

Commun. Theor. Phys. **72** (2020) 085101 (6pp) https://doi.org/10.1088/1572-9494/ab8a0c

Cryptanalysis and improvement of several quantum private comparison protocols

Zhao-Xu Ji, Pei-Ru Fan, Huan-Guo Zhang and Hou-Zhen Wang

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

E-mail: whz@whu.edu.cn

Received 31 December 2019, revised 23 February 2020
Accepted for publication 25 March 2020
Published 15 July 2020

Abstract

Recently, Wu *et al* (2019 *Int. J. Theor. Phys.* **58** 1854) found a serious information leakage problem in Ye and Ji's quantum private comparison protocol (2017 *Int. J. Theor. Phys.* **56** 1517), that is, a malicious participant can steal another's secret data without being detected through an active attack means. In this paper, we show that Wu *et al*'s active attack is also effective for several other existing protocols, including the ones proposed by Ji *et al* and Zha *et al* (2016 *Commun. Theor. Phys.* **65** 711; 2018 *Int. J. Theor. Phys.* **57** 3874). In addition, we propose what a passive attack means, which is different from Wu *et al*'s active attack in that the malicious participant can easily steal another's secret data only by using his own secret data after finishing the protocol, instead of stealing the data by forging identities when executing the protocol. Furthermore, we find that several other existing quantum private comparison protocols also have such an information leakage problem. In response to the problem, we propose a simple solution, which is more efficient than the ones proposed by Wu *et al*, because it does not consume additional classical and quantum resources.

Keywords: quantum information security, quantum cryptography, quantum private comparison, information leakage problem, passive attack

1. Introduction

Quantum cryptography is a wide concern because of its unconditional security [1–3]. A main difference between quantum cryptography and classical cryptography is that the security of the former is based on some principles of quantum mechanics, while the latter is based on some assumptions of computational complexity. quantum cryptography enables users to detect whether there is an eavesdropper in quantum channels during communications, which cannot be done by classical cryptography [2, 3]. With the rapid development of quantum computers and quantum algorithms, the security of classical cryptography has been severely challenged, which makes the role of quantum cryptography in modern cryptography more and more important [2, 3].

Since the birth of quantum cryptography, quantum key distribution (QKD) has been one of the main research directions in the quantum cryptography domain [2]. Indeed, the first quantum cryptography protocol is the QKD protocol proposed by Bennett *et al* in 1984, which is known as BB84 protocol. QKD aims to generate random shared keys between different users; combined with one-time pad encryption, it can provide unconditional security for users. Moreover, the decoy photon technology derived from QKD has become one of the effective means for eavesdropping checking [4–6].

Quantum private comparison (QPC), originated from the famous 'millionaires' problem' [5–7], aims to judge whether the date of at least two users who do not trust each other are the same or not while maintaining data privacy using some quantum mechanics laws. The comparison of the equality of data is widely used in real life, including secret bidding and auctions, secret ballot elections, e-commerce, and data mining [2]. One of the common applications is the identification of a system for users, which aims to judge whether the users' secret information (e.g., password and fingerprint) is the same as that stored in the system. QPC can also solve the 'Tiercé problem', which is also known as the 'socialist millionaires' problem' [8].

After about ten years of development, QPC has attracted extensive attention in academia. Many protocols have been proposed based on different quantum states or different quantum technologies [12, 9–11, 13–35]. Unfortunately,

information leakage often occurs; many existing QPC protocols have been proved to be insecure [42, 36–41]. Recently, Wu *et al* [42] pointed out that there is a serious information leakage problem in Ye *et al*'s QPC protocol [43]; they showed that a malicious participant in the protocol can steal another's secret information through an active attack means. To solve this problem, they put forward two solutions: one is to use a QKD protocol to establish two new key sequences, and use hash functions to complete a mutual authentication process; the other is to use a QKD protocol to establish a new key sequence and adopt unitary-operation-based symmetric encryption technology. Although the two solutions ensure the security, they both greatly reduce the efficiency of the protocol. On the one hand, both of the solutions use QKD to prepare additional keys, which obviously increases resource consumption. On the other hand, the hash functions and unitary operations need additional quantum devices and technologies, which greatly reduces the feasibility of the protocol. After all, Ye *et al*'s protocol does not use any other quantum technology except for the necessary ones such as preparing quantum states and quantum measurement.

In this paper, we will show that the active attack means proposed by Wu *et al* is also effective for the protocols presented in [44, 46, 45]. That is, these protocols are insecure under the attack. However, we will propose a passive attack means to show that a malicious participant can easily steal another's secret data without using Wu *et al*'s active attack means. Specifically, after the end of the protocol, the malicious participant can steal another's secret data only by using his own secret data. Moreover, we will point out that the passive attack is effective not only for the protocols presented in [43, 44, 46, 45], but also for the protocols presented in [47, 48]. Finally, we will propose a simple and effective solution to the information leakage problem. The rest of the paper is arranged as follows: in section 2, we review briefly the protocol proposed by Ji and Ye [44]. In section 3, we first take Ji and Ye's protocol as an example to show that Wu *et al*'s active attack is also effective to the protocols presented in [44, 46, 45], and then we describe our passive attack means. Section 4 introduces our solution to the information leakage problem. Section 5 summarizes this paper.

2. Review on Ji and Ye's protocol

Let us review the QPC protocol proposed by Ji and Ye [44]. Their protocol uses the highly entangled six-qubit genuine state as information carriers, whose form is given by

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

which is rewritten as

$$\begin{aligned}|\Upsilon\rangle = \frac{1}{4}[&(|0000\rangle - |0101\rangle - |1010\rangle + |1111\rangle) \otimes |\phi^+\rangle \\ &+ (|0001\rangle + |0100\rangle + |1011\rangle + |1110\rangle) \otimes |\psi^+\rangle \\ &+ (|0110\rangle - |0011\rangle - |1001\rangle + |1100\rangle) \otimes |\phi^-\rangle \\ &+ (|0010\rangle + |0111\rangle - |1000\rangle - |1101\rangle) \otimes |\psi^-\rangle],\end{aligned} \tag{2}$$

where

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{3}$$

are four Bell states.

The prerequisites of the protocol are:

1. Suppose that Alice and Bob have the secret data X and Y respectively, and that the binary representations of X and Y are $(x_1, x_2,\ldots,x_N)$ and $(y_1, y_2,\ldots,y_N)$ respectively, where $x_j, y_j \in\{0, 1\}$ $\forall j \in \{1, 2,\ldots,N\}$, hence $X = \sum_{j=1}^{N} x_j 2^{j-1}$, $Y = \sum_{j=1}^{N} y_j 2^{j-1}$.
2. Alice(Bob) divides the binary representation of $X(Y)$ into $\lceil N/2\rceil$ groups:
$$G_A^1, G_A^2,\ldots,G_A^{\lceil \frac{N}{2}\rceil}(G_B^1, G_B^2,\ldots,G_B^{\lceil \frac{N}{2}\rceil}). \tag{4}$$
Each group $G_A^i(G_B^i)$ includes two bits, where $i = 1, 2,\ldots,\lceil N/2\rceil$ throughout this protocol. If N mod $2 = 1$, Alice (Bob) adds one 0 into the last group $G_A^{\lceil N/2\rceil}(G_B^{\lceil N/2\rceil})$.
3. Alice and Bob generate the shared key sequences $\{K_A^1, K_A^2,\ldots,K_A^{\lceil N/2\rceil}\}$ and $\{K_B^1, K_B^2,\ldots,K_B^{\lceil N/2\rceil}\}$ through a QKD protocol, where K_A^i, $K_B^i \in \{00, 01, 10, 11\}$. Similarly, Alice(Bob) and TP generate the shared key sequence $\{K_{AC}^1, K_{AC}^2,\ldots,K_{AC}^{\lceil N/2\rceil}\}$ ($\{K_{BC}^1, K_{BC}^2,\ldots,K_{BC}^{\lceil N/2\rceil}\}$), where K_{AC}^i, $K_{BC}^i \in \{00, 01, 10, 11\}$.
4. Alice, Bob and TP agree on the following coding rules: $|0\rangle \leftrightarrow 0$, $|1\rangle \leftrightarrow 1$, $|\phi^+\rangle \leftrightarrow 00$, $|\phi^-\rangle \leftrightarrow 11$, $|\psi^+\rangle \leftrightarrow 01$, and $|\psi^-\rangle \leftrightarrow 10$.

The steps of the protocol are as follows:

1. TP prepares $\lceil N/2\rceil$ copies of the highly entangled six-qubit genuine state $|\Upsilon\rangle$, and marks them by
$$\begin{aligned}&|\Upsilon(p_1^1, p_1^2, p_1^3, p_1^4, p_1^5, p_1^6)\rangle, \\ &|\Upsilon(p_2^1, p_2^2, p_2^3, p_2^4, p_2^5, p_2^6)\rangle,\ldots, \\ &|\Upsilon(p_{\lceil N/2\rceil}^1, p_{\lceil N/2\rceil}^2, p_{\lceil N/2\rceil}^3, p_{\lceil N/2\rceil}^4, p_{\lceil N/2\rceil}^5, p_{\lceil N/2\rceil}^6)\rangle,\end{aligned} \tag{5}$$

in turn to generate an ordered sequence, where the subscripts 1, 2,…,$\lceil N/2 \rceil$ denote the order of the highly entangled six-qubit genuine states in the sequence, and the superscripts 1, 2, 3, 4, 5, 6 denote six particles in one state. Then TP takes the first two particles out from $|\Upsilon(p_i^1, p_i^2, p_i^3, p_i^4, p_i^5, p_i^6)\rangle$ to construct the new sequence

$$p_1^1, p_1^2, p_2^1, p_2^2, \ldots, p_{\lceil N/2 \rceil}^1, p_{\lceil N/2 \rceil}^2, \tag{6}$$

and denotes it as S_A. Similarly, he takes out the third and fourth particles to construct another new sequence

$$p_1^3, p_1^4, p_2^3, p_2^4, \ldots, p_{\lceil N/2 \rceil}^3, p_{\lceil N/2 \rceil}^4, \tag{7}$$

and denotes it as S_B. The remaining particles construct another new sequence

$$p_1^5, p_1^6, p_2^5, p_2^6, \ldots, p_{\lceil N/2 \rceil}^5, p_{\lceil N/2 \rceil}^6, \tag{8}$$

denoted as S_C.

2. TP prepares two sets of decoy photons in which each decoy photon is chosen randomly from the single-particle states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, where $|\pm\rangle = 1/\sqrt{2}\,(|0\rangle \pm |1\rangle)$. Then he inserts randomly the two sets of decoy photons into S_A and S_B, respectively, and records the insertion positions. Finally, he denotes the two new generated sequences as S_A^* and S_B^*, and sends them to Alice and Bob, respectively.
3. After receiving S_A^* and S_B^*, TP and Alice(Bob) use the decoy photons in S_A^* and S_B^* to judge whether eavesdroppers exist in quantum channels. The error rate exceeding the predetermined threshold will lead to the termination and restart of the protocol, otherwise the protocol proceeds to the next step.
4. Alice(Bob) measures the two particles marked by p_i^1, p_i^2 (p_i^3, p_i^4) in $S_A(S_B)$ with Z basis ($\{|0\rangle, |1\rangle\}$), and denotes the binary numbers corresponding to the measurement results as $M_A^i(M_B^i)$. Then, Alice(Bob) calculates $G_A^i \oplus M_A^i \oplus K_{AC}^i \oplus K_A^i$ ($G_B^i \oplus M_B^i \oplus K_{BC}^i \oplus K_B^i$), and marks the calculation results by $R_A^i(R_B^i)$. Finally, Alice(Bob) announces $R_A^i(R_B^i)$ to TP.
5. After receiving $R_A^i(R_B^i)$, TP performs Bell measurements on the particles marked by p_i^5, p_i^6 in S_C, and marks the binary numbers corresponding to the measurement results by M_C^i. Then, he calculates $R_A^i \oplus R_B^i \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i$, and marks the calculation results by R_i. Finally, he announces R_i to Alice and Bob.
6. After receiving R_i, Alice and Bob calculate $R_i \oplus K_A^i \oplus K_B^i$, respectively, and mark the calculation results by R_i'. If $R_i' = 00$ (i.e. each classical bits in R_i' is 0), they conclude that their data X and Y are the same. Otherwise, they conclude that X and Y are different and stop the comparison.

3. Information leakage problem

In this section, we will show that the protocol is insecure under Wu *et al*'s active attack means: a malicious participant can steal the secret information of another by forging identities. We will then propose a passive attack means by which the malicious participant can also steal the secret information of another.

3.1. Information leakage under Wu et al's active attack

Let us now show how a malicious participant steal another's secret information by using Wu *et al*'s active attack. Without losing generality, we assume that Bob is malicious. He can steal Alice's secret data through the following steps:

1. In the second step of Ji and Ye's protocol, when TP sends the particle sequence S_A^* to Alice, Bob intercepts all the particles in the sequence, and then he pretends to be Alice and tells TP that he has received all the particles.
2. Bob continues to pretends to be Alice and completes eavesdropping checking with TP. Then he performs single-particle measurements on the particles marked by p_i^1, p_i^2 in S_A, and denotes the binary numbers corresponding to the measurement results as M_{AB}^i. Finally, TP denotes the particle sequence after measurements as S_A^1.
3. Similar to the second step of Ji and Ye's protocol, Bob prepares a set of decoy photons, and then inserts them randomly into S_A^1. The new generated sequence is denoted as S_A^{1*}. Finally, Bob pretends to be TP and sends S_A^{1*} to Alice.
4. After confirming that Alice has received S_A^{1*}, Bob continues to pretends to be TP and completes eavesdropping checking with Alice. If there is no eavesdropping, according to the protocol procedures, Alice measures each particle in S_A^1 with Z basis, and denotes the binary numbers corresponding to the measurement results as M_A^i (obviously, M_A^i is the same as M_{AB}^i, i.e. $M_A^i = M_{AB}^i$). Then she calculates $G_A^i \oplus M_A^i \oplus K_{AC}^i \oplus K_A^i$, and marks the calculation results by R_A^i. Finally, Alice announces R_A^i to TP. Similarly, Bob announces R_B^i to TP after completing measurements and calculations in accordance with the protocol procedures.
5. According to the protocol procedures, TP completes measurements, calculations, and publishes R_i to Alice and Bob. After receiving R_i, Bob can calculate

$$\begin{aligned} &R_i \oplus K_{BC}^i \oplus M_C^i \oplus R_B^i \oplus K_A^i \oplus M_{AB}^i \\ &= (R_A^i \oplus R_B^i \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i) \oplus K_{BC}^i \\ &\quad \oplus M_C^i \oplus R_B^i \oplus K_A^i \oplus M_{AB}^i \\ &= R_A^i \oplus K_{AC}^i \oplus K_A^i \oplus M_{AB}^i \\ &= (G_A^i \oplus M_A^i \oplus K_{AC}^i \oplus K_A^i) \oplus K_{AC}^i \oplus K_A^i \oplus M_{AB}^i = G_A^i. \end{aligned} \tag{9}$$

Note here that $M_A^i = M_{AB}^i$, and Bob can deduce M_C^i from equation (1) based on M_{AB}^i and M_B^i. From the above equation, Bob can obtain G_A^i through the calculation, thus he can deduce Alice's secret data X.

We have shown that Wu *et al*'s active attack is also effective for Ji and Ye's protocol, that is, their protocol will leak information under Wu's active attack. In addition, we find that the protocols presented in [44, 46, 45] also have such an information leakage problem, because the process of these protocols is similar to that of Ji and Ye's protocol.

In what follows, we will present a passive attack means, by which we will show that a malicious participant can easily steal the secret data of another based on his own secret data after the end of the protocol, instead of using Wu *et al*'s active attack means.

3.2. Information leakage under the proposed passive attack

At the end of the protocol, both Alice and Bob obtain $G_A^i \oplus G_B^i$ (i.e. R_i'), that is,

$$\begin{aligned} R_i' &= R_i \oplus K_A^i \oplus K_B^i \\ &= (R_A^i \oplus R_B^i \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i) \oplus (K_A^i \oplus K_B^i) \\ &= [(G_A^i \oplus M_A^i \oplus K_{AC}^i \oplus K_A^i) \oplus (G_B^i \oplus M_B^i \oplus K_{BC}^i \oplus K_B^i) \\ &\quad \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i] \oplus (K_A^i \oplus K_B^i) \\ &= (G_A^i \oplus G_B^i) \oplus (M_A^i \oplus M_B^i \oplus M_C^i) = G_A^i \oplus G_B^i. \end{aligned} \tag{10}$$

In this case, Alice and Bob can easily steal each other's data. Specifically, Alice(Bob) can calculate $R_i' \oplus G_A^i (R_i' \oplus G_B^i)$, thus she(he) can get $G_B^i (G_A^i)$, that is, $R_i' \oplus G_A^i = (G_A^i \oplus G_B^i) \oplus G_A^i = G_B^i$ $[R_i' \oplus G_B^i = (G_A^i \oplus G_B^i) \oplus G_B^i = G_A^i]$. In fact, for a cryptography protocol, the process, prerequisites, and coding rules of the protocol are all public, except that the keys generated in the protocol is confidential. Therefore, Alice and Bob, as participants in the protocol, obviously know that the final comparison result is $G_A^i \oplus G_B^i$.

We find that the protocols in [43, 47, 48, 45, 46] also have such an information leakage problem. In these protocols, both Alice and Bob obtain $G_A^i \oplus G_B^i$ at the end of the protocol, thus they can easily know each other's data.

4. New solution to the information leakage problem

We have proposed a passive attack means, and described the information leakage problem of several QPC protocols under this attack. Indeed, the information leakage problem is the same as that under Wu *et al*'s active attack, i.e. two participants can steal each other's secret data. To solve this problem, Wu *et al* put forward two solutions, which has been mentioned in the introduction. In what follows, we will propose a new solution, and then briefly compare our solution with those of Wu *et al.*

4.1. The proposed solution

Let us now describe our solution. For simplicity and clarity, we change directly the steps 5 and 6 of Ji and Ye's protocol as follows (the first four steps of the protocol remain unchanged):

1. After receiving $R_A^i (R_B^i)$, TP performs Bell measurements on the particles marked by p_i^5, p_i^6, and marks the binary numbers corresponding to the measurement results by M_C^i. Subsequently, TP calculates $R_A^i \oplus R_B^i \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i$, and marks the calculation results by $a_i^1 a_i^2$ (note that each calculation result is a binary number which contains two bits, i.e. $a_i^1 a_i^2 \in \{00, 01, 10, 11\}$). Then, TP calculates
$$\sum_{i=1}^{\lceil N/2 \rceil} \sum_{j=1}^{2} a_i^j. \tag{11}$$
Marking the calculation result by S, TP announces S to Alice and Bob.
2. After receiving S, Alice and Bob calculate $K_A^i \oplus K_B^i$, respectively, and mark the calculation results by $b_i^1 b_i^2$. Then, they calculate
$$\sum_{i=1}^{\lceil N/2 \rceil} \sum_{j=1}^{2} b_i^j, \tag{12}$$
and marks the calculation result by S'. Finally, they calculate $S - S'$. If $S - S' = 0$, they can conclude that their data X and Y are the same. Otherwise, they conclude that X and Y are different.

The correctness of our solution is easy to verify. In Step 5, TP calculates $R_A^i \oplus R_B^i \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i$, hence we get

$$\begin{aligned} & R_A^i \oplus R_B^i \oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i \\ &= (G_A^i \oplus M_A^i \oplus K_{AC}^i \oplus K_A^i) \\ &\oplus (G_B^i \oplus M_B^i \oplus K_{BC}^i \oplus K_B^i) \\ &\oplus K_{AC}^i \oplus K_{BC}^i \oplus M_C^i \\ &= G_A^i \oplus G_B^i \oplus K_A^i \oplus K_B^i. \end{aligned} \tag{13}$$

Obviously, $S = \sum_{i=1}^{\lceil N/2 \rceil} \sum_{j=1}^{2} b_i^j$ (i.e. $S = S'$) if and only if $G_A^i = G_B^i$. Otherwise, $S \neq S'$. Note here that K_A^i and K_B^i are random keys generated by QKD, thus K_A^i and K_B^i are not all the same (the probability that they are all the same can be ignored because it is very small).

Similar improvements can be made to the protocols presented in [43, 47, 48, 45, 46]. For simplicity, we would not like to review these protocols and describe their amendments.

4.2. Comparison

Let us make a brief comparison between our solution and the ones proposed by Wu *et al.* In our solution, we just change slightly the algorithm without using any additional quantum technology and resources. In contrast, both the solutions proposed by Wu *et al* need to consume additional quantum technology and resources (see the introduction). We show these differences in table 1.

Table 1. Comparison with Wu *et al*'s solutions.

	Wu *et al*'s solution 1	Wu *et al*'s solution 2	Our solution
additional keys	√	√	×
hash functions	√	×	×
unitary operations	×	√	×

5. Conclusion

We have shown that several QPC protocols have the same information leakage problem under Wu *et al*'s active attack. We have proposed a passive attack means, and shown that several QPC protocols are insecure under this attack: a malicious participant can easily steal another's secret data after the end of the protocol. We have proposed a simple and effective solution to this problem, which is more efficient than the ones proposed by Wu *et al.* We believe that our solution is constructive to the design of a QPC protocol.

Acknowledgments

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

References

[1] Zhang H G *et al* 2015 Survey on cyberspace security *Sci. China Inform. Sci.* **58** 1–43
[2] Zhang H G *et al* 2019 Survey on quantum information security *China Commun.* **16** 1–36
[3] Ji Z X *et al* 2019 Quantum protocols for secure multi-party summation *Quantum Inf. Process.* **18** 168
[4] Ji Z X, Fan P R and Zhang H G 2019 Entanglement swapping of Bell states and a special class of Greenberger-Horne-Zeilinger states (arXiv:1911.09875)
[5] Yang Y G and Wen Q Y 2009 An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement *J. Phys. A: Math. Theor.* **42** 055305
[6] Liu W J *et al* 2013 Quantum private comparison: a review *IETE Tech. Rev.* **30** 439–45
[7] Yao A C 2008 Protocols for secure computations *XXIII Ann. Symp. on Foundations of Computer Science (SFCS'1982)* (Piscataway, NJ: IEEE) pp 160–4
[8] Boudot F *et al* 2001 A fair and efficient solution to the socialist millionaires' problem *Discrete Appl. Math.* **111** 23–36
[9] Chen X B *et al* 2010 An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement *Opt. Commun.* **283** 1561–5
[10] Ji Z X, Zhang H G and Fan P R 2019 Two-party quantum private comparison protocol with maximally entangled seven-qubit state *Mod. Phys. Lett.* A **34** 1950229
[11] Ji Z X, Fan P R and Zhang H G 2019 Several two-party protocols for quantum private comparison using entanglement and dense coding *Opt. Commun.* **459** 124911
[12] Ji Z X, Zhang H G and Wang H Z 2019 Quantum private comparison protocols with a number of multi-particle entangled states *IEEE Access* **7** 44613–21
[13] Ji Z X, Fan P R, Wang H Z and Zhang H G 2019 Entanglement-based quantum private comparison protocol with bit-flipping (arXiv:1911.08075)
[14] Liu W and Wang Y B 2012 Quantum private comparison based on GHZ entangled states *Int. J. Theor. Phys.* **51** 3596–604
[15] Lin S *et al* 2013 Quantum private comparison of equality with χ-type entangled states *Int. J. Theor. Phys.* **52** 4185–94
[16] Li J *et al* 2014 An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping *Int. J. Theor. Phys.* **53** 2167–76
[17] Sun Z and Long D 2013 Quantum private comparison protocol based on cluster states *Int. J. Theor. Phys.* **52** 212–8
[18] Xu G A *et al* 2012 An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state *Int. J. Quantum Inf.* **10** 1250045
[19] Tseng H Y, Lin J and Hwang T 2012 New quantum private comparison protocol using EPR pairs *Quantum Inf. Process.* **11** 373–84
[20] He G P 2018 Device-independent quantum private comparison protocol without a third party *Phys. Scr.* **93** 095001
[21] Li Y B *et al* 2013 Fault-tolerate quantum private comparison based on GHZ states and ECC *Int. J. Theor. Phys.* **52** 2818–25
[22] Li C *et al* 2019 Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state *Quantum Inf. Process.* **18** 158
[23] Huang W *et al* 2013 Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels *Sci. China Phys. Mech.* **56** 1670–8
[24] Li L and Shi R H 2019 A novel and efficient quantum private comparison scheme *J. Korean Phys. Soc.* **75** 15–21
[25] Guo F Z *et al* 2013 Quantum private comparison protocol based on entanglement swapping of d-level Bell states *Quantum Inf. Process.* **12** 2793–802
[26] Pan H M 2017 Quantum private comparison based on χ-type entangled states *Int. J. Theor. Phys.* **56** 3340–7
[27] Xu L and Zhao Z W 2019 High-capacity quantum private comparison protocol with two-photon hyperentangled Bell states in multiple-degree of freedom *Eur. Phys. J.* D **73** 58
[28] Liu B *et al* 2017 Quantum private comparison employing single-photon interference *Quantum Inf. Process.* **16** 180
[29] Jia H Y *et al* 2012 Quantum private comparison using genuine four-particle entangled states *Int. J. Theor. Phys.* **51** 1187–94
[30] Ji Z X and Ye T Y 2017 Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level Bell states *Quantum Inf. Process.* **16** 177
[31] Song X and Wen A 2019 Multiparty quantum private comparison of size relation based on single-particle states *IEEE Access* **7** 142507–14
[32] Abulkasim H *et al* 2019 Improved dynamic multi-party quantum private comparison for next-generation mobile network *IEEE Access* **7** 17917–26
[33] Huang S L *et al* 2015 Multi-party quantum private comparison with an almost-dishonest third party *Quantum Inf. Process.* **14** 4225–35

[34] Wang Q L *et al* 2014 Multi-party quatum private compariso protocol with n-level etagled states *Quantum Inf. Process.* **13** 2375–89
[35] Ye T Y and Ji Z X 2017 Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states *Sci. China Phys. Mech.* **60** 090312
[36] Ji S *et al* 2015 Twice-Hadamard-CNOT attack on Li *et al*'s fault-tolerant quantum private comparison and the improved scheme *Front. Phys.* **10** 192–7
[37] Pan H M 2018 Intercept-Resend-Measure attack towards quantum private comparison protocol using genuine four-particle entangled states and its improvement *Int. J. Theor. Phys.* **57** 2034–40
[38] Liu W J *et al* 2014 Cryptanalysis and improvement of quantum private comparison protocol based on Bell entangled states *Commun. Theor. Phys.* **62** 210
[39] Wang C *et al* 2013 Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs *Int. J. Quantum Inf.* **11** 1350039
[40] Liu X T *et al* 2013 Cryptanalysis of the secure quantum private comparison protocol *Phys. Scr.* **87** 065004
[41] Chang Y *et al* 2016 Cryptanalysis and improvement of the multi-user QPCE protocol with semi-honest third party *Chin. Phys. Lett.* **33** 010301
[42] Wu W Q *et al* 2019 Cryptanalysis and Improvement of Ye *et al*'s Quantum Private Comparison Protocol *Int. J. Theor. Phys.* **58** 1854–60
[43] Ye T Y and Ji Z X 2017 Two-party quantum private comparison with five-qubit entangled states *Int. J. Theor. Phys.* **56** 1517–29
[44] Ji Z X and Ye T Y 2016 Quantum private comparison of equal information based on highly entangled six-qubit genuine state *Commun. Theor. Phys.* **65** 711
[45] Zha X W *et al* 2018 Quantum private comparison protocol with five-particle cluster states *Int. J. Theor. Phys.* **57** 3874–81
[46] Zhang W W *et al* 2014 Quantum private comparison protocol with W States *Int. J. Theor. Phys.* **53** 1723–9
[47] Wang F *et al* 2016 Quantum private comparison based on quantum dense coding *Sci. China Inform. Sci.* **59** 112501
[48] Zhang W W *et al* 2013 Quantum private comparison based on quantum search algorithm *Int. J. Theor. Phys.* **52** 1466–73