IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 6, 2019, accepted March 18, 2019, date of publication April 1, 2019, date of current version April 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2906687

Quantum Private Comparison Protocols With a Number of Multi-Particle Entangled States

ZHAOXU JI, HUANGUO ZHANG, AND HOUZHEN WANG

Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Corresponding author: Houzhen Wang (whz@whu.edu.cn)

This work was supported in part by the State Key Program of National Natural Science of China under Grant 61332019, in part by the Major State Basic Research Development Program of China (973 Program) under Grant 2014CB340601, in part by the National Science Foundation of China under Grant 61202386 and Grant 61402339, and in part by the National Cryptography Development Fund under Grant MMJJ201701304.

ABSTRACT Private comparison allows $n(n \geq 2)$ participants who do not trust each other to compare whether their secret data are the same, without leaking the secret data of their own. Quantum private comparison (QPC) uses quantum mechanics to accomplish the comparison. In this paper, we present a simple and effective method which can design QPC protocols based on multi-particle entangled states including the genuinely entangled five-qubit state, the generalized Brown state, the genuine six-qubit entangled state, etc. We take the Bell state and the genuinely entangled five-qubit state as examples, respectively, to present two QPC protocols, where a semi-honest third party who assists two participants in implementing the protocols is assumed. A key feature of our protocols is that quantum states are prepared by two participants rather than by the third party, which effectively prevents the third party from preparing fake quantum states, thus improving the security of the protocols. In addition, we use the entanglement properties of multi-particle entangled states and collaborative computing between participants for privacy protection, and we use QKD to ensure the security of the cooperative computing when two participants are in different locations. We show that the security of our protocols towards both outsider and insider attacks can be guaranteed.

INDEX TERMS Information security, quantum cryptography, quantum private comparison, quantum entanglement, quantum computing.

I. INTRODUCTION

Information security is a major concern in a lot of information transactions. A familiar example is provided by the transactions between web search engines and their users. With the development of information technology, the threat events of information security often happen, which has triggered an enormous demand for secure communication [1]. Quantum cryptography is widely thought to offer unconditional security in the communication between two or more parties, which has received considerable attention and great progress has been achieved in both theory and practice [2]–[4].

Quantum cryptography differs from conventional cryptography in that security is based on the properties of quantum mechanics (e.g. quantum non-cloning theorem and Heisenberg's uncertainty principle) rather than computational complexity [2]. Quantum key distribution (QKD), which allows two parties to share a common secret key or a secret key sequence for cryptographic purposes, is arguably the most extensive and in-depth research direction in the field of quantum communication [2]. In addition to QKD, other technologies of quantum communication like quantum secure direct communication (QSDC), quantum teleportation (QT) and quantum secret sharing (QSS), have also drawn great interest from academic community.

Entanglement plays an extremely important role in the field of quantum information processing (QIP) including quantum cryptography, quantum computing and networked quantum communication [5]–[12]. The rapid progress in theory and experiment of QIP based on entanglement has been reflected by a number of successful demonstrations in the past two decades. In the field of entanglement, the ability to create and fully control multi-particle entangled states is of significant importance to QIP, which is, however, a great challenge. Nevertheless, after decades of development, great achievements have been made in this field [6], [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Angela Sara Cacciapuoti.

Multi-particle entangled states are extensively used to design quantum cryptography protocols, such as QKD protocols, QSS protocols, etc [2]. As an important branch of quantum cryptography, quantum private comparison (QPC), is no exception. QPC allows $n(n \geq 2)$ participants who do not trust each other to compare whether their secret data are the same while maintaining the privacy of their data, in which some principles of quantum mechanics are used (e.g. quantum non-cloning theorem and Heisenberg's uncertainty principle). Most of the existing QPC protocols use multi-particle entangled states as information carriers [13], such as protocols based on bi-partite entangled states [14] (e.g. the Bell state) and other multi-particle entangled states including the GHZ state [15], [16], the χ-type state [17]–[19], the W state [20], [21], the highly entangled six-qubit genuine state [22] and the d-level cat state [23] etc. In most of the previous protocols, the quantum states are prepared by a third party (conventionally called TP), who is responsible for taking part or all of the particles out and sending them to the participants. Subsequently, TP and participants complete the private comparison through quantum measurements, calculations and communications, in which case, however, the security of the protocol is challenging because TP may be misbehaving [24]. For example, TP can prepare fake quantum states or employ entanglement-measurement attack so as to steal the secret data of the participants. In order to resist these attacks, additional means must be adopted, such as the data encryption with the keys generated by QKD, which however, greatly reduces the efficiency of the protocol.

The preparation of quantum states, communication between participants, security checking and quantum measurement are necessary in QPC protocols. In order to complete these processes, corresponding quantum devices are needed. The purpose of quantum measurement is to extract the information carried by quantum states or generate keys among participants. In addition to quantum measurement, most of the QPC protocols employ other kinds of quantum technologies, such as entanglement swapping and unitary operations, all of which require additional quantum devices. However, the addition of these devices inevitably increases the difficulty of the implementation of the protocol, which leads to the decrease of the efficiency. Therefore, considering how to ensure the security and efficiency of the protocol while reducing the consumption of quantum devices has always been a great challenge. One of the best scenarios is that the protocol only uses measurement technology without additional technologies. However, only a few protocols meet this requirement so far. The purpose of security checking is to detect whether there are eavesdroppers in quantum channels. At present, there are mainly two kinds of security checking methods, one is the use of decoy photons for security checking, the other is to prepare some additional entangled states and use their entanglement properties for security checking [22], [23]. The former is preferred in terms of the consumption of measurement devices and the difficulty of preparation and manipulation of quantum states, because the difficulty of preparing and measuring single-particle states are lower than those of preparing and measuring entangled states with current technology. For these reasons, most of the QPC protocols use the former for security checking rather than the latter [22], [23].

In view of the problems mentioned above, in this Letter, we present a simple and effective method which uses several multi-particle entangled states to design QPC protocols, including the Bell state, the genuinely entangled five-qubit state, and the generalized Brown state etc. In fact, different quantum devices and techniques may be required to prepare different multi-particle entangled states. However, in reality, Alice and Bob are unlikely to have all the devices and techniques. That is to say, the devices and techniques they own can only be satisfied with the preparation of one or several multi-particle entangled states, in which case, it makes sense to study how to use our proposed method to design QPC protocols based on more multi-particle entangled states. For the sake of introducing our method, we would only like to take the Bell state and the genuinely entangled five-qubit state as examples and present two QPC protocols, respectively. Compared with most of the previous protocols, our protocols have the following advantages (we make a comparison between our protocols and some previous protocols in Table 1, and note that QKD is only needed when two participants are in different locations): First, our protocols use the entanglement properties of multi-particle entangled states and collaborative computation between participants for data encryption, such that QKD is not needed when two participants are in the same location. Second, our protocols do not use any quantum technologies mentioned above except measurement, hence no additional devices are required. Third, the quantum states are prepared by participants rather than by TP, which naturally resists TP's attacks mentioned above. (The original intention of QPC is that the participants want to achieve the purpose of comparison, in which case the participants will not prepare fake quantum states. Even if they do, they not only disrupt the protocol process, but also fail to steal the secret data from others). The rest of this Letter is structured as follows. In Sec.2, we briefly review the QPC protocols. In Sec.3, we present two QPC protocols based on Bell states and genuinely entangled five-qubit states, respectively. Subsequently, we devote Sec.4 to point out the main differences between them, and introduce some other multi-particle entangled states including the generalized Brown state, the cluster state, the χ-type state, the genuine six-qubit entangled state and the highly entangled six-qubit genuine state, all of which are also showed to be valid for designing QPC protocols by using the method presented in this Letter. We end up this Letter with some conclusions in Sec.5.

II. A BRIEF REVIEW ON THE QPC PROTOCOLS

Private comparison, originated from the millionaires' problem [25], aims to judge whether the secret data of $n(n \geq 2)$ mutually distrustful parties are equal or not without disclosing their respective data to each other. Quantum private com-

parison (QPC), which achieve the purpose of the comparison by using the principle of quantum mechanics, has attracted wide attention in recent years. Most of the QPC protocols introduce a third party (conventionally called TP), who help the participants complete the comparison task. From the point of view of quantum resource consumption and the security of the QPC protocols, the introduction of TP can usually save a lot of quantum resources and improve the security of the protocol [13], [24]. The reliability of TP is generally assumed to be semi-honest, that is, she executes the processes of the protocol loyally, but she is allowed to steal the secret data of the participants with any possible means without conspiring with any dishonest participants [13]. Generally, a QPC protocol should satisfy two conditions: (1) Fairness: all parties get the comparison result simultaneously, in no particular order. (2) Security: the secret data of each participant is confidential and unavailable to both other parties and TP. In addition, external attackers cannot steal the comparison result and the data of the participants.

In a QPC procol, TP is usually responsible for preparing quantum states and sending part or all of the particles to the participants, then participating in measurements, calculations, recording and publishing the results. There are two main opportunities for TP to steal the participants' secret data (i.e. TP's attacks). One is that he can prepare fake quantum states in the process of preparing quantum states. The other is that when he participates in the computations in the protocol, he can record the results of intermediate computations and try to deduce the secret data of the participants from these results. For the first attack, the existing protocols usually adopt the following two defensive measures: one is to prepare additional quantum entangled states, and use their entanglement correlations to verify the authenticity of the quantum states prepared by TP; the other is to encrypt the participants' secret data with the keys generated by QKD. For the second attack, the existing protocols also have two defensive measures: one is to use the entanglement correlations of the entangled states adopted in the protocol; the other is to use the keys generated by QKD to encrypt the participants' secret data, in which the keys are usually generated at the same time as the keys mentioned above. In general, TP can only be dishonest when preparing quantum states (as for the behavior of recording the intermediate calculation results, it does not belong to the processes of the protocol, and the protocol can not verify whether he has done so, hence the above defensive measures are adopted to ensure security). For the other processes of the protocol, he will faithfully implement them. In fact, even if TP is dishonest in other processes, it is not helpful for him to steal the participants' secret data. For example, if he announces false comparison results to the participants at the last step of the protocol, he can't steal the participants' secret data in this way.

In 2009, Yang and Wen [14] proposed the first QPC protocol based on decoy photons and two-photon entangled Einstein-Podolsky-Rosen (EPR) pairs. Later, Chen *et al.* [15] proposed a new protocol based on triplet entangled GHZ states in 2010. Since then, numerous multi-particle entangled states have been exploited for designing QPC protocols [26]–[33]. The early protocols aims to complete the equality comparison between two parties, and subsequent protocols expands to the multi-party situation [23], [29], [30] and size comparison [32], [33]. In recent years, the QPC protocols based on various quantum technologies have been extensively studied [34]–[37]. However, the research on QPC is still at an early stage, and many questions remain. On the one hand, a lot of protocols have been proved unsafe, e.g. information leakage problems often occur [38]–[54]. On the other hand, additional quantum resources are needed in order to ensure the security of the protocols, such that the protocols do not satisfy the high efficiency requirement. Therefore, designing a secure and efficient protocol is still challenging.

III. THE PROPOSED PROTOCOLS

In this section, we present two QPC protocols with Bell states and genuinely entangled five-qubit states, respectively. By this way, we aim to introduce our method which can use a number of multi-particle entangled states to design QPC protocols. Now let us describe our protocols.

A. PROTOCOL I: THE QUANTUM PRIVATE COMPARISON PROTOCOL WITH BELL STATES

1) PREREQUISITES

1) Assume that there are two parties, conventionally called Alice and Bob, who have secret data X and Y respectively, and the binary representations of X and Y in F_{2^N} are $(x_1, x_2, \ldots, x_N)$ and $(y_1, y_2, \ldots, y_N)$ respectively, where $x_j, y_j \in \{0, 1\}, X = \sum_{j=1}^{N} x_{j-1}2^j, Y = \sum_{j=1}^{N} y_{j-1}2^j, j = 1, 2, \ldots, N, 2^{N-1} \leq \max\{x, y\} < 2^N$. They want to judge whether or not X and Y are equal with the assistance of a semi-honest third party (named TP) who may misbehave on his own but will not conspire with either of the two parties (see Sec.II).
2) Alice(Bob) divides the binary representation of $X(Y)$ into $\lceil N/n \rceil$ groups:

$$G_a^1, G_a^2, \ldots, G_a^{\lceil \frac{N}{n} \rceil}(G_b^1, G_b^2, \ldots, G_b^{\lceil \frac{N}{n} \rceil}), \tag{1}$$

where n is a positive integer less than N (i.e. $1 \leq n \leq N$), and each group $G_a^i(G_b^i)$ includes n bits ($i = 1, 2, \ldots, \lceil N/n \rceil$ throughout this protocol). If N mod n = k, Alice(Bob) adds k 0 into the last group $G_a^{\lceil N/n \rceil}(G_b^{\lceil N/n \rceil})$.
3) Alice and Bob agree that $|0\rangle$ encodes classical bit "0" and $|1\rangle$ encodes classical bit "1".

2) THE DETAILED STEPS OF THE PROTOCOL

1) *Step 1:* Prepare quantum states.
Alice(Bob) prepares $\lceil N/n \rceil$ copies of the Bell state

$$\left| G(p^1, p^2) \right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{1,2}, \tag{2}$$

and marks them by

$$\left|G(a_1^1, a_1^2)\right\rangle, \left|G(a_2^1, a_2^2)\right\rangle, \ldots, \left|G(a_{\lceil N/n\rceil}^1, a_{\lceil N/n\rceil}^2)\right\rangle$$
$$(\left|G(b_1^1, b_1^2)\right\rangle, \left|G(b_2^1, b_2^2)\right\rangle, \ldots, \left|G(b_{\lceil N/n\rceil}^1, b_{\lceil N/n\rceil}^2)\right\rangle) \quad (3)$$

in turn to generate an ordered sequence, where the subscripts $1, 2, \ldots, \lceil N/n\rceil$ denote the order of the Bell states in the sequence, and the superscripts 1,2 denote two particles in one Bell state, respectively. Then Alice(Bob) takes the first particles marked by $a_i^1(b_i^1)$ out from $\left|G(a_i^1, a_i^2)\right\rangle(\left|G(b_i^1, b_i^2)\right\rangle)$ to construct the new sequence $a_1^1, a_2^1, \ldots, a_{\lceil N/n\rceil}^1$ (b_1^1, b_2^1,…., $b_{\lceil N/n\rceil}^1$) and denotes it by $S_a(S_b)$. The remaining particles construct another new sequence $a_1^2, a_2^2, \ldots, a_{\lceil N/n\rceil}^2(b_1^2, b_2^2, \ldots, b_{\lceil N/n\rceil}^2)$, denoted as $S_a'(S_b')$.

2) *Step 2:* Distribution.
In order to check the presence of eavesdroppers, Alice(Bob) adopts the decoy photon technique by inserting decoy photons into the sequence $S_a(S_b)$ at random positions to form a new sequence $S_a^*(S_b^*)$, in which each decoy photon is randomly chosen from four single-particle states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, ($|\pm\rangle = 1/\sqrt{2}$ ($|0\rangle \pm |1\rangle$), $|0\rangle$ and $|1\rangle$ can be measured by the Z basis $\{|0\rangle, |1\rangle\}$; $|+\rangle$ and $|-\rangle$ can be measured by the X basis $\{|+\rangle, |-\rangle\}$) [14], [18], [22], [23], [26], [28], [31]. Then Alice(Bob) sends $S_a^*(S_b^*)$ to TP.

3) *Step 3:* Security checking.
After receiving S_a^* and S_b^*, TP and Alice(Bob) use the decoy photons in $S_a^*(S_b^*)$ to check the security of the transmission. Concretely, Alice(Bob) announces the positions and bases of the decoy photons to TP. Then TP performs the corresponding measurements and returns the measurement outcomes to Alice(Bob). They can judge whether eavesdroppers exist in the quantum channels through comparing the initial states and the measurement outcomes of the decoy photons. If the error rate is higher than the predetermined threshold, they will abort the protocol and restart it. Otherwise, they proceed to next step.

4) *Step 4:* Encryption and collaborative computing.
Alice(Bob) establishes the new variables $R_a^i(R_b^i)$ and sets $R_a^i = G_a^i(R_b^i = G_b^i)$. Then she(he) performs single-particle measurements on each particle in $S_a'(S_b')$ with Z basis, and obtains the measurement outcomes marked by $M_a^i(M_b^i)$. Subsequently, Alice(Bob) encrypts her(his) secret data $G_a^i(G_b^i)$ according to the value of $M_a^i(M_b^i)$. Concretely, if $M_a^i = 1(M_b^i = 1)$, she(he) flips each bit in $R_a^i(R_b^i)$, otherwise $R_a^i(R_b^i)$ will remain unchanged. For example, suppose that $R_a^i = 10100$, flip R_a^i to 01011 if $M_a^i = 1$, otherwise keep $R_a^i = 10100$ unchanged. Subsequently, Alice and Bob cooperate together to compute $R_a^i \oplus R_b^i$, and denote the computing results as R_{AB}^i. Finally, they announce R_{AB}^i to TP publicly. (Here, the collaborative computing includes two situations: one is that Alice and Bob are at the same location, in which case they can cooperate directly to complete the computing; the other is that they are in different locations, in which case, they can complete the computing through QKD. That is, they first tell each other their computing results through QKD, and then each proceeds to the next computing. It should be pointed out that in this case, they will not be dishonest, because their original purpose is to achieve the private comparison. If they publish false data to each other and to TP, they can not get the correct comparison results. Furthermore, once TP finds that the data published to him are different, she will know that one of them is dishonest and terminate the protocol. For these reasons, Alice and Bob will not be dishonest.)

5) *Step 5:* Comparison.
After receiving R_{AB}^i, TP performs single-particle measurements on each particle in S_a and S_b with Z basis. That is, TP measures the particles marked by a_i^1 and b_i^1 in S_a and S_b, respectively. The measurement results are denoted as $M_{ac}^i M_{bc}^i$, where M_{ac}^i and M_{bc}^i corresponding to the measurement outcomes of a_i^1 and b_i^i, respectively. TP establishes the new variables R_i and sets $R_i = R_{AB}^i$. According to the values of $M_{ac}^i M_{bc}^i$, TP changes the values of R_i as follows.
   a) If $M_{ac}^i M_{bc}^i \in \{|00\rangle, |11\rangle\}$, then keep R_i unchanged.
   b) If $M_{ac}^i M_{bc}^i \in \{|01\rangle, |10\rangle\}$, then flip each bit in R_i.

   Denote the binary representation of R_i as $b_i^1 b_i^2 b_i^3 \ldots b_i^n$. TP computes

$$S = \sum_{i=1}^{\lceil N/n\rceil} \sum_{j=1}^{n} b_i^j. \quad (4)$$

   If $S = 0$, TP concludes that $X = Y$ otherwise $X \neq Y$. Finally, TP publicly tells Alice and Bob the comparison result (Here, TP will publish the correct results, for more details see Sec.II).

B. PROTOCOL II: THE QUANTUM PRIVATE COMPARISON PROTOCOL WITH GENUINELY ENTANGLED FIVE-QUBIT STATES

In what follows, in the same way introduced in Sec.3.1, we use the genuinely entangled five-qubit state to present a new QPC protocol. For the sake of simplicity, we would like to briefly describe this protocol, and we intentionally left out a few processes on the premise of not causing to misunderstand the steps of the protocol. Furthermore, as far as possible, we use the same marks adopted in Protocol I to describe the steps of this protocol.

1) PREREQUISITES

Alice(Bob) has secret data $X(Y)$, she(he) divides the binary representation of $X(Y)$ into $\lceil N/3 \rceil$ groups:

$$G_a^1, G_a^2, \ldots, G_a^{\lceil \frac{N}{3} \rceil}(G_b^1, G_b^2, \ldots, G_b^{\lceil \frac{N}{3} \rceil}), \tag{5}$$

where each group $G_a^i(G_b^i)$ includes three bits ($i = 1, 2, \ldots, \lceil N/3 \rceil$ throughout this protocol). If $N \bmod 3 = k$, Alice(Bob) adds k 0 into the last group $G_a^{\lceil N/3 \rceil}(G_b^{\lceil N/3 \rceil})$.

2) THE DETAILED STEPS OF THE PROTOCOL

1) *Step 1:* Prepare quantum states.
Alice(Bob) prepares $\lceil N/3 \rceil$ copies of the genuinely entangled five-qubit state which has the expression [28], [55]

$$\begin{aligned}\left|\Psi(p^1, p^2, p^3, p^4, p^5)\right\rangle = \frac{1}{2}(&|001\rangle \left|\psi^-\right\rangle \\ &+ |010\rangle \left|\phi^-\right\rangle + |100\rangle \left|\psi^+\right\rangle + |111\rangle \left|\phi^+\right\rangle)_{12345},\end{aligned} \tag{6}$$

where

$$\begin{aligned}\left|\phi^\pm\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ \left|\psi^\pm\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle),\end{aligned} \tag{7}$$

are four Bell states. Then she(he) marks them by

$$\begin{aligned}&\left|\Psi(a_1^1, a_1^2, a_1^3, a_1^4, a_1^5)\right\rangle, \left|\Psi(a_2^1, a_2^2, a_2^3, a_2^4, a_2^5)\right\rangle, \ldots, \\ &\left|\Psi(a_{\lceil N/3 \rceil}^1, a_{\lceil N/3 \rceil}^2, a_{\lceil N/3 \rceil}^3, a_{\lceil N/3 \rceil}^4, a_{\lceil N/3 \rceil}^5)\right\rangle \\ &(\left|\Psi(b_1^1, b_1^2, b_1^3, b_1^4, b_1^5)\right\rangle, \left|\Psi(b_2^1, b_2^2, b_2^3, b_2^4, b_2^5)\right\rangle, \ldots, \\ &\left|\Psi(b_{\lceil N/3 \rceil}^1, b_{\lceil N/3 \rceil}^2, b_{\lceil N/3 \rceil}^3, b_{\lceil N/3 \rceil}^4, b_{\lceil N/3 \rceil}^5)\right\rangle),\end{aligned} \tag{8}$$

where the subscripts $1, 2, \ldots, \lceil N/3 \rceil$ denote the order of the genuinely entangled five-qubit states in the sequence. and the superscripts 1,2,3,4,5 denote five particles in one state, respectively.
Alice(Bob) takes the particles marked by $a_i^4, a_i^5(b_i^4, b_i^5)$ out from $\left|\Psi(a_i^1, a_i^2, a_i^3, a_i^4, a_i^5)\right\rangle(\left|\Psi(b_i^1, b_i^2, b_i^3, b_i^4, b_i^5)\right\rangle)$ to construct the new sequence

$$\begin{aligned}&a_1^4 a_1^5, a_2^4 a_2^5, \ldots, a_{\lceil N/3 \rceil}^4 a_{\lceil N/3 \rceil}^5 \\ &(b_1^4 b_1^5, b_2^4 b_2^5, \ldots, b_{\lceil N/3 \rceil}^4 b_{\lceil N/3 \rceil}^5),\end{aligned} \tag{9}$$

denoted as $S_a(S_b)$. The remaining particles construct another new sequence

$$\begin{aligned}&a_1^1 a_1^2 a_1^3, a_2^1 a_2^2 a_2^3, \ldots, a_{\lceil N/3 \rceil}^1 a_{\lceil N/3 \rceil}^2 a_{\lceil N/3 \rceil}^3 \\ &(b_1^1 b_1^2 b_1^3, b_2^1 b_2^2 b_2^3, \ldots, b_{\lceil N/3 \rceil}^1 b_{\lceil N/3 \rceil}^2 b_{\lceil N/3 \rceil}^3),\end{aligned} \tag{10}$$

denoted as $S'_a(S'_b)$.
2) *Step 2:* Distribution.
Alice(Bob) inserts decoy photons into the sequence $S_a(S_b)$ at random positions to form the new sequence $S_a^*(S_b^*)$, in which each decoy photon is randomly chosen from $|0\rangle, |1\rangle, |+\rangle, |-\rangle$. Then she(he) sends $S_a^*(S_b^*)$ to TP.
3) *Step 3:* Security checking.
TP and Alice(Bob) use the decoy photons for security check. If there are no eavesdroppers, they will continue, otherwise they stop and restart the protocol.
4) *Step 4:* Encryption and collaborative computing.
Alice(Bob) performs measurements on $S'_a(S'_b)$ with Z basis. Concretely, she(he) measures three particles $a_i^1\ a_i^2\ a_i^3(b_i^1\ b_i^2\ b_i^3)$ in $S'_a(S'_b)$, and denotes the measurement outcomes as $M_a^i(M_b^i)$. After that, Alice(Bob) computes $G_a^i \oplus M_a^i(G_b^i \oplus M_b^i)$ and denotes the computing results as $R_a^i(R_b^i)$. Subsequently, Alice and Bob cooperate together to compute $R_a^i \oplus R_b^i$ and denote the results as R_{AB}^i. Finally they publicly announce R_{AB}^i to TP.
5) *Step 5:* Comparison.
After receiving R_{AB}^i, TP uses Bell basis ($\{\left|\phi^\pm\right\rangle, \left|\psi^\pm\right\rangle\}$) to measure the particles $a_i^4 a_i^5$ and $b_i^4 b_i^5$, respectively. The collapsed Bell states are denoted as $M_{ac}^i M_{bc}^i$, where M_{ac}^i and M_{bc}^i consist with the measurement outcomes of the particles $a_i^4 a_i^5$ and $b_i^4 b_i^5$, respectively.
TP establishes the new variables M_C^i, then sets the values of M_C^i according to $M_{ac}^i M_{bc}^i$. Concretely,
   a) if $M_{ac}^i M_{bc}^i \in \{\left|\phi^+\right\rangle\left|\phi^+\right\rangle, \left|\phi^-\right\rangle\left|\phi^-\right\rangle, \left|\psi^+\right\rangle\left|\psi^+\right\rangle, \left|\psi^-\right\rangle\left|\psi^-\right\rangle\}$, then $M_C^i = 000$.
   b) if $M_{ac}^i M_{bc}^i \in \{\left|\phi^-\right\rangle\left|\psi^+\right\rangle, \left|\psi^-\right\rangle\left|\phi^+\right\rangle, \left|\psi^+\right\rangle\left|\phi^-\right\rangle, \left|\phi^+\right\rangle\left|\psi^-\right\rangle\}$, then $M_C^i = 110$.
   c) if $M_{ac}^i M_{bc}^i \in \{\left|\phi^-\right\rangle\left|\psi^-\right\rangle, \left|\phi^+\right\rangle\left|\psi^+\right\rangle, \left|\psi^-\right\rangle\left|\phi^-\right\rangle, \left|\psi^+\right\rangle\left|\phi^+\right\rangle\}$, then $M_C^i = 011$.
   d) if $M_{ac}^i M_{bc}^i \in \{\left|\phi^-\right\rangle\left|\phi^+\right\rangle, \left|\psi^-\right\rangle\left|\psi^+\right\rangle, \left|\phi^+\right\rangle\left|\phi^-\right\rangle, \left|\psi^+\right\rangle\left|\psi^-\right\rangle\}$, then $M_C^i = 101$.

TP computes $R_{AB}^i \oplus M_C^i$ and denotes the results as R_i, where the binary representation of R_i is denoted as $b_i^1 b_i^2 b_i^3$. TP computes

$$S = \sum_{i=1}^{\lceil N/3 \rceil} \sum_{j=1}^{3} b_i^j. \tag{11}$$

If $S = 0$, TP concludes that $X = Y$, otherwise $X \neq Y$. Finally, TP publicly tells Alice and Bob the comparison result.

IV. DISCUSSIONS

Based on different quantum states, we have proposed two QPC protocols above. It seems to make sense that we point out the main differences between them. One is the difference of the measurement means: protocol I only uses single-particle measurements, while protocol II uses not only single-particle measurements, but also Bell measurements. Another is the difference of encryption methods: Protocol I realizes the data encryption by using the method of whether to flip each bit in the secret data or not, whereas Protocol II uses the measurement outcomes of quantum states for the data encryption (see Steps 4). Regardless of these differences, it is

TABLE 1. The comparison between our protocols and some previous QPC protocols.

Reference	[14]	[15]	[16]	[17]	[20]	[21]	[22]	[26]	[28]	[31]	Our protocols
QKD	√	×	√	√	√	√	√	×	√	×	√
Unitary operations	√	√	×	√	×	×	×	√	×	√	×
Entanglement swapping	×	×	√	√	×	√	×	×	×	×	×
Quantum resources used for security checking	Decoy photons	GHZ states	Decoy photons	χ-type states	Decoy photons	Bell states	Decoy photons	Decoy photons	Decoy photons	Decoy photons	Decoy photons

easy to find that the methods adopted by the two protocols are essentially the same. Therefore, with the same method and different quantum states, we can design QPC protocols only by changing the encoding mode and measuring means appropriately. In what follows we introduce some other multi-particle entangled states, all of which can be used to design QPC protocols by using the same encryption method adopted by Protocol II and modifying their expressions appropriately. However, we would only like to rewrite their expressions and omit the descriptions of the protocols for the sake of brevity and saving space.

A. THE GENERALIZED BROWN STATE

The generalized Brown state was derived from the genuinely entangled five-qubit state, has the expression [55]

$$|\Psi_{n+5}\rangle = \frac{1}{2}(|\eta_1\rangle_n |001\rangle |\psi^-\rangle + |\eta_2\rangle_n |010\rangle |\phi^-\rangle + |\eta_3\rangle_n |100\rangle |\psi^+\rangle + |\eta_4\rangle_n |111\rangle |\phi^+\rangle), \quad (12)$$

where the set $|\eta_i\rangle_n\,(i = 1, 2, 3, 4)$ are the computational basis of nth order. For example, if $n = 2$, the generalized seven-qubit Brown state $|\Psi_7\rangle$ is

$$|\Psi_7\rangle = \frac{1}{2}(|00\rangle |001\rangle |\psi^-\rangle + |01\rangle |010\rangle |\phi^-\rangle + |10\rangle |100\rangle |\psi^+\rangle + |11\rangle |111\rangle |\phi^+\rangle). \quad (13)$$

B. THE CLUSTER STATE

The cluster state has the form [26], [27], [58]

$$|C\rangle = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle). \quad (14)$$

C. THE χ-TYPE STATE

The χ-type state has the form

$$|\chi\rangle = \frac{\sqrt{2}}{4}(|0000\rangle - |0101\rangle + |0011\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle - |1111\rangle). \quad (15)$$

One can rewrite it as

$$|\chi\rangle = \frac{1}{2}(|00\rangle |\phi^+\rangle + |11\rangle |\phi^-\rangle - |01\rangle |\psi^-\rangle + |10\rangle |\psi^+\rangle) = \frac{1}{2}(|\phi^+\rangle |00\rangle + |\phi^-\rangle |11\rangle - |\psi^-\rangle |01\rangle + |\psi^+\rangle |10\rangle). \quad (16)$$

D. THE GENUINE SIX-QUBIT ENTANGLED STATE

The genuine six-qubit entangled state has the form [57]

$$|\Upsilon\rangle = \frac{1}{\sqrt{8}}(|000000\rangle + |011100\rangle + |111000\rangle + |100100\rangle + |001111\rangle + |010011\rangle + |110111\rangle + |101011\rangle). \quad (17)$$

One can rewrite it as

$$|\Upsilon\rangle = \frac{1}{\sqrt{8}}(|G_0^+\rangle |000\rangle + |G_1^+\rangle |111\rangle + |G_2^+\rangle |011\rangle + |G_3^+\rangle |100\rangle), \quad (18)$$

where

$$|G_0^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$
$$|G_1^+\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle),$$
$$|G_2^+\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle),$$
$$|G_3^+\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle), \quad (19)$$

can be measured by GHZ states basis.

E. THE HIGHLY ENTANGLED SIX-QUBIT GENUINE STATE

The highly entangled six-qubit genuine state has the form [22], [56]

$$\begin{aligned}|\Upsilon\rangle_{123456} = \frac{1}{\sqrt{32}}\big[&|000000\rangle + |111111\rangle + |000011\rangle \\ &+ |111100\rangle + |000101\rangle + |111010\rangle + |000110\rangle \\ &+ |111001\rangle + |001001\rangle + |110110\rangle + |001111\rangle \\ &+ |110000\rangle + |010001\rangle + |101110\rangle + |010010\rangle \\ &+ |101101\rangle + |011000\rangle + |100111\rangle + |011101\rangle \\ &+ |100010\rangle - \big(|010100\rangle + |101011\rangle + |010111\rangle \\ &+ |101000\rangle + |011011\rangle + |100100\rangle + |001010\rangle \\ &+ |110101\rangle + |001100\rangle + |110011\rangle + |011110\rangle \\ &+ |100001\rangle \big)\big]_{123456}. \end{aligned} \quad (20)$$

One can rewrite it as

$$|\Upsilon\rangle = \frac{1}{\sqrt{8}}(|000\rangle |\gamma_1\rangle + |001\rangle |\gamma_2\rangle + |010\rangle |\gamma_3\rangle + |011\rangle |\gamma_4\rangle - |100\rangle |\gamma_5\rangle - |101\rangle |\gamma_6\rangle + |110\rangle |\gamma_7\rangle + |111\rangle |\gamma_8\rangle), \quad (21)$$

where

$$\begin{aligned}
\left|\gamma_{1/6}\right\rangle &= \frac{1}{4}(|0\rangle\left|\phi^{+}\right\rangle \pm |1\rangle\left|\psi^{+}\right\rangle),\\
\left|\gamma_{2/5}\right\rangle &= \frac{1}{4}(|0\rangle\left|\psi^{+}\right\rangle \mp |1\rangle\left|\phi^{+}\right\rangle),\\
\left|\gamma_{3/8}\right\rangle &= \frac{1}{4}(|0\rangle\left|\psi^{+}\right\rangle \mp |1\rangle\left|\phi^{+}\right\rangle),\\
\left|\gamma_{4/7}\right\rangle &= \frac{1}{4}(|0\rangle\left|\psi^{+}\right\rangle \pm |1\rangle\left|\phi^{+}\right\rangle),
\end{aligned} \tag{22}$$

form a complete set of orthonormal basis on Hilbert space $C_2 \otimes C_2 \otimes C_2$.

Next, we would like to point out the main differences between our protocols and Refs. [22], [28] as they use the same quantum states as our protocols. The first is the difference in application scenarios. In Refs. [22], [28], the quantum states and decoy photons are prepared by TP. TP takes out some particles and sends them to the participants, then they make a series of calculations and measurements, and finally complete the private comparison. It can be seen that TP needs to have the corresponding devices for preparing quantum states and performing measurements, and two participants only need to have the measurement devices. While in our protocol, the participants need to have the devices for the state preparations and measurements, and TP only needs to have measurement devices. Therefore, the scenarios in which our protocols apply are different from that of Refs. [22], [28]. The second is the difference in the method of ensuring security. Reference [22], [28] use decoy photon technology, the entanglement properties of the states, and QKD to ensure the security of the protocol. While in our protocol, QKD is required only when two participants are in different locations, otherwise QKD is not needed.

V. SECURITY ANALYSIS

In what follows we analyze the security of our protocols. We would only like to analyze the security of Protocol I due to the security of Protocol II is the same as that of Protocol I, and please note that we assume that the quantum channels in our protocols are authenticated. We show that the attacks from outside eavesdroppers, and the attacks from participants and TP are all invalid to our protocols.

A. OUTSIDER ATTACK

In our protocols, we use decoy photons for security checking (see Step 3), the idea of which is derived from the proved unconditional secure QKD protocols [59]. It has been proved that the security checking process can detect any attack from external eavesdroppers, such as the intercept-resend attack, the measurement-resend attack, the entanglement-measurement attack and the denial-of-service attack, etc [59]. We would like to take the intercept-resend attack and entanglement-measurement attack as examples, respectively, to show that outsider attacks will be discovered by the security checking process.

1) INTERCEPT-RESEND ATTACK

If an external eavesdropper, conventionally called Eve, attempts to intercept the particles sent from TP to a participant and replaces them with fake ones, he will introduce extra error rate which makes him be detected during the security checking process since he does not know the exact position and the original state of the decoy photons. If using m decoy photons for security checking, the probability of detecting the existence of Eve is $1-(3/4)^m$, which is close to 1 if m is large enough [30]. Therefore, this attack will not succeed.

2) ENTANGLEMENT-MEASUREMENT ATTACK

Next we analyze the entanglement-measurement attack. Concretely, Eve intercepts part or all of the particles transmitted in the quantum channels between TP and Alice(Bob). Then Eve entangles them with ancillary particles prepared beforehand and resends them to the receiver. Finally, he performs measurements on the ancillary particles to extract information after the participants finish their communication. We would only like to analyze the case that Eve intercepts the particles transmitted in the quantum channel between TP and Alice here. As for the attack on the channel between TP and Bob, analysis can be carried out in the same way.

Without loss of generality, the action of Eve's unitary operator, marked by U, can be expressed as follows:

$$\begin{aligned}
U\left|0\right\rangle\left|\varepsilon\right\rangle &= a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle + a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle,\\
U\left|1\right\rangle\left|\varepsilon\right\rangle &= a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle + a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle,
\end{aligned} \tag{23}$$

where $|\epsilon_{00}\rangle$, $|\epsilon_{01}\rangle$, $|\epsilon_{10}\rangle$, $|\epsilon_{11}\rangle$ are pure states uniquely determined by U, $|\varepsilon\rangle$ is the ancillary particle, and $||a_{00}||^2 + ||a_{01}||^2 = 1$, $||a_{10}||^2 + ||a_{11}||^2 = 1$. The decoy photon is one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, if U acts on the decoy states $|+\rangle$ and $|-\rangle$, one can get

$$\begin{aligned}
U\left|+\right\rangle\left|\varepsilon\right\rangle &= \frac{1}{\sqrt{2}}(a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle + a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle\\
&\quad + a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle + a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle)\\
&= \frac{1}{2}\left|+\right\rangle(a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle + a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle\\
&\quad + a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle + a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle)\\
&\quad + \frac{1}{2}\left|-\right\rangle(a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle - a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle\\
&\quad + a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle - a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle),
\end{aligned} \tag{24}$$

$$\begin{aligned}
U\left|-\right\rangle\left|\varepsilon\right\rangle &= \frac{1}{\sqrt{2}}(a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle + a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle\\
&\quad - a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle - a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle)\\
&= \frac{1}{2}\left|+\right\rangle(a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle + a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle\\
&\quad - a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle - a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle)\\
&\quad + \frac{1}{2}\left|-\right\rangle(a_{00}\left|0\right\rangle\left|\epsilon_{00}\right\rangle - a_{01}\left|1\right\rangle\left|\epsilon_{01}\right\rangle\\
&\quad - a_{10}\left|0\right\rangle\left|\epsilon_{10}\right\rangle + a_{11}\left|1\right\rangle\left|\epsilon_{11}\right\rangle).
\end{aligned} \tag{25}$$

If Eve wishes to introduce no error in the security checking process, his unitary operator U must satisfies the conditions of $a_{01} = a_{10} = 0$ and $a_{00}\left|\epsilon_{00}\right\rangle = a_{11}\left|\epsilon_{11}\right\rangle$. If U is performed

on the first particle in $\left|G(p^1, p^2)\right\rangle$, one can get

$$\begin{aligned} U\left|G(p^1,p^2)\right\rangle|\varepsilon\rangle &= \frac{1}{\sqrt{2}}[(a_{00}|0\rangle|\epsilon_{00}\rangle + a_{01}|1\rangle|\epsilon_{01}\rangle)|0\rangle \\ &\quad + (a_{10}|0\rangle|\epsilon_{10}\rangle + a_{11}|1\rangle|\epsilon_{11}\rangle)|1\rangle] \\ &= \frac{1}{\sqrt{2}}(a_{00}|00\rangle|\epsilon_{00}\rangle + a_{00}|11\rangle|\epsilon_{11}\rangle) \\ &= a_{00}\left|G(p^1,p^2)\right\rangle|\epsilon_{00}\rangle . \end{aligned} \tag{26}$$

As can be seen from the above equation, no error is introduced only when the ancillary state and the state of intercepted particle are product states. Therefore, this attack is invalid to the protocol.

B. INSIDER ATTACK

In this section, we analyze the insider attacks including the ones from a dishonest participant and the ones from TP.

1) CASE 1: THE ATTACKS FROM A DISHONEST PARTICIPANT

Due to Alice and Bob play the same roles in the protocol, without loss of generality, we assume that Alice is dishonest and she wants to steal Bob's secret data. Throughout the protocol, there are no particles transmitted between Alice and Bob. If Alice attempts to intercept the transmitted particles sent from Bob to TP in Step 2, she will fail because of her attack behaviors are equivalent to those of external eavesdroppers, which has been analyzed above.

In Step 4, Alice and Bob cooperate together to compute $R^i_{AB} = R^i_a \oplus R^i_b (i = 1, 2, \ldots, \lceil N/n \rceil)$, where the values of R^i_A and R^i_B are determined by M^i_a and M^i_b, respectively (please see Step 4). In this case, Alice can guess G^i_b with the successful probability of 50%, hence she can guess Bob's secret data Y with the successful probability of $1/2^{\lceil N/n \rceil}$, where $1/2^{\lceil N/n \rceil}$ decreases with the increase of $\lceil N/n \rceil$ (We can increase $\lceil N/n \rceil$ by decreasing n). Therefore, the probability that Alice guesses Bob's secret data can be made as small as $1/2^{\lceil N/n \rceil}$ and as large as 0.5, by varying the value of n.

2) CASE 2: THE ATTACKS FROM TP

Throughout the protocol, the only information sent to TP from Alice and Bob is R^i_{AB} (see Steps 4 and 5). At the end of the protocol, TP obtains $R^i_a \oplus R^i_b$, thus TP cannot steal any information about their secret data except the comparison result.

VI. CONCLUSION

We have proposed a number of QPC protocols with different multi-particle entangled states. Our protocols use no other quantum technologies except quantum measurement. In addition, the quantum states are prepared by participants rather than by TP, which makes our protocol more secure and efficient. What is more, our protocols use the entanglement properties of multi-particle entangled states and collaborative computing for privacy protection, thus the use of QKD is avoided when the participants are in the same location. Last but not least, TP cannot steal the secret data of the participants, one participant cannot steal the other's secret data except the case that their data are identical.

We believe that there will be some multi-particle entangled states we haven't found can also be used to design QPC protocols by the method presented in this Letter. This requires further study.

ACKNOWLEDGMENT

The authors would like to thank to the anonymous referees for their helpful comments and suggestions to improve the quality of the Letter.

REFERENCES

[1] H. G. Zhang, W. B. Han, X. J. Lai, D. D. Lin, J. F. Ma, and J. H. Li, "Survey on cyberspace security," *Sci. China Inf. Sci.*, vol. 58, no. 11, pp. 1–43, 2015.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.
[3] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, 2014.
[4] R.Alléaume *et .al*, "Using quantum key distribution for cryptographic purposes: A survey," *Theor. Comput. Sci.*, vol. 560, pp. 62–81, Dec. 2014.
[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, 2009.
[7] X.-L. Wang *et .al*, "18-Qubit entanglement with six photons' three degrees of freedom," *Phys. Rev. Lett.*, vol. 120, no. 26, 2018, Art. no. 260502.
[8] L. O. Mailloux *et .al*, "A modeling framework for studying quantum key distribution system implementation nonidealities," *IEEE Access*, vol. 3, no. 1, pp. 110–130, 2015.
[9] H. Cao and W. Ma, "Verifiable threshold quantum state sharing scheme," *IEEE Access*, vol. 6, pp. 10453–10457, 2018.
[10] M. Alshowkan and K. M. Elleithy, "Deterministic and efficient quantum key distribution using entanglement parity bits and ancillary qubits," *IEEE Access*, vol. 5, pp. 25565–25575, 2017.
[11] C. H. Park *et .al*, "Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing," *IEEE Access*, vol. 6, pp. 58587–58593, 2018.
[12] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.
[13] W. Liu, C. Liu, H. Wang, and T. Jia, "Quantum private comparison: A review," *IETE Tech. Rev.*, vol. 30, no. 5, pp. 439–445, 2013.
[14] 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, 2009, Art. no. 055305.
[15] 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, 2010.
[16] W. Liu and Y.-B. Wang, "Quantum private comparison based on GHZ entangled states," *Int. J. Theor. Phys.*, vol. 51, no. 11, pp. 3596–3604, 2012.
[17] W. Liu, Y.-B. Wang, Z.-T. Jiang, and Y.-Z. Cao, "A protocol for the quantum private comparison of equality with χ-type state," *Int. J. Theor. Phys.*, vol. 51, no. 1, pp. 69–77, 2012.
[18] W. Liu, Y.-B. Wang, Z.-T. Jiang, Y.-Z. Cao, and W. Cui, "New quantum private comparison protocol using χ-Type State," *Int. J. Theor. Phys.*, vol. 51, no. 6, pp. 1953–1960, 2012.
[19] S. Lin, G.-D. Guo, and X.-F. Liu, "Quantum private comparison of equality with χ-type entangled states," *Int. J. Theor. Phys.*, vol. 52, no. 11, pp. 4185–4194, 2013.
[20] W.-W. Zhang, D. Li, and Y.-B. Li, "Quantum private comparison protocol with W states," *Int. J. Theor. Phys.*, vol. 53, no. 5, pp. 1723–1729, 2014.
[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, 2014.

[22] Z.-X. Ji and T.-Y. Ye, "Quantum private comparison of equal information based on highly entangled six-Qubit genuine state," *Commun. Theor. Phys.*, vol. 65, no. 6, p. 711, 2016.
[23] J. Zhao-Xu and Y. Tian-Yu, "Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level bell states," *Quantum Inf. Process.*, vol. 16, no. 7, p. 177, 2017.
[24] Y.-G. Yang, J. Xia, X. Jia, and H. Zhang, "Comment on quantum private comparison protocols with a semi-honest third party," *Quantum Inf. Process.*, vol. 12, no. 2, pp. 877–885, 2013.
[25] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci.*, vol. 82, Nov. 1982, pp. 160–164.
[26] Z. W. Sun and D. Y. Long, "Quantum private comparison protocol based on cluster states," *Int. J. Theor. Phys.*, vol. 52, no. 1, pp. 212–218, 2013.
[27] G.-A. Xu, X.-B. Chen, Z.-H. Wei, M.-J. Li, and Y.-X. Yang, "An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state," *Int. J. Quantum Inf.*, vol. 10, no. 4, 2012, Art. no. 1250045.
[28] T.-Y. Ye and Z.-X. Ji, "Two-party quantum private comparison with five-qubit entangled states," *Int. J. Theor. Phys.*, vol. 56, no. 5, pp. 1517–1529, 2017.
[29] Q.-L. Wang, H.-X. Sun, and W. Huang, "Multi-party quantum private comparison protocol with *n*-level entangled states," *Quantum Inf. Process.*, vol. 13, no. 11, pp. 2375–2389, 2014.
[30] Y.-J. Chang, C.-W. Tsai, and T. Hwang, "Multi-user private comparison protocol using GHZ class states," *Quantum Inf. Process.*, vol. 12, no. 2, pp. 1077–1088, 2013.
[31] 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, 2012.
[32] Q.-B. Luo, G.-W. Yang, K. She, W.-N. Niu, and Y.-Q. Wang, "Multi-party quantum private comparison protocol based on *d*-dimensional entangled states," *Quantum Inf. Process.*, vol. 13, no. 10, pp. 2343–2352, 2014.
[33] C.-Q. Ye and T.-Y. Ye, "Multi-party quantum private comparison of size relation with *d*-level single-particle states," *Quantum Inf. Process.*, vol. 17, no. 10, p. 252, 2018.
[34] X. Tan, X. Zhang, and J. Li, "Big data quantum private comparison with the intelligent third party," *J. Ambient Intell. Humanized Comput.*, vol. 6, no. 6, pp. 797–806, 2015.
[35] W. Liu and Y.-B. Wang, "Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom," *Int. J. Theor. Phys.*, vol. 55, no. 12, pp. 5307–5317, 2016.
[36] 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, 2016, Art no. 112501.
[37] G. P. He, "Device-independent quantum private comparison protocol without a third party," *Phys. Scripta*, vol. 93, no. 9, 2018, Art. no. 095001.
[38] Y. B. Li *et al.*, "Information leak in Liu et al.'s quantum private comparison and a new protocol," *Eur. Phys. J. D*, vol. 66, no. 4, p. 110, 2012.
[39] J. Lin, H.-Y. Tseng, and T. Hwang, "Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements," *Opt. Commun.*, vol. 284, no. 9, pp. 2412–2414, 2011.
[40] J. Gu, C.-Y. Ho, and T. Hwang, "Statistics attack on 'quantum private comparison with a malicious third party' and its improvement," *Quantum Inf. Process.*, vol. 17, no. 2, p. 23, 2018.
[41] S. Ji *et al.*, "Twice-hadamard-CNOT attack on Li et al.'s fault-tolerant quantum private comparison and the improved scheme," *Frontiers Phys.*, vol. 10, no. 2, pp. 192–197, 2015.
[42] G. P. He, "Comment on 'quantum private comparison of equality protocol without a third party,"ï*Quantum Inf. Process.*, vol. 14, no. 6, pp. 2301–2305, 2015.
[43] M.-K. Zhou, "Improvements of quantum private comparison protocol based on cluster states," *Int. J. Theor. Phys.*, vol. 57, no. 1, pp. 42–47, 2018.
[44] Y.-H. Zhou, W.-M. Shi, and Y.-G. Yang, "Comment on 'efficient and feasible quantum private comparison of equality against the collective amplitude damping noise'," *Quantum Inf. Process.*, vol. 13, no. 2, pp. 573–585, 2014.
[45] Y.-B. Li, T.-Y. Wang, H.-Y. Chen, M.-D. Li, and Y.-T. Yang, "Fault-tolerate quantum private comparison based on GHZ states and ECC," *Int. J. Theor. Phys.*, vol. 52, no. 8, pp. 2818–2825, 2013.
[46] W.-W. Zhang and K.-J. Zhang, "Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party," *Quantum Inf. Process.*, vol. 12, no. 5, pp. 1981–1990, 2013.
[47] Y.-T. Chen and T. Hwang, "Comment on the 'Quantum private comparison protocol based on Bell entangled states'," *Int. J. Theor. Phys.*, vol. 53, no. 3, pp. 837–840, 2014.
[48] B. Zhang, X. Liu, J. Wang, and C. Tang, "Cryptanalysis and improvement of quantum private comparison of equality protocol without a third party," *Quantum Inf. Process.*, vol. 14, no. 12, pp. 4593–4600, 2015.
[49] L. Wen-Jie, L. Chao, C. Han-Wu, L. Zhi-Qiang, and L. Zhi-Hao, "Cryptanalysis and improvement of quantum private comparison protocol based on bell entangled states," *Commun. Theor. Phys.*, vol. 62, no. 2, p. 210, 2014.
[50] Y. Chang, "Cryptanalysis and improvement of the multi-user QPCE protocol with semi-honest third party," *Chin. Phys. Lett.*, vol. 33, no. 1, 2016, Art. no. 010301.
[51] C. Wang, G. Xu, and Y.-X. Yang, "Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs," *Int. J. Quantum Inf.*, vol. 11, no. 04, 2013, Art. no. 1350039.
[52] Z. Sun and D. Long. (2012). "Cryptanalysis of the efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement." [Online]. Available: https://arxiv.org/abs/1204.4587
[53] X.-T. Liu, J.-J. Zhao, J. Wang, and C.-J. Tang, "Cryptanalysis of the secure quantum private comparison protocol," *Phys. Scripta*, vol. 87, no. 6, 2013, Art. no. 065004.
[54] W.-J. Liu, C. Liu, H.-W. Chen, Z.-H. Liu, M.-X. Yuan, and J.-S. Lu, "Improvement on 'an efficient protocol for the quantum private comparison of equality with W state'," *Int. J. Quantum Inf.*, vol. 12, no. 01, 2014, Art. no. 1450001.
[55] I. D. K. Brown, S. Stepney, A. Sudbery, and S. L. Braunstein, "Searching for highly entangled multi-qubit states," *J. Phys. A, Math. Gen.*, vol. 38, no. 5, p. 1119, 2005.
[56] A. Borras, A. R. Plastino, J. Batle, C. Zander, M. Casas, and A. Plastino, "Multiqubit systems: Highly entangled states and entanglement distribution," *J. Phys. A, Math. Theor.*, vol. 40, no. 44, p. 13407, 2007.
[57] P.-X. Chen, S.-Y. Zhu, and G.-C. Guo, "General form of genuine multipartite entanglement quantum channels for teleportation," *Phys. Rev. A*, vol. 74, no. 3, 2006, Art. no. 032324.
[58] H. J. Briegel and R. Raussendorf, "Persistent entanglement in arrays of interacting particles," *Phys. Rev. Lett.*, vol. 86, no. 5, p. 910, 2001.
[59] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 1, pp. 1–127, 2008.

ZHAOXU JI is currently pursuing the Ph.D. degree from the School of Cyber Science and Engineering, Wuhan University, China. His research interests include quantum information processing, quantum computation, and quantum cryptography.

HUANGUO ZHANG was born in 1945. He is currently a Professor and a Ph.D. Supervisor with Wuhan University. His research interests include information security, quantum cryptography, trusted computing, cloud computing, and fault tolerance.