $k_{TC}^i)$. If $k_{TA}^i = 0$ ($k_{TB}^i = 0$ and $k_{TC}^i = 0$), Alice (Bob and Charlie) generates a Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; Otherwise Alice (Bob and Charlie) generates a Bell state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Then, Alice, Bob and Charlie obtain the quantum state sequences S_A, S_B and S_C, respectively.

Alice (Bob and Charlie) picks out the first particle from each state to form an ordered sequence $S_{A1}(S_{B1}$ and $S_{C1})$. The remaining second particle from each state automatically forms the other ordered sequence $S_{A2}(S_{B2}$ and $S_{C2})$. Alice (Bob and Charlie) prepares a set of decoy photon, which are randomly chosen from the four states$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and randomly inserts them into $S_{A1}(S_{B1}$ and $S_{C1})$ to compose a new sequence S'_{A1}(S'_{B1} and S'_{C1}). Finally, Alice sends S'_{A1} to Bob, Bob sends S'_{B1} to Charlie, and Charlie sends S'_{C1} to Alice.

Step 4 After Bob receives S'_{A1}, Alice and Bob check the transmission security of S'_{A1} together. Alice tells Bob the positions and the preparation bases of decoy photons in S'_{A1}. Afterward, Bob uses the preparation basis of Alice to measure the decoy photons in S'_{A1} and tell Alice the measurement results. By comparing Bob's measurement results with the initial states of decoy photons, Alice can judge whether the transmission of S'_{A1} was secure or not.If the error rate exceeds the threshold, the communication will be aborted; otherwise, they will continue the communication and remove the decoy photons in S'_{A1} to restore S_{A1}; it should be noted that the value of the error rate depends on to the channel situation, the distance, etc. According to Refs [23–25], the threshold of the detected error rate is [$\tau \approx 2\ 8.9\%$].

Bob and Charlie, Charlie and Alice use the same eavesdropping check method to check the transmission security of S'_{B1} and S'_{C1}.

Step 5 Alice performs single-particle measurements on each particle in S_{C1} and S_{A2} with Z basis, and denotes obtaining the measurement result M^i_{C1} and M^i_{A2}. Alice transforms M^i_{C1} and M^i_{A2} into classical bit according to the following rule: if $M^i_{C1} = |0\rangle(M^i_{A2} = |0\rangle)$, then $c^i_1 = 0(a^i_2 = 0)$; and if $M^i_{C1} = |1\rangle(M^i_{A2} = |1\rangle)$, then $c^i_1 = 1(a^i_2 = 1)$. Alice computes R^i_{A1} and R^i_{A2} as follows:

$$R^i_{A1} = c^i_1 \oplus a^i_2 \oplus k^i_{AB} \oplus (k^i_{A1} \wedge x_i),$$
$$R^i_{A2} = c^i_1 \oplus a^i_2 \oplus k^i_{AC} \oplus (k^i_{A2} \wedge x_i).$$

where the symbol $\oplus$ represents XOR operation and the symbol $\wedge$ represents logical multiplication throughout this paper.

Bob measures the sequences S_{A1} and S_{B2} with Z basis and the measurement results are denoted as M^i_{A1} and M^i_{B2}. Then, according to the coding rules, he denotes binary number corresponding to the measurement result as a^i_1 and b^i_2. Bob computes R^i_{B1} and R^i_{B2} in following:

$$R^i_{B1} = a^i_1 \oplus b^i_2 \oplus k^i_{AB} \oplus k^i_{BC1} \oplus (k^i_{B1} \wedge y_i),$$
$$R^i_{B2} = a^i_1 \oplus b^i_2 \oplus k^i_{BC2} \oplus (k^i_{B2} \wedge y_i).$$

Charlie uses Z basis to measure each particle of S_{B1} and S_{C2} and get the measurement outcomes M^i_{B1} and M^i_{C2}. He transforms M^i_{B1} and M^i_{C2} into classical bit as b^i_1 and c^i_2 according to the coding rules. Charlie computes R^i_{C1} and R^i_{C2} as follows:

$$R^i_{C1} = b^i_1 \oplus c^i_2 \oplus k^i_{BC1} \oplus (k^i_{C1} \wedge z_i),$$
$$R^i_{C2} = b^i_1 \oplus c^i_2 \oplus k^i_{AC} \oplus k^i_{BC2} \oplus (k^i_{C2} \wedge z_i).$$

Finally, the binary number R^i_{A1}, R^i_{A2}, R^i_{B1}, R^i_{B2}, R^i_{C1} and R^i_{C2} are announced to TP using classical channels.

Step 6TP computes:

$$R^i_{AB1} = R^i_{A1} \oplus R^i_{B1} \oplus k^i_{AT} \oplus k^i_{BT} = c^i_1 \oplus b^i_2 \oplus k^i_{BC1} \oplus (k^i_{A1} \wedge x_i) \oplus (k^i_{B1} \wedge y_i) \oplus k^i_{BT},$$
$$R^{i\prime}_{C1} = R^i_{C1} \oplus k^i_{CT} = b^i_1 \oplus c^i_2 \oplus k^i_{BC1} \oplus (k^i_{C1} \wedge z_i) \oplus k^i_{CT}.$$

If TP discovers that $R^i_{AB1} \neq R^{i\prime}_{C1}$, TP will stop the protocol and announce that the secrets of X,Y,Z are not same; otherwise, she will continue to calculate:

$$R^i_{BC} = R^i_{B2} \oplus R^i_{C2} \oplus k^i_{AT} \oplus k^i_{BT} = a^i_1 \oplus c^i_2 \oplus k^i_{AC} \oplus (k^i_{B2} \wedge y_i) \oplus (k^i_{C2} \wedge z_i) \oplus k^i_{CT},$$
$$R^{i\prime}_{A2} = R^i_{A2} \oplus k^i_{AT} = c^i_1 \oplus a^i_2 \oplus k^i_{AC} \oplus (k^i_{A2} \wedge x_i) \oplus k^i_{AT}.$$

If there exists $R^i_{AB2} \neq R^{i\prime}_{C2}$, TP will announce the inequality of the customers' private data and terminate this work; otherwise, TP can conclude that $X = Y = Z$ and announce the comparison result to Alice, Bob and Charlie.

3 Correctness

The correctness of our protocol is proved in this section.

In step 3, Alice Bob and Charlie generate Bell states according to the value of k^i_{TA}, k^i_{TB} and k^i_{TC}, respectively. If $k^i_{TA} = 0$ ($k^i_{TB} = 0$ and $k^i_{TC} = 0$), Alice (Bob and Charlie) generates a Bell state $|\phi^+\rangle$; If $k^i_{TA} = 1$ ($k^i_{TB} = 1$ and $k^i_{TC} = 1$), Alice (Bob and Charlie) generates a Bell state $|\psi^+\rangle$. It is well known that Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ once measured will collapse to one of the two states $\{|00\rangle, |11\rangle\}$. In a similar way, the Bell state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ will collapse to one of the two states $\{|01\rangle, |10\rangle\}$. Therefore, these equation will be hold:

$$a^i_1 \oplus a^i_2 \oplus k^i_{TA} = b^i_1 \oplus b^i_2 \oplus k^i_{TB} = c^i_1 \oplus c^i_2 \oplus k^i_{TC} = 0. \tag{1}$$

We can further deduce out that:

$$\begin{aligned} c^i_1 \oplus b^i_2 \oplus k^i_{BT} &= b^i_1 \oplus c^i_2 \oplus k^i_{CT}, \\ a^i_1 \oplus c^i_2 \oplus k^i_{CT} &= c^i_1 \oplus a^i_2 \oplus k^i_{AT}, \end{aligned} \tag{2}$$

TP compares the equality of R^i_{AB} and $R^{i\prime}_{C1}$ in the last step of our protocol. Based on the above analysis, TP is essentially to compare the equality of $(k^i_{A1} \wedge x_i) \oplus (k^i_{B1} \wedge y_i)$ and $k^i_{C1} \wedge z_i$. Similarly, TP compares the equality of R^i_{BC} and $R^{i\prime}_{A2}$. In essence, it compares the equality of $(k^i_{B2} \wedge y_i) \oplus (k^i_{C2} \wedge z_i)$ and $k^i_{A2} \wedge x_i$.

In Table 1, all possible situations in the calculation process are listed. For clarity, we bold the font of the calculation result when $(k^i_{A1} \wedge x_i) \oplus (k^i_{B1} \wedge y_i) = k^i_{C1} \wedge z_i$ or $(k^i_{B2} \wedge y_i) \oplus (k^i_{C2} \wedge z_i) = k^i_{A2} \wedge x_i$. As can be seen from the table, if and only if $(k^i_{A1} \wedge x_i) \oplus (k^i_{B1} \wedge y_i) = k^i_{C1} \wedge z_i$ and $(k^i_{B2} \wedge y_i) \oplus (k^i_{C2} \wedge z_i) = k^i_{A2} \wedge x_i$ are both true, we can get $x_i = y_i = z_i$.

So the presented protocol can be performed correctly.

Table 1 Relationship of essential variables

x_i	y_i	z_i	$k_{A1}k_{B1}k_{C1}$	$(k^i_{A1} \wedge x_i) \oplus (k^i_{B1} \wedge y_i)$	$k^i_{C1} \wedge z_i$	$k_{A2}k_{B2}k_{C2}$	$(k^i_{B2} \wedge y_i) \oplus (k^i_{C2} \wedge z_i)$	$k^i_{A2} \wedge x_i$
0	0	0	011	0	0	101	0	0
0	0	1		0	1		0	1
0	1	0		1	0		0	0
0	1	1		1	1		0	1
1	0	0		0	0		1	0
1	0	1		0	1		1	1
1	1	0		1	0		1	0
1	1	1		1	1		1	1
0	0	0	011	0	0	110	0	0
0	0	1		0	1		0	0
0	1	0		1	0		1	0
0	1	1		1	1		1	0
1	0	0		0	0		0	1
1	0	1		0	1		0	1
1	1	0		1	0		1	1
1	1	1		1	1		1	1
0	0	0	101	0	0	011	0	0
0	0	1		0	1		1	0
0	1	0		0	0		1	0
0	1	1		0	1		0	0
1	0	0		1	0		0	0
1	0	1		1	1		1	0
1	1	0		1	0		1	0
1	1	1		1	1		0	0
0	0	0	101	0	0	011	0	0
0	0	1		0	1		0	0
0	1	0		0	0		1	0

Table 1 continued

x_i	y_i	z_i	$k_{A1}k_{B1}k_{C1}$	$(k^i_{A1} \wedge x_i) \oplus (k^i_{B1} \wedge y_i)$	$k^i_{C1} \wedge z_i$	$k_{A2}k_{B2}k_{C2}$	$(k^i_{B2} \wedge y_i) \oplus (k^i_{C2} \wedge z_i)$	$k^i_{A2} \wedge x_i$
0	1	1		0	1		1	0
1	0	0		1	0		0	1
1	0	1		1	1		0	1
1	1	0		1	0		1	1
1	1	1		1	1		1	1
0	0	0	110	0	0	011	0	0
0	0	1		0	0		1	0
0	1	0		1	0		1	0
0	1	1		1	0		0	0
1	0	0		1	0		0	0
1	0	1		1	0		1	0
1	1	0		0	0		1	0
1	1	1		0	0		0	0
0	0	0	110	0	0	011	0	0
0	0	1		0	1		0	0
0	1	0		0	0		1	0
0	1	1		0	1		1	0
1	0	0		1	0		0	1
1	0	1		1	1		0	1
1	1	0		1	0		0	1
1	1	1		1	1		1	1

4 Analysis

In this section, we will discuss two cases of attacks. One is the attack from an outside eavesdropper, while the other is the attack from the dishonest participant.

4.1 Outsider attack

Suppose that there is an outside attacker Eve. Eve steals the secret data of participants by attacking the communication channel among participants and between participants and TP. Next, we analyze Eve's opportunities to obtain private information of participants in each step of the protocol.

Step 1 and step 5 transmit classical information through the classical authentication channel. According to the definition of the authenticated classical channel, any outside attacker can obtain the information transmitted on the classical authentication channel, but they cannot modify the data. Even if Eve gets the classical information transmitted, he cannot infer the secret from them. In Step 5, Eve may obtain the value of R^i_{A1}/R^i_{A2} (R^i_{B1}/R^i_{B2} and R^i_{C1}/R^i_{C2}) when Alice (Bob and Charlie) sends them to TP. However, these information is encrypted by shared keys, in which the value of shared keys is unknown to Eve. Thus, x_i, y_i, z_i will not be revealed to anyone.

In step 3, Eve can launch many common attacks to obtain qubits transmitted in quantum channels. The QKD technology and decoy photon technology are used to ensure the security of the protocol. We will analyze in detail how this protocol can resist common attacks in the following sections.

Case 1 Intercept-resend attack

The intercept-resend attack means that Eve intercepts qubits transmitted in the quantum channel and generates some fake qubits to send to the receiver. Without loss of generality, we assume Eve steals the sequence S'_{A1} that Alice sent to Bob. After Alice announces the positions and bases of decoy photons, Eve performs single-particle measurement on S'_{A1}. Then, he can obtain the value of a^i_1. However, he cannot learn Bob's secret because the secret is encrypted by the keys generated by the QKD protocol. What is more, Eve's attack will fail since he only has a $\frac{1}{4}$ probability of producing the same qubit as the correct decoy photon. For m decoy photons, the detection rate is $1 - (3/4)^m$ which is close to 1 if m is large enough.

Case 2 Measure-resend attack

The measure-resend attack means that Eve intercepts qubits transmitted in the quantum channel and measures them. Then, Eve prepares Eve generates the same quantum states as the measurement result and sends them to the receiver. However, his attack will fail because Eve does not know the positions and the measurement basis of all decoy photons, the participants can detect Eve's eavesdropping in the eavesdropping check step. If Eve measures an Z basis decoy photon $\{|0\rangle, |1\rangle\}$ with X basis $\{|+\rangle, |-\rangle\}$, he will have a chance of $\frac{1}{2}$ to be discovered. Apparently, the probability of detection for each photon is $\frac{1}{4}$. Eve is detected with a probability of $1 - (3/4)^m$ when m decoy photons are used for eavesdropping checking in step 4, where the probability will gradually approach 1 when m increases.

Case 3 Entangle-measure attack

The measure-resend attack means that Eve intercepts qubits transmitted in the quantum channel and entangle them with the ancillary qubit $|e\rangle$ by performing a unitary operation U_E on them. The unitary operation U_E can be described as follows:

$$U_E|0\rangle|e\rangle = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle, \tag{3}$$

$$U_E|1\rangle|e\rangle = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle, \tag{4}$$

where $|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle$ are pure states uniquely determined by U_E; $|a|^2 + |b|^2 = 1$, and $|c|^2 + |d|^2 = 1$. Next, we take the initial Bell state is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ as an example to analyze the measure-resend attack. Suppose that Eve entangles the ancillary qubit $|e\rangle$ with qubit in Bell state, the quantum system becomes:

$$\begin{aligned} U_e|\phi^+\rangle|e\rangle =& \frac{1}{\sqrt{2}}[|0\rangle(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle) + |1\rangle(c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle)] \\ =& \frac{1}{\sqrt{2}}[a|00\rangle|e_{00}\rangle + b|01\rangle|e_{01}\rangle + c|10\rangle|e_{11}\rangle + d|1\rangle|e_{11}\rangle] \\ =& \frac{1}{2}[a(|\phi^+\rangle + |\phi^-\rangle)|e_{00}\rangle + b(|\psi^+\rangle - |\psi^-\rangle) \\ &+ c(|\psi^+\rangle + |\psi^-\rangle)|e_{10}\rangle + d(|\phi^+\rangle - |\phi^-\rangle)|e_{11}\rangle]. \end{aligned} \tag{5}$$

When the unitary operation U_E is performed on the decoy photon, the state is changed as:

$$\begin{aligned} U_E|+\rangle|e\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle + c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle) \\ &= \frac{1}{2}|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle) \\ &\quad + \frac{1}{2}|-\rangle(a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle) \end{aligned} \tag{6}$$

and

$$\begin{aligned} U_E|-\rangle|e\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle - c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle) \\ &= \frac{1}{2}|-\rangle(a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle) \\ &\quad + \frac{1}{2}|-\rangle(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle) \end{aligned} \tag{7}$$

In order to prevent Eve's attack from being detected, the unitary operation U_E must be satisfied the following conditions:

$$b = c = 0, a = d = 1, |e_{00}\rangle = |e_{11}\rangle. \tag{8}$$

From Eq.(8), the formula (5) can be rewritten as:

$$U_e|\phi^+\rangle|e\rangle = \frac{1}{2}[a(|\phi^+\rangle + |\phi^-\rangle)|e_{00}\rangle + d(|\phi^+\rangle - |\phi^-\rangle)|e_{11}\rangle] = |\phi^+\rangle|e_{00}\rangle. \quad (9)$$

From the above analysis, it can be seen that some error must be introduced if Eve wants to obtain transmitted qubits through ancillary qubits. Thus, this attack must be detected.

Case 3. Trojan horse attack

In this protocol, the quantum sequences S'_{A1}, S'_{B1} and S'_{C1} are all transmitted in one direction and will not return, so they can resist Trojan horse attacks.

4.2 Insider attack

Gao [26] proposed that we should pay more attention to internal attacks, because internal attacks pose a greater threat to the protocol than external attackers. In what follows, we will considered the internal attacks in detail from the following three aspects. The first one is TP attempts to steal the data from participants. The second one is a dishonest participant trying to obtain the private information of other participants.

Case 1 The attack from TP

In our protocol, TP is assumed to be semi-honest, that is he may try his best to obtain participants' secrets without conspiring with either of them. If TP tries to intercept the transmitted photons among participants, he will be caught as an outside attacker analyzed in the above situation. The only way for TP to obtain secret information from participants is to use the binary sequence in her hands. Although he obtains the binary number R^i_{A1}, R^i_{A2}, R^i_{B1}, R^i_{B2}, R^i_{C1} and R^i_{C2}, he cannot deduce the secret. These information is encrypted by shared keys, in which the value of shared keys is unknown to TP.

Case 2 The attack from one dishonest participant

Individual attack means that a dishonest participant may try her/his best to get the other participants' secrets without conspiring with others. Alice, Bob and Charlie play the same role in the agreement. Without loss of generality, we assume that Bob is dishonest and tries to learn other participants' data. If Bob tries to intercept the transmitted photons from Alice to Charlie, she will be caught as an outside attacker analyzed in the above situation. Another way for Bob to get Alice and Charlie's secret information is to utilize the photons send to her and all the classical information in her hands. Suppose Bob is powerful enough to obtain the classic information R^i_{A1}, R^i_{A2}, R^i_{C1} and R^i_{C2}. Next, we analyze the possibility of Bob getting x_i and y_i, respectively.

First, Bob may try to deduce out x_i from R^i_{A1} and R^i_{A2}. If Bob want to calculate the value of x_i through R^i_{A1} or R^i_{A2}, Bob needs to know the values of c^i_1, a^i_2, k^i_{AB1} and k^i_{AC} in advance. Since the value of c^i_1 and a^i_2 are related to the Bell state generated by Alice and Charlie, Bob have no knowledge about them. Therefore, Bob cannot know x_i.

Second, Bob may try to deduce out y_i from R_{C1}^i and R_{C2}^i. If Bob want to calculate the value of y_i through R_{C1}^i and R_{C2}^i, Bob needs to know the values of b_1^i, c_2^i, k_{BC1}^i, k_{BC2}^i and k_{AC}^i in advance. Since the value of c_2^i is related to the Bell state generated by Charlie, Bob have no knowledge about it. Therefore, Bob cannot know y_i.

5 Comparison

In this section, we will make a comparison among our protocol and several current representative protocols. Qubit efficiency is an important indicator for evaluating QPC protocols. Here, the qubit efficiency is defined as:

$$\eta = \frac{c}{t}$$

where c and t represent the classical bits that can be compared and the number of particles used for the comparison protocol, respectively. The photons consumed in the process of decoy photons and QKD key generation are not included in. In our protocol, each participant generates a Bell state to compare one classical bit, so the quantum bit efficiency is 16.7%. We can calculate the qubit efficiency of other related protocols using the same method, and the comparison results are shown in Table 2.

From Table 2, it is obvious that each protocol has its own advantages and disadvantages. In terms of quantum carrier, our protocol uses Bell states as quantum carrier. Our protocol is superior to those using multi-particle entangled state as quantum carrier, for example, Refs. [14, 16, 33] using multi-particle entangled states as quantum resources and Refs. [21] based on d-level quantum system. As is known to all, the more qubits contained in the quantum state, the more difficult it is to prepare and operate the quantum state. There are still many challenges in the preparation and measurement of the quantum of multi-particle entangled state in practical application.

Moreover, in addition to the necessary quantum technologies such as quantum state preparation and quantum measurement, the proposed protocol does not use extra quantum technology. For example, as the protocol of Ref. [15] uses quantum swapping gate to compare the equality of two quantum states. Reference [27] encodes the participant's secret into quantum state by unitary operation. Reference [15, 27, 29, 30] uses quantum entanglement swapping in the implementation process. To realize the above protocol, participants need not only basic quantum abilities such as quantum measurement and quantum preparation, but also additional quantum abilities. However, quantum resources are currently very scarce, and it is impractical for all participants to pay for expensive quantum equipment. Fortunately, our protocol does not have these problems, although its qubit efficiency is not high. A valuable feature of the proposed protocol is that, except for the generation and measurement of quantum states, the rest of the protocol is completely classical.

Another advantage of our protocol is that quantum states as information carriers are prepared by participants. At present, most protocols prepare quantum states through TP and send them to users, respectively, so TP has the opportunity to prepare false quantum states in this process. On this condition, the protocol will face greater risks.

Table 2 The comparison of our protocol to the other protocols

	Quantum state	Quantum measurement	QKD	Unitary operation	Entanglement swapping	Qubit efficiency
The protocol of Ref. [14]	eight-qubit entangled states	single-particle measurement	√	×	×	25%
The protocol of Ref. [33]	five-qubit entangled states	single-particle measurement and Bell state measurement	√	×	×	40%
The protocol of Ref. [16]	four-qubit cluster state and extended Bell state	Bell state measurement	√	×	√	50%
The protocol of Ref. [21]	d-level single-particle states	d-level single-particle measurement	√	√	×	100%
The protocol of Ref. [31]	Bell states	single-particle measurement	×	×	×	16.7%
The protocol of Ref. [29]	Bell states	GHZ-basis measurement	√	×	√	50%
The protocol of Ref. [15]	Bell states	single-particle measurement	×	×	√	25%
The protocol of Ref. [27]	Bell states	Bell-basis measurement	√	√	√	100%
The protocol of Ref. [30]	Bell states	Bell-basis measurement	×	×	√	25%
The proposed protocol	Bell states	single-particle measurement	√	×	×	16.7%

So the preparation of quantum states by participants can improve the security and efficiency of the protocol to a certain extent.

6 Conclusion

In this paper, we propose a three-party quantum privacy comparison protocol based on classical-quantum authentication channel, which can compare the information equality of three participants by executing the protocol once. Our protocol uses Bell states as quantum resources, and it does not use quantum technologies that may consume expensive equipment, such as entanglement exchange and unitary transformation. Therefore, the proposed protocol does not need expensive quantum equipment, which is more in line with the actual needs. The protocol uses the entanglement correlation of Bell states, decoy photon technology and shared key sequence to ensure the security of the protocol. Finally, security analysis shows that our proposed protocol can resist external attacks and participant attacks.

Acknowledgements The authors are supported by the Science and technology research project of Hebei higher education Nos. ZD2021011.

Data Availability My manuscript has no association with data.

Declarations

Conflict of interest All authors have no conflict of interest, financial or otherwise.

References

1. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
2. Henderson, M., Novak, J., Cook, T.: Leveraging quantum annealing for election forecasting. J. Phys. Soc. Jpn. **88**(6), 061009 (2019)
3. Gao, W., Yang, L.: Quantum Election Protocol Based on Quantum Public Key Cryptosystem, vol. 2021. Security and Communication Networks, USA (2021)
4. Liao, Q., Liu, H., Zhu, L., Guo, Y.: Quantum secret sharing using discretely modulated coherent states. Phys. Rev. A **103**(3), 032410 (2021)
5. Wu, X., Wang, Y., Huang, D.: Passive continuous-variable quantum secret sharing using a thermal source. Phys. Rev. A **101**(2), 022301 (2020)
6. Lucamarini, M., Yuan, Z.L., Dynes, J.F., Shields, A.J.: Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature **557**(7705), 400–403 (2018)
7. Xu, F., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. **92**(2), 025002 (2020)
8. An, X.-B., Zhang, H., Zhang, C.-M., Chen, W., Wang, S., Yin, Z.-Q., Wang, Q., He, D.-Y., Hao, P.-L., Liu, S.-F., et al.: Practical quantum digital signature with a gigahertz bb84 quantum key distribution system. Opt. Lett. **44**(1), 139–142 (2019)
9. Yin, H.-L., Fu, Y., Liu, H., Tang, Q.-J., Wang, J., You, L.-X., Zhang, W.-J., Chen, S.-J., Wang, Z., Zhang, Q., et al.: Experimental quantum digital signature over 102 km. Phys. Rev. A **95**(3), 032334 (2017)
10. Yao, A.C.: Protocols for secure computations, in: 23rd annual symposium on foundations of computer science (sfcs 1982), IEEE, 1982, pp. 160–164

11. Yang, Y.-G., Cao, W.-F., Wen, Q.-Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
12. Wu, W., Zhao, Y.: Quantum private comparison of size using d-level bell states with a semi-honest third party. Quantum Inf. Process. **20**(4), 1–18 (2021)
13. Zhang, W.-W., Li, D., Li, Y.-B.: Quantum private comparison protocol with w states. Int. J. Theor. Phys. **53**(5), 1723–1729 (2014)
14. Fan, P., Rahman, A.U., Ji, Z., Ji, X., Hao, Z., Zhang, H.: Two-party quantum private comparison based on eight-qubit entangled state. Modern Phys. Lett. A **37**(5), 2250026 (2022)
15. Wu, W., Ma, X.: Quantum private comparison protocol without a third party. Int. J. Theor. Phys. **59**(6), 1854–1865 (2020)
16. Li, C., Chen, X., Li, H., Yang, Y., Li, J.: Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended bell state. Quantum Inf. Process. **18**(5), 1–12 (2019)
17. Xu, Q.-D., Chen, H.-Y., Gong, L.-H., Zhou, N.-R.: Quantum private comparison protocol based on four-particle ghz states. Int. J. Theor. Phys. **59**(6), 1798–1806 (2020)
18. 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., Xiong, J.-X.: Quantum private comparison of equality based on five-particle cluster state. Commun. Theor. Phys. **66**(6), 621 (2016)
19. Ji, Z.-X., Ye, T.-Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. **65**(6), 711 (2016)
20. Wu, W., Cai, Q., Wu, S., Zhang, H.: Cryptanalysis of he's quantum private comparison protocol and a new protocol. Int. J. Quantum Inform. **17**(03), 1950026 (2019)
21. Ming-Yi, D.: Multi-party quantum private comparison with qudit shifting operation. Int. J. Theor. Phys. **59**(10), 3079–3085 (2020)
22. Lo, H.-K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154 (1997)
23. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., Zeilinger, A.: Quantum cryptography with entangled photons. Phys. Rev. Lett. **84**(20), 4729 (2000)
24. Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10 km in daylight and at night. New J. Phys. **4**(1), 43 (2002)
25. Gobby, C., Yuan, a., Shields, A.: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. (2004) 84(19): 3762–3764
26. Gao, F., Qin, S.-J., Wen, Q.-Y., Zhu, F.-C.: A simple participant attack on the brádler-dušek protocol. Quantum Inform. Comput. **7**(4), 329–334 (2007)
27. Ji, Z.-X., Fan, P.-R., Zhang, H.-G., Wang, H.-Z.: Several two-party protocols for quantum private comparison using entanglement and dense coding. Optics Commun. **459**, 124911 (2020)
28. Chong-Qiang, Y., Tian-Yu, Y.: Circular multi-party quantum private comparison with n-level single-particle states. Int. J. Theor. Phys. **58**(4), 1282–1294 (2019)
29. Huang, X., Zhang, S.-B., Chang, Y., Hou, M., Cheng, W.: Efficient quantum private comparison based on entanglement swapping of bell states. Int. J. Theor. Phys. **60**(10), 3783–3796 (2021)
30. Ye, T.-Y.: Multi-party quantum private comparison protocol based on entanglement swapping of bell entangled states. Commun. Theor. Phys. **66**(3), 280 (2016)
31. Lang, Y.-F.: Quantum private comparison using single bell state. Int. J. Theor. Phys. **60**(11), 4030–4036 (2021)
32. Ye, T., Ji, Z.: Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. Sci. China Phys. Mech. Astron. **60**(9), 1–10 (2017)
33. Ye, T.-Y., Ji, Z.-X.: Two-party quantum private comparison with five-qubit entangled states. Int. J. Theor. Phys. **56**(5), 1517–1529 (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.