

## RESEARCH ARTICLE

# High-Capacity Quantum Private Comparison Protocol With Six-Qubit Hyperentangled Bell States and Hypercoding

JIAN LI<sup>1,2</sup>, FANTING CHE<sup>1,2</sup>, ZHUO WANG<sup>2</sup>, AND JUN YANG<sup>1</sup><sup>1</sup>School of Information Engineering, Ningxia University, Yinchuan 750000, China<sup>2</sup>School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing 100876, China

Corresponding author: Fanting Che (chefanting@bupt.edu.cn)

This work was supported in part by the Key Research and Development Program of Ningxia Hui Autonomous Region under Grant 2021BEG02007, and in part by the Open Research Fund of the Key Laboratory of Cryptography of Zhejiang Province under Grant ZCL21006.

**ABSTRACT** Based on the two-photon six-qubit hyperentangled Bell states and hyper-coding, a new high-capacity quantum privacy comparison (QPC) protocol is proposed to realize a high utilization of quantum resources. The protocol enables two particles of hyperentangled Bell states to compare the equality of 6 classical bits of secret information between two quantum users. The unitary operations are used to encode the secret information and achieve dense coding. In the proposed protocol, decoy photons and the quantum uncertainty principle are used to ensure transmission channel security and particle security. Comparisons with other QPC protocols in terms of quantum resources and efficiency reveal that the proposed protocol has significant advantages in quantum efficiency.


**INDEX TERMS** Quantum private comparison, Hyperentangled bell states, hypercoding, decoy photon.

## I. INTRODUCTION

With the rapid development of the information age, privacy protection has become a critical issue. While traditional encryption techniques have made significant progress in securing classical information, the security of these methods is now being challenged by the rapid advancement of quantum computing and communication technologies. To address this challenge, Quantum Privacy Comparison (QPC) has emerged as a novel approach for privacy protection. QPC is a privacy comparison protocol based on the principles of quantum mechanics, aiming to compare the privacy of sensitive information between two parties without directly revealing the content.

As early as 1982, Yao [1] proposed the famous Millionaires' Problem, which involves two millionaires who want to compare the amount of their wealth without revealing the specific amounts of their assets. This sparked research

interest in privacy comparisons. Subsequently, in 2009, Yang and Wen et al. [2] proposed a QPC protocol to solve Yao's Millionaires' Problem. This protocol utilized properties of quantum mechanics such as quantum superposition and measurement to achieve privacy comparison while protecting the privacy of wealth information. Later on, QPC protocols based on different quantum states were proposed, such as single-particle states [3], [4], [5], Bell states [6], [7], [8], GHZ states [9], [10], [11], and multi-qubit entangled states [6], [12], [13]. However, most existing quantum privacy comparison protocols are based on single particles and entangled states, using multiple quantum particles to encode classical bit information, which leads to limitations in utilizing quantum resources in the protocols. In [14] and [15], these protocols used two quantum particles of the Bell states to compare a classical bit of the users' secret information. To improve the quantum efficiency of the QPC protocol, [6] and [16] used multi-qubit entangled states, such as four-qubit entangled states and five-qubit entangled states, to transmit the secret information.

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen .

However, the quantum efficiency of these protocols is not more than 100%.

To address these limitations, some QPC protocols have been proposed based on the hyper-coding or used hyper-entangled quantum state, which can encrypt more than one classical bit of information with one quantum particle. Xu and Zhao [17] proposed a QPC protocol using the two-photon six-qubit hyperentangled Bell states. The efficiency of the Xu and Zhao's protocol is equal to 150% (without calculating the cost of decoy photons). The quantum resource used in their protocol is the hyperentangled Bell state, which not only contains the entanglement between the different particles but also contains the multi-dimensional entanglements, such as spatial degree of freedom (DoF) and polarization degree of freedom. Therefore, the hyperentangled states can transmit more qubits of information.

Inspired by the above analysis, we propose a novel QPC protocol based on hyperentangled Bell states and unitary operations in this paper. This protocol harnesses the unique characteristics of hyperentangled Bell states and the pivotal role of unitary operations to achieve efficient privacy comparison. In contrast to conventional methods, the proposed protocol requires only a small number of hyperentangled Bell state particles to compare a large amount of classical bit information, significantly enhancing the utilization efficiency of quantum resources. Moreover, the protocol incorporates decoy photon techniques using particles with multiple degrees of freedom, enhancing the security and correctness of the protocol.

The structure of this paper is arranged as follows: the knowledge preparation and the details of the proposed protocol are given in Sect II. The security of the proposed protocol is analyzed in Sect III. The qubit efficiency of the proposed protocol and the work of this paper are analyzed in Sect IV.

## II. QPC PROTOCOL WITH SIX-QUBIT HYPERENTANGLED BELL STATES

In the proposed QPC protocol, three parties, such as Alice, Bob, and TP, are allowed to participate in the private comparison. Alice and Bob are users who need to compare their secret  $M_A$  and  $M_B$ . TP is a semi-honest third party, and he must help compute the equality of the secret by completing the procedures of the protocol honestly. However, TP may try to infer the secret but does not cooperate with others.

### A. TWO-PHOTON SIX-QUBIT HYPERENTANGLED BELL STATES

In this section, the important quantum source and the rule of coding are described in detail. The two-photon six-qubit hyperentangled states required in the proposed protocol can be prepared by the method mentioned in [18] and 20. It can be written as follows:

$$|\Gamma\rangle_{AB}^{PFS} = \frac{1}{\sqrt{2}} (|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B)$$

$$\begin{aligned} & \otimes \frac{1}{\sqrt{2}} (|l\rangle_A |l\rangle_B + |r\rangle_A |r\rangle_B) \\ & \otimes \frac{1}{\sqrt{2}} (|I\rangle_A |I\rangle_B + |E\rangle_A |E\rangle_B) \end{aligned} \quad (1)$$

where  $|\Gamma\rangle_{AB}^{PFS}$  denotes the two-photon six-qubit hyperentangled Bell state, in which three DoFs are utilized to present the secret information.  $A$  and  $B$  denote the two photons of each hyperentangled Bell state.  $|H\rangle$  and  $|V\rangle$  indicate the horizontal and vertical polarization modes in the polarization DoF of the photons, respectively.  $|l\rangle$  and  $|r\rangle$  indicate the left and right modes in the first longitudinal-momentum DoF of the photons, respectively.  $|I\rangle$  and  $|E\rangle$  indicate the internal and external modes in the second longitudinal-momentum DoF of the photons, respectively.

The two-photon six-qubit hyperentangled Bell states in the polarization DoF and the two longitudinal momentum DoFs can also be described as follows:

$$|\Gamma\rangle_{AB}^{PFS} = |\tau\rangle_{AB}^P \otimes |\tau\rangle_{AB}^F \otimes |\tau\rangle_{AB}^S \quad (2)$$

where  $|\tau\rangle_{AB}^P$ ,  $|\tau\rangle_{AB}^F$  and  $|\tau\rangle_{AB}^S$  denote one of the four Bell states in the corresponding DoF, respectively. So there are 64 different kinds of two-photon six-qubit hyperentangled Bell states.

Here,  $\sigma_i$  is one of the four unitary operations on the polarization state.

$$\begin{aligned} \sigma_I &= |H\rangle \langle H| + |V\rangle \langle V|, \sigma_X = |H\rangle \langle V| + |V\rangle \langle H| \\ \sigma_Y &= |V\rangle \langle H| - |H\rangle \langle V|, \sigma_Z = |H\rangle \langle H| - |V\rangle \langle V| \end{aligned} \quad (3)$$

$\sigma'_j$  is one of the four unitary operations on the first longitudinal-momentum state.

$$\begin{aligned} \sigma'_I &= |l\rangle \langle l| + |r\rangle \langle r|, \sigma'_X = |l\rangle \langle r| + |r\rangle \langle l| \\ \sigma'_Y &= |r\rangle \langle l| - |l\rangle \langle r|, \sigma'_Z = |l\rangle \langle l| - |r\rangle \langle r| \end{aligned} \quad (4)$$

$\sigma''_k$  is one of the four unitary operations on the second longitudinal-momentum state.

$$\begin{aligned} \sigma''_I &= |I\rangle \langle I| + |E\rangle \langle E|, \sigma''_X = |I\rangle \langle E| + |E\rangle \langle I| \\ \sigma''_Y &= |E\rangle \langle I| - |I\rangle \langle E|, \sigma''_Z = |I\rangle \langle I| - |E\rangle \langle E| \end{aligned} \quad (5)$$

### B. DESCRIPTION OF THE PROPOSED QPC PROTOCOL

Here, the step of the proposed QPC protocol is described in detail. TP needs to prepare the quantum sources and compare the result of the computation. Alice and Bob need to perform the corresponding unitary operation on the hyperentangled photon according to their own secret. Moreover, all parties must do eavesdropping detection after receiving the particle string.

In the proposed protocol, a semi-honesty third party is allowed to participate in the comparison, where the semi-honesty third party must accomplish his task ordered in the protocol without any fake action, but he is allowed to take other action to attempt to gain the secret, such as Inferring secret information based on comparative results and intermediate measurement outcomes, and other attack methods.

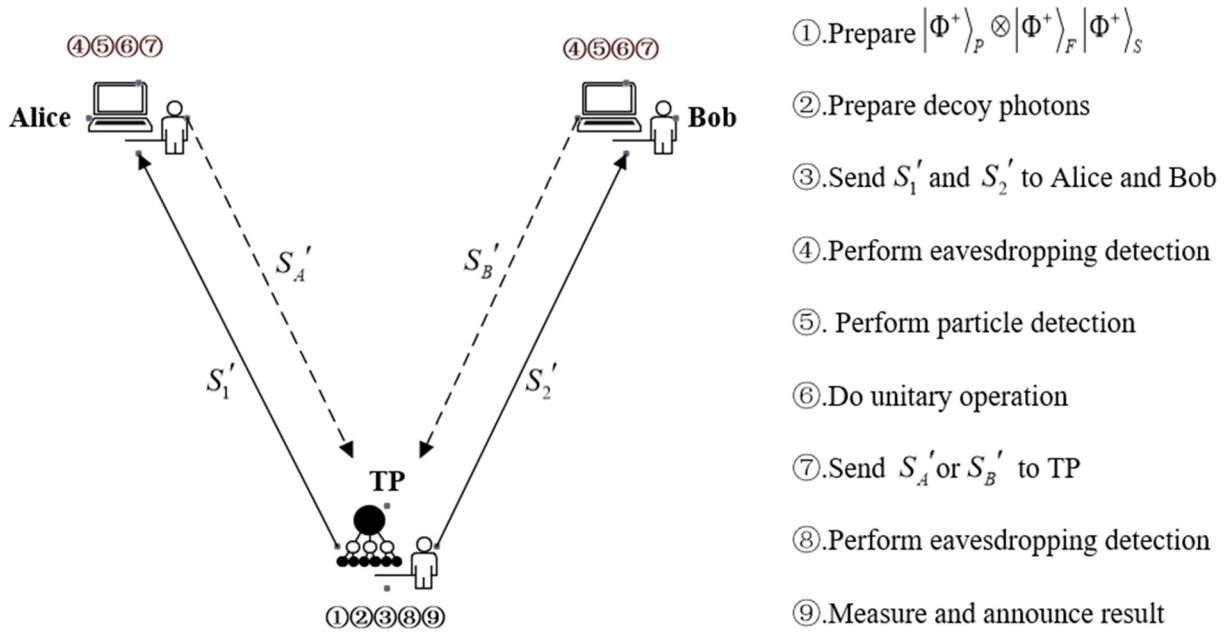


FIGURE 1. The model of the proposed protocol.

**Step 1:** TP prepares  $N(= L+l)$  hyperentangled Bell states  $|\Phi_P^+\rangle_{AB} \otimes |\Phi_F^+\rangle_{AB} \otimes |\Phi_S^+\rangle_{AB}$  and divides them into two particles sequences  $S_1$  and  $S_2$ , where  $S_i$  includes the  $i$ -th particle of the each prepared state.

$$S_1 = \{p_1^A, p_2^A, \dots, p_N^A\} \quad (6)$$

$$S_2 = \{p_1^B, p_2^B, \dots, p_N^B\} \quad (7)$$

where  $p_i$  denotes the one particle of the hyperentangled Bell state.

**Step 2:** Then, TP prepares  $2m$  hyperentangled Bell states as the decoy photon, and divides these decoy photons into two sets on average, in which each decoy photon is selected randomly from the 64 nonorthogonal single-photon states. TP inserts a set of the decoy photon into the sequence  $S_1$  to form a new photon sequence  $S_1'$ , and inserts the rest set into the sequence  $S_2$  to form a new sequence  $S_2'$ . The positions and bases of the decoy photon in  $S_1$  is noted as  $P_1$  and  $B_1$ , respectively. The positions and bases of the decoy photon in  $S_2$  is noted as  $P_2$  and  $B_2$ , respectively.

**Step 3:** After preparing hyperentangled Bell states and decoy photon, TP sends  $S_1$  and  $S_2$  to Alice and Bob, respectively.

**Step 4:** Upon receiving the sequences  $S_1$  and  $S_2$  sent by TP, Alice and Bob would do eavesdropping detection at first. TP announces to Alice and Bob the position  $P_1$  and  $P_2$  and the bases  $B_1$  and  $B_2$  of the decoy photon in sequences  $S_1$  and  $S_2$ , respectively. According to the positions and bases, Alice (Bob) selects out the decoy photon and measures their quantum states. Then, Alice (Bob) computes the error rate of the measurement result to analyze the security of the quantum transmission channel. If the error rate exceeds the

predetermined threshold, Alice (Bob) ensures that the transmission channel is not secure and terminates and repeats the protocol. Otherwise, Alice and Bob can ensure that the transmission channel is safe and can continue the protocol.

**Step 5:** Before starting to encode their secret information, Alice and Bob need to check the feasibility of utilizing these particles. Alice randomly selects  $l$  particles from the sequence  $S_1$  discarded these decoy photons and announces the selection to Bob publicly. Then Bob randomly selects measurement, Z basis or X basis, to measure these particles, and announces to Alice the corresponding measurement basis. Alice does the corresponding measurement. Alice and Bob announce their measurement result and determine the result of this detection. When the measurement outcomes are consistent within the same measurement basis, it signifies the viability of the quantum particles prepared by TP.

**Step 6:** After ensuring the transmission channel and the particles are safe, Alice and Bob discard the decoy photon in the sequences  $S_1$  and  $S_2$ . Then, Alice and Bob select the correct unitary operation to encode the new  $S_1$  and  $S_2$ . The unitary operation is corresponding to the secret group  $m_i$ , and the corresponding rules of  $m_i$  and the unitary operation is shown in Table.1. Alice and Bob form the encoding result to new quantum sequences  $S_A$  and  $S_B$ .

The secret groups:

$$m_i = \{(q_1, q_2), (q_3, q_4) \dots, (q_{6L-1}, q_{6L})\} \quad (8)$$

**Step 7:** Alice and Bob prepare two sets of the decoy photon and insert them into the sequences  $S_A$  and  $S_B$  to form two new quantum sequences  $S_A'$  and  $S_B'$ , respectively. Then, Alice and Bob send the  $S_A'$  and  $S_B'$  to TP.

**Step 8:** Upon receiving the sequences  $S'_A$  and  $S'_B$ , TP does eavesdropping detection at first, which is similar to the step 5. Next, TP forms the particles of  $S'_A$  and  $S'_B$  to a new sequence  $S_T$  (Shown as (15)).

$$S_T = \{(p_1^A, p_1^B), (p_2^A, p_2^B), \dots, (p_L^A, p_L^B)\} \quad (9)$$

**Step 9:** TP measures the photon pair  $\{p_i^A, p_i^B\}$  and analyses the equality of the secret information. If all the measurement result of the two-photon six-qubit hyperentangled Bell states are  $|\Phi_P^+\rangle_{AB} \otimes |\Phi_F^+\rangle_{AB} \otimes |\Phi_S^+\rangle_{AB}$  (shown as the Table.2), the secret of Alice and Bob is equal. Otherwise, the secret between Alice and Bob is different.

**TABLE 1.** The corresponding rules of  $m_i$  and the unitary operation.

$m_i$	00	01	10	11
Unitary operation	$I$	$X$	$Y$	$Z$

**TABLE 2.** The summary table of the correct measurement result.

Unitary operation	Unitary operation	Measurement result
$I$	$I$	$ \Phi_K^+\rangle_{AB}$
$X$	$X$	$ \Phi_K^+\rangle_{AB}$
$Y$	$Y$	$ \Phi_K^+\rangle_{AB}$
$Z$	$Z$	$ \Phi_K^+\rangle_{AB}$

where  $K$  can get the value of  $P, F$  and  $S$ , which denote the three kinds of DoFs of hyperentangled Bell states.

**TABLE 3.** The summary of the incorrect measurement result.

Unitary operation	Unitary operation	Measurement result
$I$	$X$	$ \Psi_K^+\rangle_{AB}$
$I$	$Y$	$ \Psi_K^-\rangle_{AB}$
$I$	$Z$	$ \Phi_K^-\rangle_{AB}$
$X$	$I$	$ \Psi_K^+\rangle_{AB}$
$X$	$Y$	$ \Phi_K^-\rangle_{AB}$
$X$	$Z$	$ \Psi_K^-\rangle_{AB}$
$Y$	$I$	$ \Psi_K^-\rangle_{AB}$
$Y$	$X$	$ \Phi_K^-\rangle_{AB}$
$Y$	$Z$	$ \Psi_K^+\rangle_{AB}$
$Z$	$I$	$ \Phi_K^-\rangle_{AB}$
$Z$	$X$	$ \Psi_K^-\rangle_{AB}$
$Z$	$Y$	$ \Psi_K^+\rangle_{AB}$

where  $K$  can get the value of  $P, F$  and  $S$ , which denote the three kinds of DoFs of hyperentangled Bell states.

### C. CORRECTNESS

There are two secret  $M_A$  and  $M_B$  held by the quantum users Alice and Bob who want to compare the equality of the secret. Alice and Bob divide the secret bits into groups according to the rule ordered.

Then, TP prepares the quantum sources and divides them into two quantum sequences  $S_1$  and  $S_2$ . Meanwhile, TP generates decoy photon and insert them into the sequences  $S_1$  and  $S_2$  randomly to form two new quantum sequences  $S_1$  and  $S_2$ . TP sends  $S_1$  and  $S_2$  to Alice and Bob, respectively.

After receiving the quantum sequences  $S_1$  and  $S_2$  sent by TP, Alice and Bob perform eavesdropping detection and check the particles at first. Upon ensuring the channel is secure and the particle is well, Alice and Bob carry out unitary operations according to the groups of their own secret. Then, Alice and Bob also prepare the decoy photon, and form two new sequences  $S_A'$  and  $S_B'$  with the result of unitary operations and the decoy photon. Alice and Bob send  $S_A'$  and  $S_B'$  to TP, respectively.

Upon receiving the  $S_A'$  and  $S_B'$  sent by Alice and Bob, TP perform eavesdropping detection at first. Then, TP combines the  $S_A'$  and  $S_B'$  to a new sequence  $S_T$ , and does the measurement on each pair in the sequence  $S_T$ . Moreover, TP will announce the result of the equality of the secret comparison according to the rule shown as Table.2 and Table.3.

### III. SECURITY ANALYSES

As shown in the description of the proposed protocol, two types of attacks, such as external attacks and participant attacks, may be used to attack the protocol. The external attacks include some attack methods, such as the measurement-resend attack, the intercept-resend attack, and the entanglement-measurement attack. These attacks are invalid in the proposed protocol, which is shown in detail as follows. Moreover, Alice, Bob and the third party TP can not obtain the specific information of the secret in comparison.

#### A. EXTERNAL ATTACKS

The decoy photons are used to detect the existence of an eavesdropper in the transmission channel. Assume that Eve is an external attacker who wants to steal the secret of Alice and Bob without being discovered. The attack methods that Eve could take may be the measurement-resend attack, the intercept-resend attack, and the entanglement-measurement attack. However, since Eve has no idea to know the position and basis of the decoy photon, any measurement performed on the decoy photon by Eve is introduced to some mistake. The error rate in Step 4 and Step 8 would increase significantly. So the intercept-resend attack and the measurement-resend attack are invalid for the proposed protocol. Meanwhile, the entanglement-resend attack is also invalid. The auxiliary particles Eve used to entangle the target particle are independent of the target particle [20], [21], since Eve does not want to introduce any mistake in Step 4 and

Step 8. Eve has no idea to obtain any information through her auxiliary particles. Therefore, the proposed protocol can resist these common external attacks. Meanwhile, the application of the decoy photon can resist the CNOT attack [24] since the particles with secret information are confused with these decoy photons. The Eve can not know the specific position of the particles with secret information.

Due to the particles in the proposed protocol need to be transmitted back and forth, the security measures against Trojan-horse attacks also need to be carefully considered [25], [26]. A filter is required to be inserted in the front of the device of participants to filter out the quantum signals with illegal wavelengths. This method can avoid Eve to gain no information about the secret with Trojan-horse attacks. Moreover, the proposed protocol transmits a sequence of quantum photons rather than a single particle at a time. This creates an opportunity to make Eve do quantum-number-splitting attacks to [26], which use quantum non-demolition measurement to split photons and obtain some useful information through the splitting photons. To address this issue, a beam splitter is also inserted in the front of the device of participants to make the signal photons transmit in different channels. So Eve has no chance to gain the whole information through the quantum-number-splitting attack.

## B. PARTICIPANT ATTACKS

Compared with external attackers, internal participants have more attack opportunities and advantages, and have a greater threat of attack. The possibility of a successful attack by each participant will be analyzed in detail in this section.

### Case 1: Alice(Bob)'s attack

Alice and Bob play the same role in the proposed protocol. Without loss of generality, assume that Alice is Eve who wants to steal Bob's secret information without being discovered. If Alice intends to intercept the quantum sequence  $S_2$  sent by TP to Bob and the quantum sequence  $S_B'$  sent by Bob to TP, she will be seen as an external attacker. According to section III, such attacks are unsuccessful. Moreover, Alice can not steal the secret of Bob with the help of TP, so the only way Alice may obtain the secret of Bob is to analyze the quantum sequence  $S_1$  that TP sends to her. When Alice receives the  $S_1$ , Alice can not know the position and basis of the decoy photon until TP announces them. So Alice has no choice do any operation on  $S_1$ . Meanwhile, since the unitary operation does not change the entanglement state of the quantum source, Alice also cannot know the kind of unitary operation that Bob takes on the  $S_2$ . Therefore, Alice or Bob cannot obtain the secret of the other users.

### Case 2: TP's attack

TP is a semi-honest third party. TP must prepare the quantum states required by the protocol and complete each procedure of the protocol. As one of the participants, TP knows more information than other external attackers. TP knows the position and basis of the decoy photon he sends to Alice and Bob, the position and basis of the decoy photon Alice and

Bob send to him after they announce this information, and the specific measurement outcomes. Therefore, TP has two ways to steal the secret of Alice and Bob. One way is to speculate the secret of Alice and Bob through the messages he has known. However, TP can not judge the specific unitary operations performed by Alice and Bob from the measurement outcomes. Because TP does not measure the particles that he sends out and receives one by one. The other way is to become an external attacker. The distinction between TP's attacks and Eve's is that TP can introduce no error in Step 4. TP knows the position and basis of decoy photons in the sequences he sends out, but he would introduce many mistakes in Step 5. Step 5 aims to check the usage of the particle TP prepares, and also check the honesty of TP. In another way, while TP prepares to attack the channel in which Alice and Bob send photon sequences to TP, some error would be introduced in Step 8, which has shown in section III. Since TP can not know the position and basis of the decoy photons in the sequences before Alice and Bob announce. Although TP may attempt to steal secret information, he also must perform the operation ordered in protocol first rather than other attack actions. Therefore, TP cannot obtain the secret of the other users.

## IV. DISCUSSION AND CONCLUSION

The efficiency of a QPC protocol can be measured by the relationship between the number of classical bits being compared and the quantity of quantum particles used in the comparison, which can be expressed with the following equation:  $\eta_e = \eta_c / \eta_t$ , where  $\eta_e$  donates the QPC protocol's efficiency,  $\eta_c$  donates the number of the compared classical bits in each comparison, and  $\eta_t$  donates the number of the generated quantum particles in each comparison. The  $\eta_t$  include the number of the signal photon used to encode the secret and the number of the decoy photon used to detect eavesdropping and check the honesty of the third party.

In the proposed protocol, TP prepares  $N(= L+l)$  the ordered two-photon six-qubit hyperentangled Bell states, in which  $L$  photon pairs are used to encode secret information and  $l$  photon pairs are used to check particles. TP also needs to prepare  $2m$  decoy photons. Alice and Bob need to prepare  $2m$  decoy photons in total. So the number of the generated quantum particles is  $L+l+4m$  (i.e.,  $\eta_t = L + l + 4m$ ). In each comparison,  $6L$  bits of secret information are required to be encoded in  $L$  hyperentangled Bell states with unitary operations. So the number of the compared classical bits is  $6L$  (i.e.,  $\eta_c = 6L$ ). The quantum efficiency of the proposed protocol:

$$\eta_e = \frac{6L}{2L + 2l + 4m} = \frac{3L}{L + l + 2m} \quad (10)$$

According to Eq (10), when the number of decoy photons and quantum pairs used to check particles is much less than the number of quantum pairs used to encode the secret, the efficiency approaches 300%. The number of decoy photons and detection particles needs to be based on the actual use

TABLE 4. Comparison between the proposed protocol with some other protocols.

Property	Quantum resource	QKD method	Entanglement swapping	Decoy photon	Unitary operation	Quantum efficiency
Ref.[9]	Hyperentangled GHZ states	Yes	Yes	Yes	No	50%
Ref.[6]	Bell state/Entangled five-qubit state/ $\chi$ -type states	No	No	Yes	No	50%
Ref.[17]	Two-photon six-qubit hyperentangled Bell states	Yes	No	Yes	No	100%
Ref.[22]	GHZ states	No	No	No	Yes	22.2%
Ref.[23]	EPR states	Yes	No	Yes	No	50%
The proposed protocol	Two-photon six-qubit hyperentangled Bell states	No	No	Yes	Yes	120%

of the situation. We suppose  $l = m = L/2$ , which is used to express the advantages of this protocol more intuitively. Therefore, the quantum efficiency of the proposed protocol is 120%.

In Gianni et al.'s protocol [9],  $3L$  particles of GHZ states are transmitted to compare  $2L$  bits of secret information. Meanwhile, the protocol uses decoy photons to perform eavesdropping detection. Assume  $L/2$  decoy photons are used in each channel. So the number of quantum photons used to compare secret information is  $3L + 2 \cdot L/2 = 4L$ . The efficiency of this protocol is 50%.

In Ji et al.'s paper [6], several protocols with different quantum states are introduced to compare the secret. As the Ji et al.'s analysis of their protocol, the quantum efficiency has reached 100%. However, the decoy photons are detected twice for eavesdropping detection in the process of transmitting particles back and forth. The cost of decoy photons also needs to be considered. So the highest efficiency in Ji et al.'s paper is 50%.

In Xu et al.'s protocol [17], the quantum resource that is the same as the proposed protocol, is two-photon six-qubit hyperentangled Bell states. Unlike our proposed protocol, Xu et al.'s protocol uses the key distributed by the hyperentangled Bell state to encrypt the secret information, but our protocol uses unitary operations to encode the secret information into the particles of hyperentangled Bell States.  $3L$  bits of secret information are compared with  $2L$  particles of hyperentangled Bell states, and the cost of decoy photons is  $2 \cdot L/2$  in each key distribution. So the efficiency is 100%.

In Chen et al.'s protocol [22], GHZ states are used to compare the equality of the secret of each user. Three particles from a GHZ state are used to compare one bit of classical secret information. This means  $3L$  GHZ particles are used to compare  $L$  bits of secret. Some GHZ states are used to do eavesdropping detection. Assume the number of particles for checking is  $L/2 + L/2 + L/2 = 3L/2$ . so the efficiency of Chen's protocol is  $2/9 = 22.2\%$ . In Tsing et al.'s protocol [23], EPR states are used to distribute a key for Alice and Bob. The qubit efficiency is 50%. The comparison is shown in Table 4.

The QPC protocol proposed in the paper allows two parties, such as Alice and Bob, to compare the equality of their secret with the help of a semi-honesty third party. Compared

with most previous QPC protocols, the proposed protocol is more efficient. In the proposed protocol, we use the hyperentangled Bell states to disseminate quantum information and use the unitary operations to encode the hyperentangled Bell state particles according to secret information. Through the research, the proposed protocol aims to provide an efficient and secure quantum privacy comparison method that maximizes the advantages of two-photon six-qubit hyperentangled Bell states and unitary operations, thereby improving the efficiency and security of privacy protection.

## REFERENCES

- [1] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci. (SFCS)*, Nov. 1982, pp. 160–164.
- [2] Y.-G. Yang and Q.-Y. Wen, "An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement," *J. Phys. A, Math. Theor.*, vol. 42, no. 5, Feb. 2009, Art. no. 055305.
- [3] L. Yan-Feng, "Semi-quantum private comparison using single photons," *Int. J. Theor. Phys.*, vol. 57, no. 10, pp. 3048–3055, Oct. 2018.
- [4] X. Song, A. Wen, and R. Gou, "Multiparty quantum private comparison of size relation based on single-particle states," *IEEE Access*, vol. 7, pp. 142507–142514, 2019.
- [5] Y.-C. Li, Z.-Y. Chen, Q.-D. Xu, and L.-H. Gong, "Two semi-quantum private comparison protocols of size relation based on single particles," *Int. J. Theor. Phys.*, vol. 61, no. 6, p. 157, Jun. 2022.
- [6] Z.-X. Ji, P.-R. Fan, H.-G. Zhang, and H.-Z. Wang, "Several two-party protocols for quantum private comparison using entanglement and dense coding," *Opt. Commun.*, vol. 459, Mar. 2020, Art. no. 124911.
- [7] C. Li, X. Chen, H. Li, Y. Yang, and J. Li, "Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state," *Quantum Inf. Process.*, vol. 18, no. 5, pp. 1–12, May 2019.
- [8] M.-J. Geng, Y. Chen, T.-J. Xu, and T.-Y. Ye, "Single-state semiquantum private comparison based on Bell states," *EPJ Quantum Technol.*, vol. 9, no. 1, pp. 1–24, Dec. 2022.
- [9] J. Gianni and Z. Qu, "New quantum private comparison using hyperentangled GHZ state," *J. Quantum Comput.*, vol. 3, no. 2, pp. 45–54, 2021.
- [10] W. Liu and H.-W. Yin, "A new multi-party quantum private comparison based on  $n$ -dimensional  $n$ -particle GHZ state," *Modern Phys. Lett. A*, vol. 36, no. 12, Apr. 2021, Art. no. 2150083.
- [11] Q.-D. Xu, H.-Y. Chen, L.-H. Gong, and N.-R. Zhou, "Quantum private comparison protocol based on four-particle GHZ states," *Int. J. Theor. Phys.*, vol. 59, no. 6, pp. 1798–1806, Jun. 2020.
- [12] P. Fan, A. U. Rahman, Z. Ji, X. Ji, Z. Hao, and H. Zhang, "Two-party quantum private comparison based on eight-qubit entangled state," *Modern Phys. Lett. A*, vol. 37, no. 5, Feb. 2022, Art. no. 2250026.
- [13] Z. Ji, P. Fan, and H. Zhang, "Entanglement swapping for Bell states and Greenberger–Horne–Zeilinger states in qubit systems," *Phys. A, Stat. Mech. Appl.*, vol. 585, Jan. 2022, Art. no. 126400.

- [14] T. Zheng, S. Zhang, X. Gao, and Y. Chang, "Practical quantum private query based on Bell state," *Modern Phys. Lett. A*, vol. 34, no. 24, Aug. 2019, Art. no. 1950196.
- [15] F. Wang, M. Luo, H. Li, Z. Qu, and X. Wang, "Quantum private comparison based on quantum dense coding," *Sci. China Inf. Sci.*, vol. 59, no. 11, Nov. 2016, Art. no. 112501.
- [16] H.-Y. Jia, Q.-Y. Wen, Y.-B. Li, and F. Gao, "Quantum private comparison using genuine four-particle entangled states," *Int. J. Theor. Phys.*, vol. 51, no. 4, pp. 1187–1194, Apr. 2012.
- [17] L. Xu and Z.-W. Zhao, "High-capacity quantum private comparison protocol with two-photon hyperentangled Bell states in multiple-degree of freedom," *Eur. Phys. J. D*, vol. 73, no. 3, pp. 1–11, Mar. 2019.
- [18] X.-H. Li and S. Ghose, "Hyperentangled Bell-state analysis and hyperdense coding assisted by auxiliary entanglement," *Phys. Rev. A, Gen. Phys.*, vol. 96, no. 2, Aug. 2017, Art. no. 020303.
- [19] G. Vallone, R. Ceccarelli, F. De Martini, and P. Mataloni, "Hyperentanglement of two photons in three degrees of freedom," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 3, Mar. 2009, Art. no. 030301.
- [20] H.-K. Lo, "A simple proof of the unconditional security of quantum key distribution," *J. Phys. A, Math. Gen.*, vol. 34, no. 35, pp. 6957–6967, Sep. 2001.
- [21] J. Li, H.-F. Zhou, L. Jia, and T.-T. Zhang, "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.*, vol. 53, no. 7, pp. 2167–2176, Jul. 2014.
- [22] X.-B. Chen, G. Xu, X.-X. Niu, Q.-Y. Wen, and Y.-X. Yang, "An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement," *Opt. Commun.*, vol. 283, no. 7, pp. 1561–1565, Apr. 2010.
- [23] H.-Y. Tseng, J. Lin, and T. Hwang, "New quantum private comparison protocol using EPR pairs," *Quantum Inf. Process.*, vol. 11, no. 2, pp. 373–384, Apr. 2012.
- [24] C.-W. Yang, "Efficient and secure semi-quantum secure direct communication protocol against double CNOT attack," *Quantum Inf. Process.*, vol. 19, no. 2, pp. 1–15, Feb. 2020.
- [25] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, "Improving the security of secure direct communication based on the secret transmitting order of particles," *Phys. Rev. A, Gen. Phys.*, vol. 74, no. 5, Nov. 2006, Art. no. 054302.
- [26] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-J. Zhang, "Improving the security of multiparty quantum secret sharing against trojan horse attack," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 4, Oct. 2005, Art. no. 044302.



**JIAN LI** received the Ph.D. degree from the Beijing Institute of Technology, Beijing, China, in 2005. He is currently a Professor with the School of Cyber Security, Beijing University of Posts and Telecommunications, Beijing. His research interests include information security and quantum cryptography.



**FANTING CHE** received the B.E. degree in mechanical engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2022, where he is currently pursuing the M.S. degree in artificial intelligence. His research interests include quantum cryptography and artificial intelligence.



**ZHUO WANG** is currently pursuing the Ph.D. degree with the Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include quantum cryptography and block chain.



**JUN YANG** received the Ph.D. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China. He is currently a Professor with the School of Information Engineering, Ningxia University, Yinchuan, China. His research interests include network security and edge computing.

• • •